الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

X.1142

(2006/06)

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة والأمن

أمن الاتصالات

لغة وسم موسعة للتحكم في النفاذ (XACML 2.0)

التوصيـــة ITU-T X.1142

ITU-T

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة والأمن

الشبكات العمومية للبيانات	
الخدمات والمرافق	X.19–X.1
السطوح البينية	X.49–X.20
الإرسال والتشوير والتبديل	X.89–X.50
جوانب الشبكة	X.149–X.90
الصيانة	X.179–X.150
الترتيبات الإدارية	X.199–X.180
التوصيل البيني للأنظمة المفتوحة	
النموذج والترميز	X.209–X.200
تعاريف الخدمات	X.219–X.210
مواصفات البروتوكول بأسلوب التوصيل	X.229–X.220
مواصفات البروتوكول بأسلوب غياب التوصيل	X.239–X.230
جداول إعلان المطابقة (PICS)	X.259–X.240
تعرّف هوية البروتوكول	X.269–X.260
بروتوكولات الأمن	X.279–X.270
أشياء مسيرة على الطبقة	X.289–X.280
اختبار المطابقة	X.299–X.290
التشغيل البيني للشبكات	
اعتبارات عامة	X.349–X.300
الأنظمة الساتلية لإرسال البيانات	X.369–X.350
الشبكات القائمة على بروتوكول الإنترنت	X.399–X.370
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التوصيل الشبكي في التوصيل البيني للأنظمة المفتوحة (OSI) وجوانب النظام	
التوصيل الشبكي	X.629–X.600
الفعالية	X.639–X.630
نوعية الخدمة	X.649–X.640
التسمية والعنونة والتسجيل	X.679–X.650
ترميز النظم المجرد واحد (ASN.1)	X.699–X.680
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	
الإطار والهيكل المعماري لإدارة الأنظمة	X.709–X.700
خدمة اتصالات الإدارة وبروتوكولاتها	X.719–X.710
هيكل معلومات الإدارة	X.729–X.720
وظائف الإدارة ووظائف الهيكل المعماري للإدارة الموزعة المفتوحة	X.799–X.730
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	
الالتزام والتلازم والاستعادة	X.859–X.850
معالجة المعاملات	X.879–X.860
العمليات البُعدية	X.889–X.880
التطبيقات التنوعية لترميز النظم المجرد واحد (ASN.1)	X.899–X.890
المعالجة الموزعة المفتوحة	X.999–X.900
أمن الاتصالات	**X.1000–**

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

التوصيـــة ITU-T X.1142

لغة وسم موسعة للتحكم في النفاذ (XACML 2.0)

ملخص

اللغة XACML هي مجموعة مفردات لغة الوسم الموسعة (XML) التي تستخدم في التعبير عن سياسات التحكم في النفاذ. وينطوي التحكم في النفاذ على اتخاذ قرار بقبول طلب النفاذ إلى موارد ما وتنفيذ هذا القرار. وتعرّف هذه التوصية اللغة XACML المركزية بما فيها قواعد هذه اللغة ونماذجها والسياق مع نموذج لغة السياسة وقواعد التركيب والمعالجة. وتحدد هذه التوصية مواصفة التحكم في النفاذ القائم على اللغة XACML المركزية والدور التراتبي. كما تتحدد مواصفة موارد متعددة للغة XACML والمواصفة SAML 2.0 للغة XACML. وحرصاً على تعزيز أمن تبادل السياسات القائمة على اللغة XACML، تحدد هذه التوصية أيضاً مواصفة التوقيع الرقمي (XML) في اللغة XACML لضمان أمن المعطيات. وتتحدد مواصفة الخصوصية بهدف تقديم إرشادات للمنفذين.

وتكافئ هذه التوصية المعيار OASIS XACML 2.0 وتتواءم معه.

المصدر

وافقت لجنة الدراسات 17 (2005-2008) لقطاع تقييس الاتصالات على التوصية ITU-T X.1142 بتاريخ 13 يونيو 2006 وذلك بموجب الإجراء المحدد في التوصية ITU-T A.8.

تمهيـــد

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).

ملاحظـــة

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

المحتـــويات

الصفحة

الصفحة

التوصيـــة ITU-T X.1142

لغة وسم موسعة للتحكم في النفاذ (XACML 2.0)

1 مجال التطبيق

تعرّف هذه التوصية النسخة 2.0 من لغة وسم التحكم في النفاذ القابلة للتوسيع (XACML). كما تعرّف لغة عامة للتعبير عن سياسة الأمن. والبواعث الكامنة وراء إعداد اللغة XACML هي وضع لغة سياسة قائمة على اللغة XML يمكن استخدامها في توفير:

- طريقة لجمع قواعد وسياسات متفرقة في مجموعة واحدة تطبق على طلب قرار خاص.
- طريقة تعريف مرن للإجراء الذي تُجمع بموجبه القواعد والسياسات.
- طريقة للتعامل مع جهات مستعملة متعددة تعمل بمقدرات مختلفة.
- طريقة لإصدار قرار الترخيص استناداً إلى نعوت الموضوع والموارد.
- طريقة للتعامل مع نعوت متعددة القيم.
- طريقة لإصدار قرار الترخيص استناداً إلى محتويات مورد المعلومات.
- مجموعة مؤثرات منطقية ورياضية بشأن نعوت الموضوع والموارد والبيئة.
- طريقة لمعالجة مجموعة موزعة من مكونات السياسة بغض النظر عن الطريقة المتعلقة بتحديد موقع مكونات السياسة واستعادتها واستيقائها.
- طريقة سريعة لتحديد السياسة التي تطبق على إجراء معين على أساس قيم نعوت البنود والموارد والإجراءات.
- طبقة نظرية مجردة تعزل كاتب السياسة عن تفاصيل بيئة التطبيق.
- طبقة لتحديد مجموعة إجراءات يتعين القيام بها مع تنفيذ السياسة.

وترد الحلول XACML الخاصة بكل من هذه المتطلبات في هذه التوصية. وخصوصاً في الفقرة 7 التي تعرض لب اللغة XACML بما فيها النماذج XACML ونموذج لغة السياسة وقواعد تركيبها وقواعد المعالجة. وتعرض الفقرة 8 لب اللغة XACML ومواصفة التحكم في النفاذ القائم على الدور (RBAC) التراتبي. وتعرض الفقرة 9 مواصفة تعدد موارد اللغة XACML. أما الفقرة 10 فتناقش التكنولوجيات الكفيلة بالحفاظ على أمن الاتصالات XACML من خلال تطوير المواصفة SAML 2.0 للغة XACML. وتستند الفقرة 11 إلى الفقرة 10 لوضع مواصفة التوقيع الرقمي XACML. وتناقش الفقرة 12 جمع المواصفات XACML الواردة في الفقرات من 7 إلى 11 من خلال وضع مواصفة الموارد التراتبية للغة XACML. أما قضايا السرية فتطرح في الفقرة 13.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، نحث جميع المستعملين لهذه التوصية على السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية. وينشر المعهد IETF قائمة بالمعايير RFC مع تلك التي بطل مفعولها واستبدلت بالمعايير RFC الحديثة. وتنشر مجموعة الشبكات المعلوماتية العالمية (W3C) قائمة بأحدث التوصيات والمنشورات الأخرى.

- التوصية ITU-T X.811 (1995) | المعيار ISO/IEC 10181-2:1996، تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن في الأنظمة المفتوحة: إطار الاستيقان.
- ITU-T Recommendation X.811 (1995) | ISO/IEC 10181-2:1996, Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.
- 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.1141 (2006), Security Assertion Markup Language (SAML 2.0).
- IETF RFC 822 (1982), Standard for the Format of ARPA Internet Text Messages.
- IETF RFC 2119 (1997), Key words for use in RFCs to Indicate Requirement Levels.
- IETF RFC 2253 (1997), Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names.

– IETF RFC 2256 (1997), A Summary of the X.500 (96) User Schema for use with LDAPv3.
– IETF RFC 2396 (1998), Uniform Resource Identifiers (URI): Generic Syntax.
– IETF RFC 2732 (1999), Format for Literal IPv6 Addresses in URL's.
– IETF RFC 2821 (2001), Simple Mail Transfer Protocol.
– IETF RFC 3280 (2002), Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
– W3C Canonicalization:2002, Exclusive XML Canonicalization Version 1.0, W3C Recommendation, Copyright © [18 July 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/xml-exc-c14n/.
– W3C Datatypes:2001, XML Schema Part 2: Datatypes, W3C Recommendation, Copyright © [2 May 2001] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/.
– W3C Encryption:2002, XML Encryption Syntax and Processing, W3C Recommendation, Copyright © [10 December 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/.
– W3C MathML:2003, Mathematical Markup Language (MathML), Version 2.0, W3C Recommendation, Copyright © [21 October 2003] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2003/REC-MathML2-20031021/.
– W3C Signature:2002, XML-Signature Syntax and Processing, W3C Recommendation, Copyright © [12 February 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/.
– W3C XML:2004, Extensible Markup Language (XML) 1.0 (Third Edition), W3C Recommendation, Copyright © [4 February 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/REC-xml/.
– W3C XPATH:1999, XML Path Language, Version 1.0, W3C Recommendation, Copyright © [16 November 1999] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/1999/REC-xpath-19991116.
– W3C XSLT:1999, XSL Transformations (XSLT) Version 1.0, W3C Recommendation, Copyright © [16 November 1999] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/1999/REC-xslt-19991116.

ملاحظة - الإشارة إلى وثيقة في هذه التوصية لا تضفي على الوثيقة صفة التوصية.

3 التعاريف

تستخدم التعاريف التالية لأغراض هذه التوصية.

1.3 تعاريف مستمدة من مراجع أخرى

1.1.3 تستخدم هذه التوصية المصطلح التالي المعرف في التوصية ITU-T X.811:

أ) المبدأ

2.1.3 تستخدم هذه التوصية المصطلحين التاليين المعرفين في التوصية ITU-T X.812:

أ) معلومات بشأن التحكم في النفاذ؛

ب) المستعمل.

3.1.3 تستخدم هذه التوصية المصطلحين التاليين المعرفين في معجم خدمات الويب الصادر عن المجموعة W3C:

أ) مكان الاسم؛

ب) مخطط اللغة XML.

4.1.3 تستخدم هذه التوصية المصطلحات التالية المعرفة في المعيار IETF RFC 2828:

أ) النفاذ؛

ب) التحكم في النفاذ؛

ج) نقطة إدارة السياسة؛

د) نقطة قرار السياسة؛

هـ) نقطة تطبيق السياسة؛

و) معمارية الأمن؛

ز) سياسة الأمن؛

ح) خدمة الأمن.

5.1.3 تستخدم هذه التوصية المصطلحين التاليين المعرفين في المعيار IETF RFC 2396:

أ) معرف هوية مورد عالمي؛

ب) مرجع معرف URI.

6.1.3 تستخدم هذه التوصية المصطلح التالي المعرف في التوقيع W3C XML:

أ) غرض معطيات.

2.3 تعاريف إضافية

1.2.3 **نفاذ**: أداء إجراء ما.

2.2.3 **التحكم في النفاذ**: التحكم في النفاذ وفقاً لسياسة ما.

3.2.3 **إجراء**: عملية تتم في المورْد.

4.2.3 **سياسة قابلة للتطبيق**: مجموعة سياسات ومجموعات سياسية تتحكم في النفاذ لأغراض طلب قرار محدد.

5.2.3 **نعت**: صفة لجهة أو مورْد أو إجراء أو بيئة يمكن الإحالة إليها في عبارة منطقية أو في هدف ما.

6.2.3 **سلطة النعت (AA)**: كيان يجمع بين النعوت والهويات. ويمكن التعبير عن تجميع من هذا القبيل باستخدام مزعم نعت SAML يصدر عن سلطة النعت.

7.2.3 **قرار الترخيص**: نتيجة تقييم سياسة مستخدمة ترسلها النقطة PDP إلى النقطة PEP. وهو وظيفة تقيِّم أن غرضاً ما "مسموح" أو "مرفوض" أو "غير محدد" أو "غير قابل للتطبيق" وتضع (خيارياً) مجموعة التزامات.

8.2.3 **سلة**: مجموعة غير مرتبة من القيم قد تتواجد فيها قيم مضاعفة.

9.2.3 **شرط**: عبارة من المسندات. وهو الوظيفة التي تقيّم بالصفات "صح" أو "خطأ" أو "غير محدد".

10.2.3 **تتابع ربط**: تتابع عبارات منطقية تربط بينها العملية المنطقية 'و' ('AND').

11.2.3 **سياق**: تمثيل منظم لطلب القرار وقرار الترخيص.

12.2.3 **إدارة السياق**: كيان النظام الذي يحوِّل طلبات القرار من نسق الطلب الأصلي إلى الشكل النظامي للغة XACML ويحوِّل قرارات الترخيص من الشكل النظامي للغة XACML إلى نسق الإجابة الأصلي.

13.2.3 **الحارس**: الكيان الذي تودع لديه المعلومات الكفيلة بتحديد هوية الشخص.

14.2.3 **غرض معطيات**: وهو غرض رقمي تم توقيعه. ويحال إلى غرض المعطيات في العنصر (Reference) باستعمال المعرّف URI.

15.2.3 **قرار**: نتيجة تقييم قاعدة أو سياسة أو مجموعة سياسات.

16.2.3 **طلب قرار**: طلب توجه النقطة PEP إلى النقطة PDP من أجل الحصول على قرار ترخيص.

17.2.3 **تتابع فصل**: تتابع عبارات منطقية تفصل بينها العملية المنطقية 'أو' ('OR').

18.2.3 **أثر**: النتيجة المتوقعة لقاعدة مستوفاة شروطها ("مسموح" أو "مرفوض").

19.2.3 **بيئة**: مجموعة النعوت المتصلة بقرار ترخيص والمستقلة عن جهة مستعملة أو مورد أو إجراء ما.

20.2.3 السياسة HasPrivilegesOfRole: نمط خياري للمعلمة <Policy> يمكن إدراجه في الرخصة <PolicySet> بغية إتاحة طرح أسئلة عما إذا كان لجهة ما "امتيازات" في دور محدد.

21.2.3 مورد تراتبي: مورد ينتظم على شكل تفرع (شجرة) أو مجموعة تفرعات (غابة) (خط بياني موجه لا دوري) لموارد إفرادية اسمها عُقَد.

22.2.3 دور صغير: يكون الدور A في تراتبية الأدوار صغيراً نسبةً إلى الدور B إذا ورث الدور B جميع الرخص المصاحبة للدور A.

23.2.3 الرخص متعددة الأدوار: مجموعة رخص يتعين أن يمتلك المستعمل أكثر من واحدة منها في آن، لكي يتمكن من النفاذ.

24.2.3 نعت مسمّى: حالة محددة من النعت يحددها اسم النعت ونمطه وهوية صاحب النعت (الذي قد يكون من النمط: جهة مستعملة أو مورد أو إجراء أو بيئة) و(خيارياً) هوية السلطة التي تصدره.

25.2.3 عقدة: مورد منفرد يشكل جزءاً من المورد التراتبي.

26.2.3 التزام: عملية محددة في سياسة أو مجموعة سياسات ينبغي أن تقوم بها النقطة PEP بالترافق مع تنفيذ قرار الترخيص.

27.2.3 مالك: الجهة التي تحدد المعلومات هويتها الشخصية.

28.2.3 الرخصة: التخويل أو الحق الذي يتيح إجراء بعض الأعمال في بعض الموارد وفق شروط محددة حسب الاقتضاء.

29.2.3 مجموعة سياسات الرخصة (<Policy Set>) (PPS): هي معلمة <PolicySet> تضم الرخص الفعلية المرتبطة بدور معين.

30.2.3 نقطة معلومات عن السياسة (PIP): كيان في النظام يعمل كمصدر لقيم النعوت.

31.2.3 مجموعة سياسات: مجموعة سياسات ومجموعات سياسية أخرى وخوارزمية جمع سياسات و(خيارياً) مجموعة التزامات. وقد تشكل مكونةً من مجموعة سياسات أخرى.

32.2.3 عبارة منطقية: بيان عن نعوت يمكن تقدير صحتها.

33.2.3 مورد: معطيات أو خدمة أو مكونة نظام.

34.2.3 دور: وظيفة في سياق تنظيم له دلالات تصاحبه تتعلق بالسلطة وبالمسؤولية الموكلة إلى المستعمل المخصص لهذا الدور.

35.2.3 التحكم في النفاذ القائم على الدور (RBAC): نموذج للتحكم في النفاذ إلى الموارد حيث تتحدد الأفعال المسموح بها في الموارد تبعاً للأدوار وليس لهويات الجهات المستعملة المختلفة.

36.2.3 سلطة تفعيل الدور: كيان يخصص نعوت الدور والقيم للمستعملين أو يفعِّل نعوت الدور والقيم أثناء جلسة مستعمل ما.

37.2.3 مجموعة سياسات (<PolicySet>) (RPS): معلمة <PolicySet> تجمع بين أصحاب نعت دور معين وقيمته وبين <PolicySet> الرخصة التي تحتوي على الرخص الفعلية المصاحبة لهذا الدور.

38.2.3 دور كبير: يكون الدور A في تراتبية الأدوار كبيراً نسبةً إلى الدور B إذا ورث جميع الرخص المصاحبة للدور B.

39.2.3 قاعدة: تضم هدفاً وأثراً وظرفاً وهي مكونة سياسة ما.

40.2.3 خوارزمية تجميع القواعد: الإجراء الخاص بتجميع قرارات من قواعد متعددة.

41.2.3 جهة مستعملة: كيان فاعل يمكن تسمية نعوته في عبارة.

42.2.3 هدف: مجموعة طلبات قرار تتحدد هويتها في تعاريف الموارد والجهات المستعملة والإجراءات التي يفترض تقييمها بقاعدة أو سياسة أو مجموعة سياسات.

43.2.3 توحيد النمط: طريقة "توحيد" بين عبارتي نمط. وعبارات النمط تتواءم في بنيتها. وعند ظهور متغير نمط في إحدى العبارات يتم "توحيده" كي يمثل عنصر البنية المقابلة للعبارة الأخرى أكان متغيراً آخراً أم عبارة فرعية. ويجب أن تبقى جميع تخصيصات المتغير متسقة في كلتا البنيتين. ويفشل التوحيد إن لم تتراصف العبارتان بسبب بنيتهما المختلفة أو النـــزاعات القائمة بينهما من قبيل احتياج المتغير إلى تمثيل المعلمتين "**xs:string**" و"**xs:integer**" في نفس الوقت.

4 المختصرات

تستخدم المختصرات التالية لأغراض هذه التوصية:

AA سلطة النعت *(Attribute Authority)*

ASP مزود خدمة التطبيقات *(Application Service Provider)*

CA سلطة إصدار الشهادات *(Certification Authority)*

CMP بروتوكول إدارة الشهادة *(Certificate Management Protocol)*

CRL قائمة رفض الشهادات *(Certificate Revocation List)*

ECP زبون/وكيل معزز *(Enhanced Client/Proxy)*

HTTP بروتوكول نقل النص الموسوعي *(Hypertext Transfer Protocol)*

ID معرف هوية *(IDentifier)*

IPSEC بروتوكول الأمن لبروتوكول الإنترنت *(IP SECurity protocol)*

LDAP بروتوكول مبسط للنفاذ إلى الدليل *(Lightweight Directory Access Protocol)*

PAP نقطة إدارة السياسة *(Policy Administration Point)*

PDP نقطة قرار السياسة *(Policy Decision Point)*

PEP نقطة تنفيذ السياسة *(Policy Enforcement Point)*

PIP نقطة معلومات السياسة *(Policy Information Point)*

PKI بنية تحتية لمفتاح عمومي *(Public-Key Infrastructure)*

POP إثبات الملكية *(Proof of Possession)*

PPS الرخصة <Policy Set> *(Permission <Policy Set>)*

RA سلطة التسجيل *(Registration Authority)*

RBAC التحكم في النفاذ القائم على الدور *(Role Based Access Control)*

RPS الدور <PolicySet> *(Role <PolicySet>)*

RSA ريفست، شامير، أدلمان (خوارزمية المفتاح العمومي) *((Rivest, Shamir, Adleman (public key algorithm)*

SAML لغة وسم زعم الأمن *(Security Assertion Markup Language)*

SP مزود الخدمة *(Service Provider)*

SSO توقيع وحيد *(Single Sign On)*

TLS أمن طبقة النقل *(Transport Layer Security)*

URI معرّف هوية عالمي للمورد *(Uniform Resource Identifier)*

URN اسم نظامي للمورد *(Uniform Resource Name)*

XML لغة وسم موسعة *(eXtensible Markup Language)*

XPath لغة مسير *(XML Path Language XML)*

XSLT لغة الأسلوب الموسعة *(eXtensible Stylesheet Language)*

5 اصطلاحات

تستخدم هذه التوصية الكلمات الأساسية "يجب" و"يجب ألاّ" و"متطلب" وصيغة المضارع و"ينبغي" و"ينبغي ألاّ" و"يوصى به" و"يجوز" و"خياري". وينبغي فهم هذه المصطلحات في هذه التوصية تبعاً لوصفها الوارد في المعيار RFC 2119.

وتعني الجملة "معياري لكنه خياري" في هذه التوصية أن الوظائف الموصوفة خيارية في التطبيقات XACML وإذا كانت الوظائف المزعومة المطابقة تتوفر وفقاً لهذه المواصفة فإنها تعمل حسب الطريقة الوارد وصفها.

ينبغي لدى وصف قواعد التركيب، استبدال العناصر في الرمزين ("<" ,">") بالقيم المناسبة، أما المعقوفتين ("[" ,"]") فتضمان عناصر خيارية، والعناصر بين مزدوجتين هي مكونات حرفية. ويدل الرمز "*" على أن العنصر المشار إليه قد لا يظهر أو يظهر مرة واحدة أو أكثر.

6 لمحة عامة

دفعت "الاقتصادات الكبيرة" مصنعي القواعد الحاسوبية إلى تطوير منتجات ذات وظائف عامة جداً يمكن استخدامها في أوسع مدى ممكن من الحالات. وما أن يكشف النقاب عن هذه المنتجات حتى تزود بأكبر امتياز ممكن للنفاذ إلى المعطيات وتنفيذ البرمجيات بحيث يمكن استعمالها في أكبر قدر ممكن من بيئات التطبيق، بما فيها تلك التي تستخدم سياسات الأمن الأكثر تساهلاً. أما في أكثر الحالات شيوعاً لسياسات الأمن الصارمة نسبياً فإنه يجب الحد من امتيازات الملازمة للقواعد من خلال عمليات التشكيل.

ولسياسة الأمن في منشأة كبيرة عناصر عديدة ونقاط تنفيذ كثيرة. وتتم إدارة عناصر السياسة في دائرة أنظمة المعلومات وباللجوء إلى موارد بشرية وفي الدائرة القانونية والدائرة المالية. ويمكن تنفيذ السياسة من خلال الشبكة الخارجية والبريد الإلكتروني والشبكات المحلية وأنظمة النفاذ عن بعد؛ وهي قواعد تنفذ بطبيعتها سياسة أمن متساهلة. وتكمن الممارسة الشائعة في إدارة تشكيلة كل نقطة تنفيذ على حدة بهدف تنفيذ سياسة الأمن على أدق وجه ممكن. وبناءً على ذلك فإن تعديل سياسة الأمن اقتراح باهظ التكاليف وغير موثوق. كما أنه يتعذر افتراضاً تكوين رؤية متكاملة للحراسة الفعلية في كامل المنشأة من أجل تفعيل سياسة الأمن وفي الوقت ذاته يتزايد ضغط المستهلكين وأصحاب الأسهم والمنظمين على إدارة المنشأة كي تبرهن عن اتباعها لأفضل الممارسات في حماية معلومات المنشأة وزبائنها.

ولهذه الأسباب تبرز الحاجة الملحة إلى لغة مشتركة في صياغة سياسة الأمن. وتتيح لغة السياسة المشتركة للمنشأة إذا ما طبقتها إدارة تفعيل جميع عناصر سياستها الأمنية في جميع مكونات أنظمة معلوماتها. وقد تضم إدارة سياسة الأمن بعض الخطوات التالية أو جميعها: الكتابة والمراجعة والاختبار والموافقة والإصدار والجمع والتحليل والتعديل والسحب والاستعادة وتفعيل السياسة.

7 أساس اللغة XACML

تضع هذه الفقرة أسس اللغة XACML بما فيها متطلبات السياسة العامة والنماذج والسياق العام وقواعد تركيب السياسة، وتقدم بعض الأمثلة لها.

1.7 الخلفية

ترد هذه الفقرة على سبيل الإعلام.

واللغة XML خيار طبيعي لأساس اللغة المشتركة لسياسة الأمن، بسبب سهولة إمكانية توسيع قواعد تركيبها ودلالاتها كي تلبي المتطلبات الفريدة لتطبيق ما وبسبب الدعم الواسع الذي تلقاه من جميع المصنعين الرئيسيين للأجهزة والأدوات.

1.1.7 المتطلبات

المتطلبات الأساسية للغة السياسة الخاصة بالتعبير عن سياسة أمن نظام معلومات هي توفير ما يلي:

- طريقة جمع قواعد وسياسات متفرقة في مجموعة سياسة واحدة تنطبق على طلب قرار محدد.
- طريقة تعريف مرن للإجراء يمكن من خلاله جمع القواعد والسياسات.
- طريقة التعامل مع جهات مستعملة متعددة تعمل في مجالات مختلفة.
- طريقة لإصدار قرارات الترخيص استناداً إلى نعوت الجهة المستعملة والمرود.
- طريقة لمعالجة النعوت ذات القيم المتعددة.
- طريقة لإصدار قرارات الترخيص استناداً على محتويات مورد المعلومات.
- مجموعة مؤثرات منطقية ورياضية بشأن نعوت الجهة المستعملة والمورد والبيئة.
- طريقة لمعالجة مجموعة موزعة من مكونات السياسة بغض النظر عن طريقة تحديد موقع مكونات السياسة واستعادتها واستيقافها.
- طريقة سريعة لتحديد هوية السياسة التي تنطبق على إجراء معين استناداً إلى قيم نعوت الجهات المستعملة والموارد والإجراءات.
- طبقة تجريد تعزل كاتب السياسة عن تفاصيل بيئة التطبيق.
- طريقة تحديد مجموعة إجراءات يجب القيام بها بالترافق مع تفعيل السياسة.

والبواعث الكامنة وراء اللغة XACML هي التعبير عن الأفكار الراسخة في مجال سياسة التحكم في النفاذ التي تستخدم لغة توسيع اللغة XML. وتناقش الفقرات التالية الحلول XACML لكل من المتطلبات الآنفة الذكر.

2.1.7 جمع القواعد والسياسات

تتكون السياسة الكاملة المطبقة على طلب قرار خاص من عدد من القواعد والسياسات. على سبيل المثال في تطبيق ذي خصوصية شخصية، قد يحدد مالك المعلومات الشخصية بعض جوانب سياسة الإفشاء بينما تحدد المنشأة التي تقوم بحراسة المعلومات بعض الجوانب الأخرى. ومن أجل اتخاذ قرار الترخيص، يجب التمكن من جمع سياستين منفصلتين بهدف تشكيل سياسة واحدة يمكن تطبيقها على الطلب.

وتحدد اللغة XACML ثلاثة عناصر سياسية عالية السوية هي: <Rule> (قاعدة) و<Policy> (سياسة) و<PolicySet> (مجموعة سياسات). ويضم العنصر <Rule> تعبيراً بولانياً يمكن تقييمه على حدة، لكنه لا يفترض أن يتم النفاذ إليه بمعزل عن النقطة PDP. وبذلك فإنه لا يشكل بمفرده أساساً لقرار الترخيص، ولا يتواجد بمفرده إلا ضمن نقطة XACML PAP حيث يمكنه تشكيل وحدة أساسية للإدارة ويمكن استعماله من جديد في سياسات متعددة.

ويضم العنصر <Policy> مجموعة عناصر <Rule> ويحدد إجراءً لجمع نتائج تقييمها. وهو الوحدة الأساسية للسياسة التي تستخدمها النقطة PDP وهو يشكل بذلك أساس قرار الترخيص.

ويحتوي العنصر <PolicySet> على مجموعة من العناصر <Policy> أو عناصر <PolicySet> أخرى، ويحدد إجراءً يجمع نتائج تقييمها. وهو الوسيلة المعيارية لجمع السياسات المتفرقة في سياسة مجتمعة واحدة.

3.1.7 خوارزميات الجمع

تحدد اللغة SACML عدداً من خوارزميات التجميع التي يمكن للنعت RuleCombiningAlgId أو PolicyCombiningAlgId في العنصرين <Policy> أو <PolicySet> على التوالي أن تعرف هويتها. وتعرّف خوارزمية تجميع القواعد على أنه إجراء للوصول إلى قرار الترخيص استناداً إلى النتائج الإفرادية لتقييم مجموعة القواعد. وبنفس الطريقة تعرف خوارزمية جمع السياسات إجراءً للوصول إلى قرار ترخيص استناداً إلى النتائج الإفرادية لتقييم مجموعة السياسات. وتتحدد خوارزميات الجمع المعيارية للأغراض التالية:

- رفض ذو أولوية (Deny-overrides) (منتظم وغير منتظم)؛
- سماح ذو أولوية (Permit-overrides) (منتظم وغير منتظم)؛
- يطبق العنصر الأول (First-applicable)؛
- لا تطبق إلا سياسة واحدة (Only-one-applicable).

في حالة خوارزمية الرفض ذي الأولوية، إذا وجد عنصر واحد <Rule> أو <Policy> يعادل "Deny" (الرفض) عندئذٍ وبغض النظر عن نتيجة تقييم العناصر الأخرى <Rule> أو <Policy> في السياسة المطبقة، تكون نتيجة التجميع الرفض ("Deny").

وبطريقة مماثلة إذا وجدت نتيجة "Permit" (سماح) واحدة في حالة خوارزمية السماح ذي الأولوية تكون نتيجة التجميع السماح ("Permit").

وفي حالة خوارزمية الجمع "First-applicable" (يطبق العنصر الأول) تكون نتيجة التجميع هي نفس نتيجة تقييم أول عنصر <Rule> أو <Policy> في قائمة القواعد التي ينطبق هدفها على طلب القرار.

ولا تنطبق خوارزمية تجميع السياسات "Only-one-applicable" إلاّ على السياسات. وتضمن نتيجة خوارزمية التجميع هذه ألاّ تطبق إلاّ سياسة واحدة أو مجموعة سياسية واحدة تبعاً لأهدافهما. وإن لم تنطبق أي سياسة أو مجموعة سياسية تكون النتيجة "NotApplicable" (غير قابلة للتطبيق). أما في حال صلاح أكثر من سياسة أو مجموعة سياسات واحدة فتكون النتيجة "Indeterminate" (غير محددة). وعند وجود سياسة أو مجموعة سياسية واحدة فقط تكون نتيجة خوارزمية التجميع هي نتيجة تقييم السياسة أو مجموعة السياسات الوحيدة القابلة للتطبيق.

وقد تتخذ السياسات ومجموعات السياسات معلمات تغيّر من سلوك خوارزميات التجميع. غير أن أياً من خوارزميات التجميع المعيارية لا تتأثر بالمعلمات.

ويجوز لمستعملي هذه التوصية خوارزميات تجميع خاصة بهم إن اقتضت الحاجة.

4.1.7 جهات مستعملة متعددة

غالباً ما تفرض سياسات التحكم في النفاذ شروطاً على الإجراءات في أكثر من جهة مستعملة. فالسياسة التي تتحكم في تنفيذ العمليات المالية الكبيرة مثلاً قد تتطلب موافقة عدة أفراد يعملون بمقدرات مختلفة. لذلك فإن اللغة XACML تقر باحتمال وجود عدة جهات مستعملة تتصل بطلب القرار. وثمة نعت اسمه "subject-category" (فئة الجهة المستعملة) يستعمل للتمييز بين هذه الجهات العاملة بمقدرات مختلفة. وهناك بعض القيم المعيارية لهذا النعت، ويمكن للمستعملين تحديد قيم إضافية.

5.1.7 السياسات القائمة على نعوت الجهات المستعملة والموارد

ثمة متطلب عام آخر هو أن يقوم قرار الترخيص على أساس بعض خصائص الجهة المستعملة فضلاً عن هويته. وربما يكون التطبيق الأكثر شيوعاً لهذه الفكرة هو دور الجهة. وتقدم اللغة XACML تسهيلات تدعم هذا النهج. ويمكن تحديد نعوت الجهات التي يتضمنها سياق الطلب من خلال العنصر <SubjectAttributeDesignator>. ويضم هذا العنصر اسم المورد النظامي (URN) الذي يحدد النعت. كما يمكن

للعنصر <AttributeSelector> أن يضم عبارة XPath في سياق الطلب من أجل تحديد قيمة نعت جهة خاصة من خلال موقعها في السياق.

وتقدم اللغة XACML طريقة معيارية للإحالة إلى النعوت التي يعرفها المعيار IETF RFC 2253. والغرض من ذلك هو تشجيع المنفذين على استعمال معرفات هوية معيارية لبعض النعوت المشتركة للجهة المستعملة.

وهناك متطلب مشترك آخر يقضي بوضع قرار الترخيص على أساس بعض خصائص المورد غير المتعلقة بهويته. وتوفر اللغة XACML التسهيلات لهذا النهج. ويمكن تحديد نعوت المورد باستعمال العنصر <ResourceAttributeDesignator>. ويضم هذا العنصر اسم URN يعرف هوية النعت. ومن ناحية أخرى يضم العنصر <AttributeSelector> تعبيراً من اللغة XPath في سياق الطلب من أجل تعرف هوية قيمة نعت مورد معين من خلال موقعه في السياق.

6.1.7 نعوت متعددة القيم

تقدم تقنيات نقل النعوت الأكثر انتشاراً (LDAP، XPath، SAML وغيرها) قيماً متعددة للنعت الواحد. وبالتالي عندما تستعيد النقطة XACML PDP قيمة نعت معين فإن النتيجة تضم عدة قيم. وتسمى مجموعة القيم هذه سلّة. وتختلف سلة مجموعة قد تضم قيماً مضاعفة عن تلك التي لا تضم هذه القيم. وتظهر أخطاء في هذه الحالة أحياناً. وأحياناً تستوفى شروط قاعدة اللغة XACML عندما تطابق أي قيمة للنعت المعيار المحدد في القاعدة.

وتقدم اللغة XACML مجموعة من الوظائف تتيح لكاتب السياسة أن يعبر بوضوح تام عن كيفية معالجة النقطة PDP لحالة قيم النعت المتعددة وهي وظائف "المرتبة العليا".

7.1.7 السياسات القائمة على محتويات الموارد

من المطلوب في العديد من التطبيقات أن يقوم قرار الترخيص على أساس المعطيات الواردة في مورد المعلومات التي يطلب النفاذ إليه. فالمكونة العامة لسياسة الخصوصية مثلاً تنطوي على السماح لشخص ما أن يقرأ التسجيلات التي يشكل موضوعها. ويجب أن تضم السياسة المقابلة إحالة لهذه الجهة المستعملة المحددة في مورد المعلومات ذاته.

وتوفر اللغة XACML تسهيلات للقيام بذلك عندما يكون بالإمكان تقديم مورد المعلومات كوثيقة XML. وقد يضم العنصر <AttributeSelector> عبارة XPath في سياق الطلب من أجل تعرف هوية المعطيات في مورد المعلومات لاستعماله في تقدير السياسة.

8.1.7 المؤثرات

تعمل سياسات أمن المعلومات على نعوت الجهات المستعملة والموارد والإجراءات والبيئة بهدف الوصول إلى قرار الترخيص. وقد تتطلب نعوت أنماط كثيرة أثناء عملية الوصول إلى قرار الترخيص عمليات مقارنة وحساب. على سبيل المثال يمكن حساب الائتمان المتاح لشخص ما في التطبيقات المالية بإضافة الحد الأقصى المسموح به من الائتمان إلى رصيد حسابه. ويمكن عندئذ مقارنة النتيجة بقيمة العملية وينجم عن هذه الحالة ضرورة إجراء عمليات حسابية لنعوت الجهة المستعملة (رصيد الحساب والحد الأقصى للائتمان المتاح لها) والمورد (قيمة العملية).

وغالباً ما تحدد سياسة ما مجموعة أدوار مسموحة لأداء إجراء ما. وتنطوي العمليات الضرورية على التحقق من وجود تقاطع غير فارغ بين مجموعة الأدوار التي تشغلها الجهة المستعملة ومجموعة الأدوار التي تحددها السياسة. مما يفسر الحاجة إلى عمليات متكاملة.

وتضم اللغة XACML عدداً من الوظائف المدمجة وطريقة لإضافة وظائف غير معيارية. وتصفف هذه الوظائف بحيث تؤلف تعابير<Apply> معقدة اعتباطية. ويتم ذلك باستعمال العنصر <Apply> (تطبيق). وللعنصر <Apply> نعت XML اسمه FunctionId (معرف هوية الوظيفة) يحدد الوظيفة الواجب تطبيقها على محتويات العنصر. وتتحدد كل وظيفة معيارية من أجل تركيبة معينة من أنماط المعطيات والقيم ويتحدد أيضاً نمط معطيات رجوعها. وبالتالي يمكن التحقق من اتساق أنماط معطيات السياسة في الوقت الذي توضع فيه هذه السياسة أو تحلل. كما يمكن التحقق من أنماط قيم المعطيات المقدمة في سياق الطلب بمقارنتها مع القيم المقبولة في السياسة من أجل ضمان النتيجة المتوقعة.

وإضافة إلى المؤثرات الحسابية في القيم الرقمية والإجمالية، تتحدد مؤثرات خاصة بقيم التاريخ والزمن والمدة.

كما تتحدد أيضاً مؤثرات العلاقات (تساوي ومقارنة) لعدد من أنماط المعطيات، ومنها أشكال الاسم والسلسلات المحددة في المعيار IETF RFC 822 والتوصية X.500 والمعرفات URI وغيرها.

ويجدر بالذكر أيضاً مؤثرات أنماط المعطيات البولانية التي تسمح بالجمع المنطقي لمقولات حسب القاعدة. فعلى سبيل المثال، قد تضم قاعدة ما تصريحاً يقضي بالسماح بالنفاذ أثناء ساعات العمل ومن مطراف قائم في مكان العمل.

9.1.7 توزيع السياسة

يمكن في نظام موزّع وضع بيانات السياسات المتفرقة من قبل عدة أطراف وأن تُفعل في عدة نقاط تفعيل. ويسمح هذا النهج إضافة إلى تسهيل جمع وتركيب مكونات سياسات مستقلة، بتحديث السياسات حسب الاقتضاء. وقد توزع بيانات السياسة XACML في أي طريقة من الطرق. لكن اللغة XACML لا تصف أي طريقة معيارية للقيام بذلك. ويفترض بغض النظر عن وسائل التوزيع، أن تؤكد النقاط PDP أن السياسة قابلة للتطبيق على طلب القرار الذي هي بصدد معالجته وذلك من خلال تفحص عنصر السياسة <Target> (الهدف).

ويمكن إرفاق العناصر <Policy> بموارد المعلومات التي تطبق عليها. كما يمكن الإبقاء على العناصر <Policy> في موقع واحد أو أكثر من المواقع التي أخذت منها بالتقييم. وفي مثل هذه الحالة يحال إلى السياسة التي يمكن تطبيقها باستعمال معرّف هوية أو دليل موقع وثيق الارتباط بمورد المعلومات.

10.1.7 فهرسة السياسات

من أجل تقييم فعّال وإدارة سهلة، يمكن التعبير عن سياسة الأمن العامة النافذة في منشأة ما من خلال عدة مكونات سياسية متفرقة. ومن الضروري في هذه الحالة تحديد بيانات السياسة القابلة للتطبيق واستعادتها والتحقق من أنها السياسة الصحيحة للإجراء المطلوب قبل البدء بتقييمها. وهذا هو الغرض من العنصر <Target> في اللغة XACML.

وثمة نهجان لذلك هما:

1) تخزين بيانات السياسة في قاعدة معطيات. وينبغي في هذه الحالة أن تشكل النقطة PDP قاعدة معطيات للتمكن من ضبط استعادة تلك السياسات التي تطبق على مجموعة طلبات القرار والتي يتوقع أن تفي بالغرض. علاوة على ذلك، ينبغي أن تقيم النقطة PDP عنصر <Target> في بيانات السياسة أو مجموعة السياسات المستعادة.
2) تحميل النقطة PDP مع جميع السياسات المتيسرة وتقييم العناصر <Target> التابعة لها في سياق طلب قرار معين بهدف تعرف هوية السياسات ومجموعات السياسات التي يمكن تطبيقها على ذلك الطلب.

11.1.7 الطبقة التجريدية

تتخذ النقاط PEP أشكال عديدة؛ كأن تكون جزءاً من بوابة نفاذ بعيدة أو جزءاً من مخدم شبكة ويب أو جزءاً من وكيل مستعمل لبريد إلكتروني مثلاً. ومن غير العملي افتراض أن تقوم جميع النقاط PEP في منشأة ما حالياً أو لاحقاً بإصدار طلبات قرار إلى النقطة PDP في نسق مشترك. ومع ذلك قد يكون من الضروري تنفيذ سياسة ما في عدة نقاط PEP. ومن غير المجدي إلزام كاتب السياسة على كتابة نفس السياسة في عدة طرق مختلفة بهدف تلبية متطلبات النسق في كل نقطة PEP. ويمكن وضع النعوت المتماثلة في أنماط تغليف مختلفة (مثال: شهادات النعوت X.509 وتأكيد النعوت SAML) وغيرها). وتنتج عن ذلك حاجة إلى شكل نظامي للطلبات وللاستجابات التي تعالجها النقطة XACML DPD. وهذا الشكل النظامي اسمه السياق XACML. وتتحدد قاعدة تركيبه في المخطط XML.

ويجوز بالطبع للنقاط PEP المطابقة للغة XACML أن تصدر الطلبات وتستقبل الاستجابات في شكل السياق XACML. غير أنه يُطلب في غياب هذه الحالة، وجود مرحلة وسيطة من أجل التحويل من نسق الطلب/الاستجابة المتضمنين في النقطة PEP ونسق السياق XACML الذي تتضمنه النقطة PDP.

وتكمن أهمية هذا النهج في إمكانية كتابة تلك السياسات وتحليلها بمعزل عن البيئة المحددة التي ستعمل فيها.

وفي الحالة التي يكون فيها نسق الطلب/الاستجابة الأصلي محدداً في المخطط XML (مثل نقطة مطابقة للغة SAML)، يتحدد التحويل من النسق الأصلي إلى نسق السياق XACML في الشكل تحويل اللغة ورقة الأسلوب الموسعة.

وبصورة مماثلة عندما يكون المورد الذي يطلب إليه النفاذ وثيقة XML، قد يكون المورد ذاته مدرجاً في سياق الطلب أو يحيل إليه هذا السياق. وبذلك ومن خلال استعمال التعابير XPath في السياسة يمكن إدراج القيم الموجودة في المورد في تقييم السياسة.

12.1.7 الإجراءات التي ترافق تنفيذ السياسة

تحدد السياسات في العديد من التطبيقات الإجراءات التي يجب القيام بها إما بدلاً من الإجراءات التي يمكن القيام بها وإما إضافة إليها. وتتيح اللغة XACML مرافق من أجل الإجراءات الواجب أداؤها مع تقييم السياسة في العنصر <Obligations> (التزامات). ولا توجد تعاريف معيارية لهذه الإجراءات في النسخة 2.0 اللغة XACML. وبالتالي لا بد من اتفاق ثنائي بين النقطتين PAP وPEP من شأنه تفعيل سياساتهما بهدف تحقيق تفسير سليم لها. ويتعين أن ترفض النقاط PEP المطابقة للنسخة 2.0 من اللغة XACML النفاذ، إلا إذا فهمت جميع العناصر <Obligations> المصاحبة للسياسة المطبقة وكانت قادرة على الوفاء بها. وتعاد العناصر <Obligations> إلى النقطة PEP لتفعيلها.

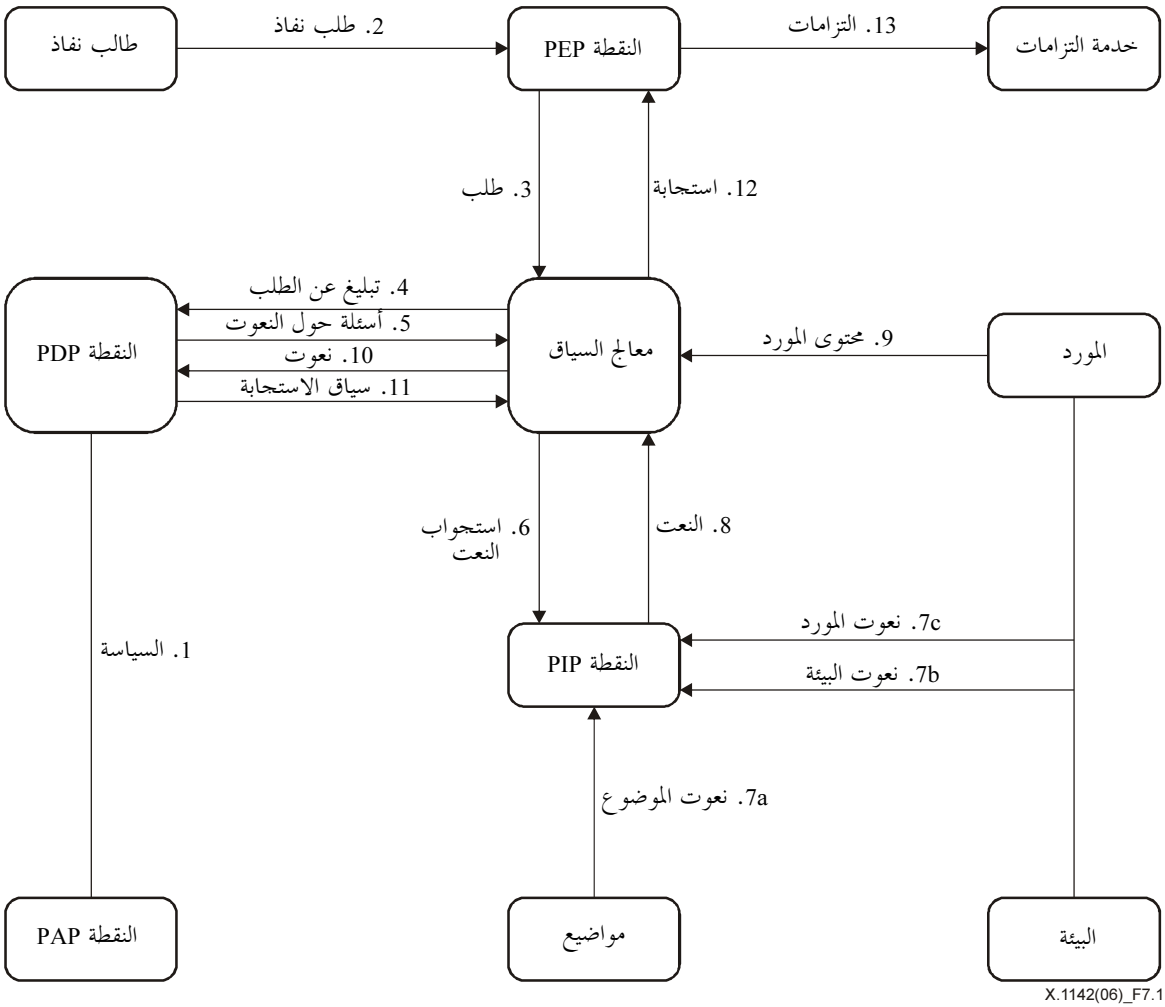
2.7 نماذج اللغة XACML

ترد هذه الفقرة على سبيل الإعلام.

ويرد وصف نموذج تدفق المعطيات ونموذج اللغة XACML في الفقرات التالية.

1.2.7 نموذج تدفق المعطيات

تظهر العناصر الرئيسية لمجال اللغة XACML في مخطط تدفق المعطيات المبين في الشكل 1-7.



الشكل X.1142/1-7 – مخطط تدفق المعطيات

ملاحظة - يمكن تسهيل بعض تدفقات المعطيات المبينة في المخطط باستعمال فهرس فمثلاً يمكن تسهيل الاتصالات بين معالج السياق والنقطة PIP أو بين النقطة PDP والنقطة PAP باللجوء إلى فهرس. وليس الغرض من هذه التوصية وضع قيود على موقع أي من هذه الفهارس أو وضع مواصفة لبروتوكول اتصالات خاص لأي من تدفقات المعطيات.

ويعمل هذا النموذج حسب المراحل التالية:

1) تضع النقاط PAP السياسات ومجموعات السياسات وتتيحهم في النقطة PDP. وتمثل هذه السياسات أو مجموعات السياسات السياسة الكاملة لخدمة هدف محدد.
2) يرسل طالب النفاذ طلباً للنفاذ إلى النقطة PEP.
3) ترسل النقطة PEP طلب النفاذ إلى معالج السياق في نسقه الأصلي وخيارياً مع نعوت الجهة المستعملة والمورد والإجراء والبيئة.
4) يعد معالج السياق سياق طلب XACML ويرسله إلى النقطة PDP.
5) تطلب النقطة PDP كل النعوت الإضافية للجهة المستعملة والمورد والإجراء والبيئة من معالج السياق.
6) يطلب معالج السياق النعوت من النقطة PIP.
7) تحصل النقطة PIP على النعوت المطلوبة.
8) تعيد النقطة PIP النعوت المطلوبة إلى معالج السياق.

9) يدرج معالج السياق، خيارياً، المورد في السياق.

10) يرسل معالج السياق النعوت المطلوبة و(خيارياً) المورد إلى النقطة PDP. وتقيّم النقطة PDP السياسية.

11) تعيد النقطة PDP سياق الاستجابة (بما فيها قرار الترخيص) إلى معالج السياق.

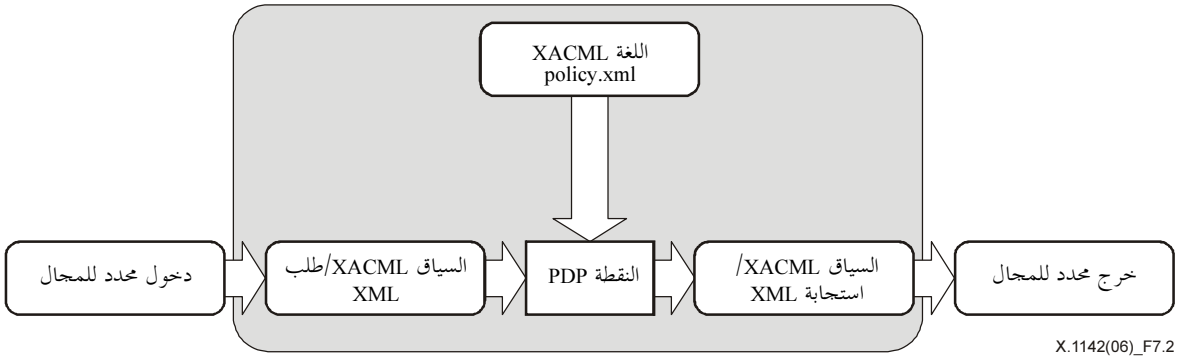
12) يحوّل معالج السياق سياق الاستجابة إلى نسق الاستجابة الأصلي للنقطة PEP. ويعيد الاستجابة إلى النقطة PEP.

13) تفي النقطة PEP بالإلتزامات.

14) إذا سمح بالنفاذ تسمح النقطة PEP بالنفاذ إلى المورد، وإلاّ فإنها ترفضه (لا تظهر هذه المرحلة في الشكل).

3.7 السياق XACML

صممت اللغة XACML لتتمشى مع بيئات تطبيقات مختلفة. ويعزل أساس اللغة عن بيئة التطبيق من خلال السياق XACML كما يبين الشكل 7-2 الذي يظهر النطاق XACML في المنطقة الظليلة. ويعرف السياق XACML في المخطط XML الذي يصف تمثيلاً نظامياً بدخل وخرج النقطة PDP. وقد تتخذ النعوت التي تحيل إليها إحدى وحدات السياسة XACML شكل تعابير XPath في السياق أو شكل مؤشرات نعوت تعرف النعت من خلال الجهة المستعملة أو المورد أو الإجراء أو البيئة ومعرف هويته ونمط معطياته و(خيارياً) الجهة التي أصدرتها. ويجب أن يحوّل التنفيذ بين تمثيل النعت في بيئة التطبيق (مثل SAML) وتمثيل النعت في السياق XACML. ولا تندرج كيفية القيام بهذه العمليات ضمن نطاق هذه التوصية. ويتم هذا التحويل في بعض الحالات من قبيل اللغة SMAL بطريقة مؤتمتة من خلال استعمال التحويل XSLT (انظر المعيار W3C XSLT:1999).



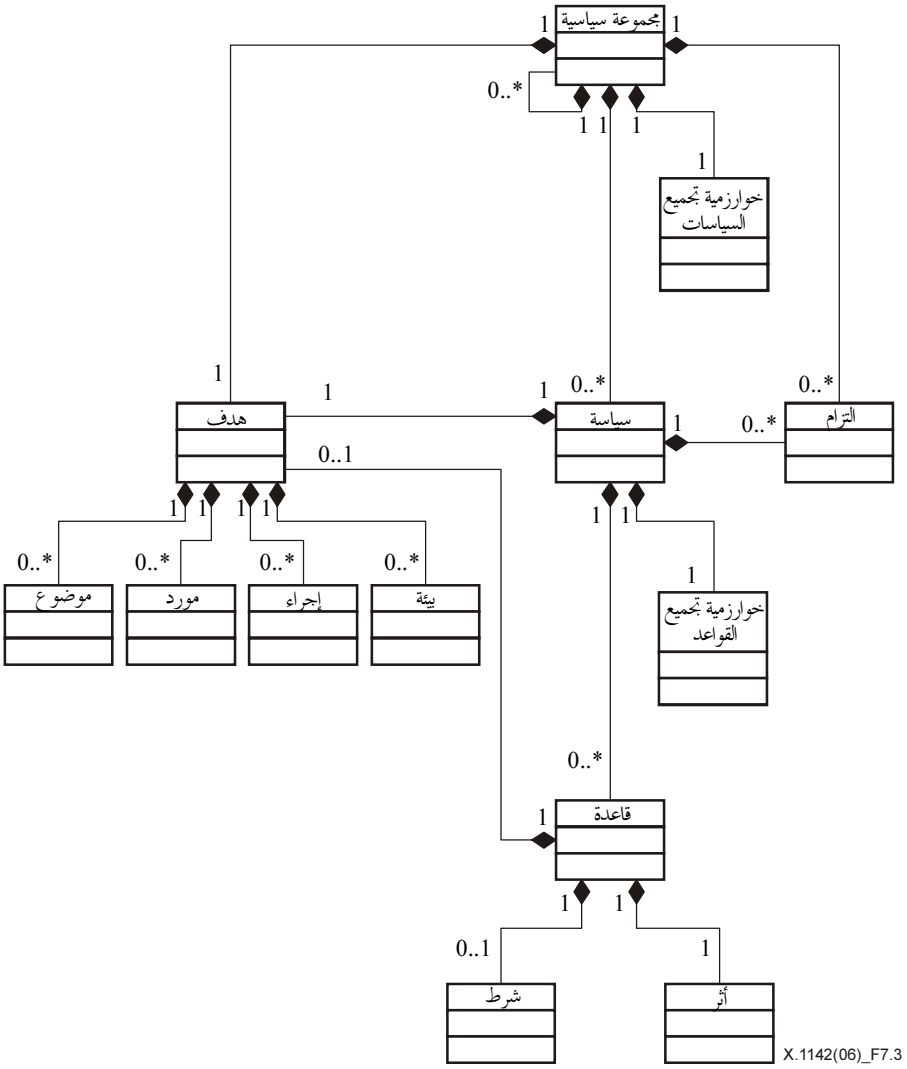
الشكل X.1142/2-7 – السياق XACML

النقطة PDP غير ملزمة بالعمل مباشرة في تمثيل سياسة ما باللغة XACML. وقد تعمل مباشرة في تمثيل بديل.

1.3.7 نموذج لغة السياسة

يظهر نموذج لغة السياسة في الشكل 7-3 ومكونات النموذج الرئيسية هي التالية:

- القواعد؛
- السياسة؛
- مجموعة السياسات.



الشكل X.1142/3-7 – نموذج لغة السياسة

1.1.3.7 القاعدة

القاعدة هي أصغر وحدة في السياسة. ولا توجد بمفردها إلا ضمن أحد العناصر الرئيسية للمجال XACML. ويستدعي تبادل القواعد إدراجها في سياسة ما. وتقيم القاعدة على أساس محتوياتها. أما مكوناتها الرئيسية فهي:

- الهدف؛
- الأثر؛
- الشرط.

1.1.1.3.7 هدف القاعدة

يعرف الهدف مجموعات:

- الموارد؛
- الجهات المستعملة؛
- الإجراءات؛
- البيئة،

والتي يُفترض تطبيق القاعدة عليها. ويضيف العنصر <Condition> (الظرف) تفاصيل إلى إمكانية التطبيق التي يضعها الهدف. وإذا خُصصت القاعدة للتطبيق على جميع كيانات نمط معطيات معين حذف الكيان المقابل من الهدف. وتتحقق النقطة XACML PDP أن التقابلات التي يحددها الهدف مستوفاة في نعوت الجهات المستعملة والموارد والإجراءات والبيئة ضمن السياق المطلوب. وتعاريف الهدف منفصلة بحيث يمكن للنقطة PDP تحديد القواعد القابلة للتطبيق بشكل فعال.

وقد يغيب العنصر <Target> من <Rule>. ويكون هدف العنصر <Rule> عندئذٍ هو نفس هدف العنصر <Policy> الأصل.

وتنتظم بعض أشكال اسم الجهة المستعملة وأشكال اسم المورد وبعض أنماط المورد في بنية داخلية. فشكل اسم الدليل X.500 وشكل الاسم IETF RFC 822 مثلاً لهما بنية الشكل النظامي لاسم الجهة المستعملة، بينما لا يعتمد رقم الحساب عموماً بنية واضحة. وأسماء مسارات نظام الملفات UNIX والمعرفات URI أمثلة لأشكال اسم المورد ذات البنية النظامية. ووثائق اللغة XML مثال لمورد ذي بنية نظامية.

وعموماً، يكون أيضاً اسم عقدة ما (غير عقدة الورقة) في شكل اسم منتظم البنية حالة نظامية لشكل الاسم. وبذلك مثلاً يكون الاسم "med.example.com" حسب المعيار IETF RFC 822 اسماً نظامياً لمعيار IETF RFC 822 يعرّف مجموعة العناوين الإلكترونية الموجودة في مخدم البريد الإلكتروني med.example.com. والقيمة XPath/XPointer يعبر عنها على النحو -//xacml-context:Request/xacml context:Resource/xacml-context:ResourceContent/md:record/md:patient/ قيمة نظامية XPath/XPointer تعرف مجموعة عقد في الوثيقة XML.

وهنا يطرح السؤال: كيف ينبغي أن تفسر النقطة PDP اسماً يعرف مجموعة جهات مستعملة أو موارد إذا ما ظهر في سياق سياسة أو في سياق طلب؟ وهل الغرض منه مجرد تمثيل العقدة المعرفة صراحة في الاسم أو تمثيل التفرع الفرعي التابع لتلك العقدة؟

ولا يوجد في حالة الجهات المستعملة أي كيان فعلي يقابل عقدة من هذا القبيل. وهكذا تحيل أسماء هذا النمط دائماً إلى مجموعة الجهات التابعة إلى العقدة المحددة في بنية الاسم. وبناءً على ذلك ينبغي عدم استعمال أسماء الجهات دون تفرعات ورقة في وظائف المتساوي بل في وظائف التقابل، مثل "urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match" وليس "urn:oasis:names:tc:xacml:1.0:function:rfc822Name-equal".

2.1.1.3.7 التأثير

يدل تأثير القاعدة على النتائج التي يتوقعها واضع القواعد بالتقييم "صح" للقاعدة. والقيمتان المتاحتان هما "مسموح" ("Permit") و"مرفوض" ("Deny").

3.1.1.3.7 الظرف

يمثل الظرف تعابير بولانية تتيح تفاصيل أدق لإمكانية تطبيق القاعدة تتجاوز المعطيات التي يفترضها الهدف. ولذا يكون غيابها ممكناً.

2.1.3.7 السياسة

يمكن استناداً إلى نموذج تدفق المعطيات ملاحظة أنه لا يتم تبادل القواعد بين كيانات النظام. ولذلك تجمع النقطة PAP القواعد ضمن سياسة ما. وتشتمل السياسة على أربع مكونات رئيسية هي:

- الهدف؛
- معرف هوية خوارزمية جمع القواعد؛
- مجموعة القواعد؛
- الالتزامات.

1.2.1.3.7 هدف السياسة

يحتوي العنصر <PolicySet> أو <Policy> أو <Rule> في اللغة XACML على عنصر <Target> يحدد مجموعة الجهات المستعملة والموارد والإجراءات والبيئات التي ينطبق عليها. وقد يصرح مؤلف <PolicySet> أو <Policy> عن العنصر <Target> التابع للعنصر <PolicySet> أو <Policy>، أو يحسب هذا العنصر استناداً إلى العناصر <Target> الموجودة في العناصر <Policy> و<Rule>.

ولا تعرف اللغة XACML كيان نظام يحسب العنصر <Target> بهذه الطريقة، لكن هناك طريقتين منطقيتين يمكن استخدامهما. وفي الطريقة الأولى، يحسب العنصر <Target> للمكونة <PolicySet> أو <Policy> الخارجية ("المكونة الخارجية") على أنه مجموع العناصر <Target> للعناصر <PolicySet> أو <Policy> أو <Rule> المحال إليها ("المكونات الداخلية"). أما في الطريقة الثانية فيحسب العنصر <Target> للمكونة الخارجية على أنه تقاطع جميع العناصر <Target> للمكونات الداخلية. ونتائج التقييم في الحالتين شديدة التفاوت: ففي الحالة الأولى ينطبق عنصر <Target> للمكونة الخارجية على كل طلب قرار يتمشى مع عنصر <Target> مكونة داخلية واحدة على الأقل؛ أما في الحالة الثانية، فلا ينطبق العنصر <Target> للمكونة الخارجية إلاّ مع طلبات القرار التي تتمشى مع عناصر <Target> في جميع المكونات الداخلية. وتجدر الإشارة إلى أن تقاطع مجموعة من العناصر <Target> يبدو غير عملي إلاّ إذا كان نموذج معطيات الهدف بسيطاً نسبياً.

وفي الحالات التي يفصح فيها واضع السياسة عن هدف <السياسة> يجوز لكل مكونة عناصر <القاعدة> في <السياسة> التي تضم نفس عنصر <الهدف> كعنصر <سياسة> أن تحذف العنصر <هدف>. وترث هذه العناصر <قاعدة> <هدف> <السياسة> التي تتضمنها.

2.2.1.3.7 خوارزمية تجميع القواعد

تحدد خوارزمية تجميع القواعد الإجراء الذي يجمِّع نتائج تقييم قواعد المكونات عند تقييم السياسة، أي أن قيمة القرار (Decision) التي تحددها النقطة PDP في سياق الاستجابة هي قيمة السياسة كما تحددها خوارزمية تجميع القواعد. وقد تحتوي سياسة ما على معلمات تجميع تؤثر على عمل خوارزمية تجميع القواعد.

3.2.1.3.7 الالتزامات

يجوز لواضع السياسة أن يضيف بعض الالتزامات.

وعندما تقيم نقطة PDP سياسة ما تتضمن التزامات فإنها تعيد بعض هذه الالتزامات إلى النقطة PEP في سياق الاستجابة.

3.1.3.7 مجموعة السياسات

وتضم مجموعة السياسات أربع مكونات رئيسية هي:

- الهدف؛
- معرف هوية خوارزمية تجميع السياسات؛
- مجموعة السياسات؛
- الالتزامات.

1.3.1.3.7 خوارزمية تجميع السياسات

تحدد خوارزمية تجميع السياسات الإجراء الذي يجمّع نتائج تقييم سياسات المكونات عند تقييم مجموعة السياسات؛ أي أن قيمة القرار (Decision) التي تحددها النقطة PDP في سياق الاستجابة هي نتيجة تقييم مجموعة السياسات كما تعرفها خوارزمية تجميع السياسات. وقد تحتوي مجموعة السياسات على معلمات تجميع تؤثر على عمل خوارزمية تجميع السياسات.

2.3.1.3.7 الالتزامات

يجوز لواضع مجموعة السياسات أن يضيف التزامات إلى تلك التي تتضمنها سياسات المكونة ومجموعات السياسات.

وعندما تقيّم النقطة PDP مجموعة سياسات تضم التزامات فإنها تعيد بعض هذه الالتزامات إلى النقطة PEP في سياق استجابتها.

4.7 قواعد تركيب السياسة

بعض أجزاء من المخططات الواردة في الفقرات التالية غير معيارية.

1.4.7 العنصر <PolicySet> <مجموعة سياسات>

العنصر <PolicySet> هو عنصر من السوية العليا في مخطط سياسة اللغة XACML. وهو تراكم مجموعات سياسية وسياسات أخرى. ويمكن إدراج مجموعات سياسية في عنصر <PolicySet> عام إما مباشرة باستعمال عنصر <PolicySet> أو بطريقة غير مباشرة باستعمال العنصر <PolicySetIdReference>. ويمكن إدراج سياسات في عنصر <PolicySet> عام إما مباشرة باستعمال العنصر <Policy> أو بطريقة غير مباشرة العنصر <PolicySetIdReference>.

ويمكن تقييم العنصر <PolicySet>؛ وفي هذه الحالة يتوجب استخدام إجراء التقييم المحدد في هذه التوصية.

وإذا ضم العنصر <PolicySet> إحالات إلى مجموعات سياسية أو سياسات أخرى على شكل URL (محدد موقع نظامي للمورد)، أمكن حل هذه الإحالات.

ويجب تجميع مجموعات السياسة والسياسات المدرجة في العنصر <PolicySet> باستخدام الخوارزمية التي يحددها النعت PolicyCombiningAlgId. وتعالج العنصر <PolicySet> تماماً كعنصر <Policy> في جميع خوارزميات تجميع السياسات.

ويحدد العنصر <Target> قابلية تطبيق العنصر <PolicySet> على مجموعة طلبات قرار. وإذا تلاءم العنصر <Target> داخل العنصر <PolicySet> مع سياق الاستجابة أمكن استخدام النقطة PDP للعنصر <PolicySet> عند اتخاذها لقرار الترخيص.

ويضم العنصر <Obligations> مجموعة من الالتزامات التي يجب أن تستوفيها النقطة PEP المرتبطة بقرار الترخيص. وإذا لم تفهم النقطة PEP أي من هذه الالتزامات أو لم تستطع الوفاء بها يجب عندئذ العمل كما لو أن النقطة PDP أعادت قيمة "رفض" قرار الترخيص.

```
<xs:element name="PolicySet" type="xacml:PolicySetType"/>
<xs:complexType name="PolicySetType">
   <xs:sequence>
         <xs:element ref="xacml:Description" minOccurs="0"/>
         <xs:element ref="xacml:PolicySetDefaults" minOccurs="0"/>
         <xs:element ref="xacml:Target"/>
         <xs:choice minOccurs="0" maxOccurs="unbounded">
               <xs:element ref="xacml:PolicySet"/>
               <xs:element ref="xacml:Policy"/>
               <xs:element ref="xacml:PolicySetIdReference"/>
               <xs:element ref="xacml:PolicyIdReference"/>
               <xs:element ref="xacml:CombinerParameters"/>
               <xs:element ref="xacml:PolicyCombinerParameters"/>
               <xs:element ref="xacml:PolicySetCombinerParameters"/>
         </xs:choice>
         <xs:element ref="xacml:Obligations" minOccurs="0"/>
   </xs:sequence>
   <xs:attribute name="PolicySetId" type="xs:anyURI" use="required"/>
   <xs:attribute name="Version" type="xacml:VersionType" default="1.0"/>
   <xs:attribute name="PolicyCombiningAlgId" type="xs:anyURI" use="required"/>
</xs:complexType>
```

العنصر <PolicySet> هو من النمط المعقد **PolicySetType**.

ويضم العنصر <PolicySet> النعوت والعناصر التالية:

- PolicySetId [إلزامي]

هو معرف مجموعة سياسية. وتكمن مسؤولية النقطة PAP في ضمان عدم وجود سياستين واضحتين للنقطة PDP تحملان نفس معرف الهوية. وقد يتحقق ذلك باتباع مخطط مسبق التحديد للاسم URN أو المعرف URI. وإذا كان معرف هوية مجموعة السياسات في شكل URL يكون عندئذٍ قابلاً للحل.

- Version [1.0 بالتغيب]

وهو رقم نسخة مجموعة السياسات.

- PolicyCombiningAlgId [إلزامي]

وهو معرف هوية خوارزمية تجميع السياسة الذي يجمّع المكونات <PolicySet> و<CombinerParameters> و<PolicyCombinerParameters> و<PolicySetCombinerParameters>.

- <Description> [خياري]

وهو وصف شكل لمجموعة السياسات

- <PolicySetDefaults> [خياري]

مجموعة من قيم التغيب المستخدمة في مجموعة السياسات. ونطاق تطبيق العنصر <PolicySetDefaults> هو مجموعة السياسات العامة.

- <Target> [إلزامي]

يحدد العنصر <Target> قابلية تطبيق مجموعة سياسات على مجموعة طلبات قرار.

وقد يفصح مستحدث <مجموعة السياسات> عن العنصر <Target> أو قد يحسب استناداً إلى العناصر <Target> التابعة للعناصر <Policy> المحال إليها إما كتقاطع وإما كمجموع.

- <PolicySet> [أي رقم]

وهي مجموعة سياسات تتضمنها هذه المجموعة من السياسات.

- <Policyt> [أي رقم]

وهي السياسة المتضمنة في مجموعة السياسات هذه.

- <PolicySetIdReference> [أي رقم]

وهي إحالة إلى مجموعة سياسات يجب أن تدرج في هذه المجموعة من السياسات وإذا كان العنصر <PolicySetIdReference> موقع URL، قد يكون عندئذٍ قابلاً للحل.

- <PolicyIdReference> [أي رقم]

وهي إحالة لمجموعة سياسات يجب أن تدرج في هذه المجموعة من السياسات. وإذا كان العنصر <PolicyIdReference> موقع URL، قد يكون قابلاً للحل.

- <Obligations> [خياري].

ويضم مجموعة العناصر <Obligations>

- <CombinerParameters> [خياري]

ويضم تتابعاً من العناصر <CombinerParameters>.

- <PolicyCombinerParameters> [خياري]

ويضم تتابعاً من العناصر <CombinerParameter> المصاحبة لعنصر <Policy> أو <PolicyIdReference> داخل <PolicySet>.

- <PolicySetCombinerParameters> [خياري]

ويضم تتابعاً من العناصر <CombinerParameter> المصاحبة لعنصر <PolicySet> أو عنصر <PolicySetIdReference> داخل <PolicySet>.

2.4.7 العنصر <Description>

بضم العنصر <Description> وصفاً لشلك حر للعنصر <PolicySet>.أو <Policy> أو <Rule>. والعنصر <Description> هو من النمط البسيط **xs:string**.

```
<xs:element name="Description" type="xs:string"/>
```

3.4.7 العنصر <PolicySetDefaults>

يحدد العنصر <PolicySetDefaults> قيم التغيب التي تنطبق على العنصر <PolicySet>.

```
<xs:element name="PolicySetDefaults" type="xacml:DefaultsType"/>
<xs:complexType name="DefaultsType">
   <xs:sequence>
         <xs:choice>
               <xs:element ref="xacml:XPathVersion" minOccurs="0"/>
         </xs:choice>
   </xs:sequence>
</xs:complexType>
```

والعنصر <PolicySetDefaults> هو من النمط المعقد **DefaultsType**.

ويضم العنصر <PolicySetDefaults> العناصر التالية:

- <XPathVersion> [خياري]

وهي النسخة XPath بالتغيب.

4.4.7 العنصر <XPathVersion>

يحدد العنصر <XPathVersion> نسخة المعيار W3C XPath:1999 التي تستعملها العناصر <AttributeSelector> والوظائف القائمة على اللغة XPath في مجموعة السياسات أو في السياسة.

```
<xs:element name="XPathVersion" type="xs:anyURI"/>
```

وعنوان المعرف URI للمعيار W3C XPath:1999 هو "http://www.w3.org/TR/1999/Rec-xpath-19991116". ويكون العنصر <XPathVersion> إلزامي إذا ضمت مجموعة السياسات أو السياسة العامة XACML العناصر <AttributeSelector> أو الوظائف القائمة على اللغة XPath.

5.4.7 العنصر <Target>

يعرّف العنصر <Target> مجموعة طلبات القرار التي يفترض أن يقيمها العنصر الأصل. ويظهر العنصر <Target> كفرع عنصر <PolicySet> و<Policy> وقد يظهر كفرع لعنصر <rule>. ويضم تعاريف الجهات المستعملة والموارد والإجراءات والبيئات.

ويضم العنصر <Target> تتابعاً رابطاً من العناصر <Subjects> و<Resources> و<Actions> و<Environments>. ولكي ينطبق أصل العنصر <Target> على طلب القرار يشترط وجود تلاؤم إيجابي واحد على الأقل بين كل قسم من العنصر <Target> والقسم المقابل للعنصر <xacml-context:Request>.

```
<xs:element name="Target" type="xacml:TargetType"/>
<xs:complexType name="TargetType">
   <xs:sequence>
         <xs:element ref="xacml:Subjects" minOccurs="0"/>
         <xs:element ref="xacml:Resources" minOccurs="0"/>
         <xs:element ref="xacml:Actions" minOccurs="0"/>
         <xs:element ref="xacml:Environments" minOccurs="0"/>
   </xs:sequence>
</xs:complexType>
```

والعنصر <Target> هو من النمط المعقد **TargetType**.

ويضم العنصر <Target> العناصر التالية:

- <Subjects> [خياري]

وهي مواصفة خاصة بتقابل نعوت الجهة المستعملة مع السياق. وفي حال غياب هذا العنصر يكون الهدف متلائماً مع جميع مواضيع الجهات المستعملة.

- <Resources> [خياري]

وهي مواصفة لتلاؤم نعوت المورد مع السياق. وفي حال غياب هذا العنصر يتلاءم الهدف مع جميع الموارد.

- <Actions> [خياري]

وهي مواصفة لتلاؤم نعوت الإجراء مع السياق. وفي حال غياب هذا العنصر يتلاءم الهدف مع جميع الإجراءات.

- <Environments> [خياري]

وهي مواصفة لتلاؤم نعوت البيئة مع السياق. وفي حال غياب هذا العنصر يتلاءم الهدف مع جميع البيئات.

6.4.7 العنصر <Subjects>

يضم العنصر <Subjects> تتابعاً مفككاً من العناصر <Subjects>.

```
<xs:element name="Subjects" type="xacml:SubjectsType"/>
<xs:complexType name="SubjectsType">
   <xs:sequence>
         <xs:element ref="xacml:Subject" maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>
```

والعنصر <Subjects> من النمط المعقد **SubjectsType**.

ويضم العنصر <Subjects> العناصر التالية:

- <Subject> [واحد أو أكثر، إلزامي]

كما تحدده الفقرة 7.4.7.

7.4.7 العنصر <Subject>

يضم العنصر <Subject> تتابعاً ترابطياً من العناصر <SubjectMatch>.

```
<xs:element name="Subject" type="xacml:SubjectType"/>
<xs:complexType name="SubjectType">
   <xs:sequence>
         <xs:element ref="xacml:SubjectMatch" maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>
```

والعنصر <Subject> من النمط المعقد **SubjectType**.

ويضم العنصر <Subject> العناصر التالية:

- <SubjectMatch> [واحد أو أكثر]

وهو تتابع ترابطي من تقابلات نعوت الجهة المستعملة في سياق الطلب وقيم النعوت المدمجة.

8.4.7 العنصر <SubjectMatch>

يعرف العنصر <SubjectMatch> مجموعة كيانات متصلة بالجهة المستعملة من خلال قيم نعت التلاؤم في العنصر <xacml-context:Subject> لسياق الطلب مع قيمة النعت المدمجة.

```
<xs:element name="SubjectMatch" type="xacml:SubjectMatchType"/>
<xs:complexType name="SubjectMatchType">
   <xs:sequence>
         <xs:element ref="xacml:AttributeValue"/>
         <xs:choice>
               <xs:element ref="xacml:SubjectAttributeDesignator"/>
               <xs:element ref="xacml:AttributeSelector"/>
         </xs:choice>
   </xs:sequence>
   <xs:attribute name="MatchId" type="xs:anyURI" use="required"/>
</xs:complexType>
```

والعنصر <SubjectMatch> من النمط المعقد **SubjectMatchType**.

ويضم العنصر <SubjectMatch> النعوت والعناصر التالية:

- MatchId [إلزامي]

وهو يحدد وظيفة التلاؤم. ويجب أن تكون قيمة هذا النعت من النمط **xs:anyURI** مع قيم نظامية من قبيل ما يرد في الفقرة 5.6.7.

- <xacml:AttributeValue> [إلزامي]

وهي قيمة النعت المدمجة.

- <SubjectAttributeDesignator> [اختيار إلزامي]

ويمكن استعمال هذا العنصر لتعرّف قيمة نعت واحدة أو أكثر في عنصر <Subject> من سياق الطلب.

- <AttributeSelector> [اختيار إلزامي]

ويمكن استعمال هذا العنصر لتعرف قيمة نعت واحدة أو أكثر في سياق الطلب وينبغي أن تنتهي عبارة XPath إلى نعت في عنصر <Subject> لسياق الطلب.

9.4.7 العنصر <Resources>

يضم العنصر <Resources> تتابعاً مفككاً للعناصر <Resources>.

```
<xs:element name="Resources" type="xacml:ResourcesType"/>
<xs:complexType name="ResourcesType">
   <xs:sequence>
         <xs:element ref="xacml:Resource" maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>
```

والعنصر <Resources> من النمط المعقد **ResourcesType**.

ويضم العنصر <Resources> العنصر التالي:

- <Resource> [واحد أو أكثر، إلزامي]

يرجى مراجعة الفقرة 10.4.7.

10.4.7 العنصر <Resource>

يضم العنصر <Resource> تتابعاً ترابطياً من العناصر <ResourceMatch>.

```
<xs:element name="Resource" type="xacml:ResourceType"/>
<xs:complexType name="ResourceType">
   <xs:sequence>
         <xs:element ref="xacml:ResourceMatch" maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>
```

والعنصر <Resource> هو من النمط المعقد **ResourceType**.

ويضم العنصر <Resource> العنصر التالي:

- <ResourceMatch> [واحد أو أكثر]

وهو تتابع ترابطي لتقابلات نعوت المورد في سياق الطلب مع قيم النعوت المدمجة.

11.4.7 العنصر <ResourceMatch>

يعرّف العنصر <ResourceMatch> مجموعة الكيانات المتصلة بالمورد من خلال مقابلة قيم النعوت في العنصر <xacml-context:Resource> لسياق الطلب مع قيمة النعت المدمجة.

```
<xs:element name="ResourceMatch" type="xacml:ResourceMatchType"/>
<xs:complexType name="ResourceMatchType">
   <xs:sequence>
         <xs:element ref="xacml:AttributeValue"/>
         <xs:choice>
               <xs:element ref="xacml:ResourceAttributeDesignator"/>
               <xs:element ref="xacml:AttributeSelector"/>
         </xs:choice>
   </xs:sequence>
   <xs:attribute name="MatchId" type="xs:anyURI" use="required"/>
</xs:complexType>
```

والعنصر <ResourceMatch> هو من النمط المعقد **ResourceMatchType**.

ويضم العنصر <ResourceMatch> النعوت والعناصر التالية:

- MatchId [إلزامي]

وهو يحدد وظيفة تلاؤم. ويجب أن تكون قيم هذا النعت من النمط **xs:anyURI**، مع قيم نظامية من قبيل القيم الواردة في الفقرة 5.6.7.

- <xacml:AttributeValue> [إلزامي]

قيمة نعت مدمجة.

- <ResourceAttributeDesignator> [اختيار إلزامي]

ويمكن استخدامه في تعرف قيمة نعت واحدة أو أكثر في العنصر <Resource> لسياق الطلب.

- <AttributeSelector> [اختيار إلزامي]

ويمكن استخدامه في تعرف قيمة نعت واحدة أو أكثر في سياق الطلب. وينبغي أن تنتهي عبارة XPath في نعت في العنصر <Resource> لسياق الطلب.

12.4.7 العنصر <Actions>

يضم العنصر <Actions> تتابعاً تفككياً للعناصر <Action>.

```
<xs:element name="Actions" type="xacml:ActionsType"/>
<xs:complexType name="ActionsType">
   <xs:sequence>
         <xs:element ref="xacml:Action" maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>
```

والعنصر <Actions> من النمط المعقد **ActionsType**.

ويضم العنصر <Actions> العنصر التالي:

- <Action> [واحد أو أكثر، إلزامي]

يرجى مراجعة الفقرة 13.4.7.

13.4.7 العنصر <Action>

يضم العنصر <Action> تتابعاً ترابطياً من العناصر <ActionMatch>.

```
<xs:element name="Action" type="xacml:ActionType"/>
<xs:complexType name="ActionType">
   <xs:sequence>
         <xs:element ref="xacml:ActionMatch" maxOccurs="unbounded"/>
```

```
    </xs:sequence>
</xs:complexType>
```

والعنصر <Action> من النمط المعقد **ActionType**.

ويضم العنصر <Action> العنصر التالي:

- <ActionMatch> [واحد أو أكثر]

وهو تتابع ترابطي من تقابلات نعوت الإجراء في سياق الطلب وقيم النعت المدمجة، انظر الفقرة 14.4.7.

14.4.7 العنصر <ActionMatch>

يعرّف العنصر <ActionMatch> مجموعة كيانات متصلة بالإجراء من خلال مقابلة قيم النعوت في العنصر <xacml-context:Action> لسياق الطلب مع قيمة النعت المدمجة.

```
<xs:element name="ActionMatch" type="xacml:ActionMatchType"/>
<xs:complexType name="ActionMatchType">
    <xs:sequence>
          <xs:element ref="xacml:AttributeValue"/>
          <xs:choice>
                <xs:element ref="xacml:ActionAttributeDesignator"/>
                <xs:element ref="xacml:AttributeSelector"/>
          </xs:choice>
    </xs:sequence>
    <xs:attribute name="MatchId" type="xs:anyURI" use="required"/>
</xs:complexType>
```

والعنصر <ActionMatch> هو من النمط المعقد **ActionMatchType**.

ويضم العنصر <ActionMatch> النعوت والعناصر التالية:

- MatchId [إلزامي]

وهو يحدد وظيفة التلاؤم. ويجب أن تكون قيمة هذا النعت من النمط **xs:anyURI** مع قيم نظامية من قبيل القيم الواردة في الفقرة 5.6.7.

- <xacml:AttributeValue> [إلزامي]

قيمة نعت مدمجة.

- <ActionAttributeDesignator> [اختيار إلزامي]

يمكن استخدامه في تعرّف قيمة نعت واحدة أو أكثر في العنصر <Action> لسياق الطلب.

- <AttributeSelector> [اختيار إلزامي]

يمكن استخدامه في تعرّف قيمة نعت واحدة أو أكثر في سياق الطلب. وينبغي أن تنتهي العبارة XPath في نعت في العنصر <Action> للسياق.

15.4.7 العنصر <Environments>

يضم العنصر <Environments> تتابعاً تفكيكياً للعناصر <Environment>.

```
<xs:element name="Environments" type="xacml:EnvironmentsType"/>
<xs:complexType name="EnvironmentsType">
    <xs:sequence>
          <xs:element ref="xacml:Environment" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
```

والعنصر <Environments> هو من النمط المعقد **EnvironmentsType**.

ويضم Environments العنصر التالي:

- <Environment> [واحد أو أكثر، إلزامي]

انظر الفقرة 16.4.7.

16.4.7 العنصر <Environment>

يضم العنصر <Environment> تتابعاً ترابطياً للعناصر <EnvironmentMatch>.

```
<xs:element name="Environment" type="xacml:EnvironmentType"/>
<xs:complexType name="EnvironmentType">
   <xs:sequence>
          <xs:element ref="xacml:EnvironmentMatch" maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>
```

والعنصر <Environment> هو من النمط المعقد **EnvironmentType**.

ويضم العنصر <Environment> العنصر التالي:

- <EnvironmentMatch> [واحد أو أكثر]

وهو تتابع ترابطي من تقابلات نعوت البيئة في سياق الطلب وقيم النعوت المدمجة.

17.4.7 العنصر <EnvironmentMatch>

يعرّف العنصر <EnvironmentMatch> بيئة ما من خلال مقابلة قيم النعوت في العنصر <xacml-context:Environment> لسياق الطلب مع قيمة النعت المدمجة.

```
<xs:element name="EnvironmentMatch" type="xacml:EnvironmentMatchType"/>
<xs:complexType name="EnvironmentMatchType">
   <xs:sequence>
          <xs:element ref="xacml:AttributeValue"/>
          <xs:choice>
                 <xs:element ref="xacml:EnvironmentAttributeDesignator"/>
                 <xs:element ref="xacml:AttributeSelector"/>
          </xs:choice>
   </xs:sequence>
   <xs:attribute name="MatchId" type="xs:anyURI" use="required"/>
</xs:complexType>
```

العنصر <EnvironmentMatch> هو من النمط المعقد **EnvironmentMatchType**.

ويضم العنصر <EnvironmentMatch> النعوت والعناصر التالية:

- MatchId [إلزامي]

وهو يحدد وظيفة تلاؤم. وينبغي أن تكون قيمة هذا النعت من النمط **xs:anyURI** مع قيم نظامية كتلك الواردة في الفقرة 5.6.7.

- <xacml:AttributeValue> [إلزامي]

قيمة نعت مدمجة.

- <EnvironmentAttributeDesignator> [اختيار إلزامي]

يمكن استخدامه في تعرّف قيمة نعت واحدة أو أكثر في العنصر <Environment> لسياق الطلب.

- <AttributeSelector> [اختيار إلزامي]

يمكن استخدامه في تعرف قيمة نعت واحدة أو أكثر في سياق الطلب. وينبغي أن تنتهي العبارة XPath إلى نعت في العنصر <Environment> لسياق الطلب.

18.4.7 العنصر <PolicySetIdReference>

يستخدم العنصر <PolicySetIdReference> في الإحالة إلى عنصر <PolicySet> من خلال معرّف الهوية. وإذا كان <PolicySetIdReference> موقعاً URL يمكن عندئذٍ حله في العنصر <PolicySet>. لكن آلية تحويل إحالة مجموعة سياسات إلى مجموعة السياسات المقابلة لا تقع ضمن نطاق هذه التوصية.

```
<xs:element name="PolicySetIdReference" type="xacml:IdReferenceType"/>
xs:complexType name="IdReferenceType">
   <xs:simpleContent>
          <xs:extension base="xs:anyURI">
                 <xs:attribute name="xacml:Version" type="xacml:VersionMatchType"
                 use="optional"/>
                 <xs:attribute name="xacml:EarliestVersion"
type="xacml:VersionMatchType" use="optional"/>
```

```
                <xs:attribute name="xacml:LatestVersion"
type="xacml:VersionMatchType" use="optional"/>
          </xs:extension>
   </xs:simpleContent>
</xs:complexType>
```

العنصر <PolicySetIdReference> هو من النمط المعقد **xacml:IdReferenceType**.

ويوسع النمط **IdReferenceType** النمط **xs:anyURI** باستعمال النعوت التالية:

- Version [إلزامي]

  وهو يحدد عبارة التلاؤم لنسخة مجموعة السياسات المحال إليها.

- EarliestVersion [خياري]

  يحدد عبارة التلاؤم لأول نسخة مقبولة لمجموعة السياسات المحال إليها.

- LatestVersion [خياري]

  يحدد عبارة التلاؤم لآخر نسخة مقبولة لمجموعة السياسات المحال إليها.

ويمكن تواجد أي مجموعة من هذه النعوت في العنصر <PolicySetIdReference> ويجب أن تلائم مجموعة السياسات المحال إليها جميع العبارات. وفي حال عدم وجود أي من هذه النعوت لا تقبل أي نسخة من مجموعة السياسات. وفي حال وجود أكثر من نسخة ملائمة ينبغي استخدام أحدثها.

19.4.7 العنصر <PolicyIdReference>

يستخدم العنصر <PolicyIdReference> في الإحالة إلى العنصر <Policy> باستعمال معرف هويته. وإذا كان العنصر <PolicyIdReference> موقعاً URL، أمكن عندئذٍ حله في العنصر <Policy>. ولكن آلية تحويل إحالة سياسة إلى السياسة المقابلة لا تقع ضمن نطاق هذه التوصية.

```
<xs:element name="PolicyIdReference" type="xacml:IdReferenceType"/>
```

والعنصر <PolicyIdReference> هو من النمط المعقد **xacml:IdReferenceType**.

20.4.7 نمط بسيط للعنصر VersionType

تضم عناصر هذا النمط رقم نسخة السياسة أو مجموعة السياسات.

```
<xs:simpleType name="VersionType">
   <xs:restriction base="xs:string">
         <xs:pattern value="(\d+\.)*\d+"/>
   </xs:restriction>
</xs:simpleType>
```

ويعبر عن رقم النسخة في تتابع من الأرقام العشرية تفصل فيما بينها نقطة (.). وتمثل العلامة 'd+' تتابعاً من رقم عشري واحد أو أكثر.

21.4.7 نمط بسيط للعنصر VersionMatchType

تضم عناصر هذا النمط عبارة موحدة موجزة تقابل رقم النسخة. وتقابل العبارة نسخاً من السياسة أو مجموعة السياسات المحال إليها والمقبولة لإدراجها في الإحالة إلى السياسة أو مجموعة السياسات.

```
<xs:simpleType name="VersionMatchType">
   <xs:restriction base="xs:string">
         <xs:pattern value="((\d+|\*)\.)*(\d+|\*|\+)"/>
   </xs:restriction>
</xs:simpleType>
```

ويفصل بين تقابلات النسخ بالعلامة '.' مثل سلسلة من النسخ. ويمثل الرقم تقابل رقمي مباشر. فالعلامة '*' A تعني أن أي رقم وحيد صالح، والعلامة '+' A أن أي رقم وأي أرقام متتالية صالحة. وبهذه الطريقة تكون النماذج الأربعة التالية ملائمة لسلسلة النسخ '1.2.3': '1.2.3'، '1.*.3'، '1.2.*' و'1.+'.

22.4.7 العنصر <Policy>

العنصر <Policy> هو أصغر كيان يقدم إلى النقطة PDP لأغراض التقييم.

ويمكن تقييم العنصر <Policy> وفي هذه الحالة ينبغي استخدام إجراء التقييم المحدد في الفقرة 10.6.7.

والمكونات الرئيسية لهذا العنصر هي العناصر <Target> و<Rule> و<CombinerParameters> و<RuleCombinerParameters> و<Obligations>، والنعت RuleCombiningAlgId.

ويعرّف العنصر <Target> قابلية تطبيق العنصر <Policy> على مجموعة من طلبات القرار. وإذا تلاءم العنصر <Target> الموجود في العنصر <Policy> سياق الطلب أمكن استخدام النقطة PDP للعنصر <Policy> في اتخاذها قرار الترخيص.

ويضم العنصر <Policy> تتابعاً من الخيارات بين العنصرين <VariableDefinition> و<Rule>.

ويجب تجميع القواعد الموجودة في العنصر <Policy> باستعمال الخوارزمية التي يحددها النعت RuleCombiningAlgId.

ويضم العنصر <Obligations> مجموعة التزامات يجب أن تفي بها النقطة PEP المرتبطة بقرار الترخيص.

```
<xs:element name="Policy" type="xacml:PolicyType"/>
<xs:complexType name="PolicyType">
   <xs:sequence>
         <xs:element ref="xacml:Description" minOccurs="0"/>
         <xs:element ref="xacml:PolicyDefaults" minOccurs="0"/>
         <xs:element ref="xacml:CombinerParameters" minOccurs="0"/>
         <xs:element ref="xacml:Target"/>
         <xs:choice maxOccurs="unbounded">
               <xs:element ref="xacml:CombinerParameters" minOccurs="0"/>
               <xs:element ref="xacml:RuleCombinerParameters" minOccurs="0"/>
               <xs:element ref="xacml:VariableDefinition"/>
               <xs:element ref="xacml:Rule"/>
         </xs:choice>
         <xs:element ref="xacml:Obligations" minOccurs="0"/>
   </xs:sequence>
   <xs:attribute name="PolicyId" type="xs:anyURI" use="required"/>
   <xs:attribute name="Version" type="xacml:VersionType" default="1.0"/>
   <xs:attribute name="RuleCombiningAlgId" type="xs:anyURI" use="required"/>
</xs:complexType>
```

والعنصر <Policy> هو من النمط المعقد **PolicyType**.

ويضم العنصر <Policy> النعوت والعناصر التالية:

- PolicyId [إلزامي]

معرف هوية السياسة. وتكمن مسؤولية النقطة PAP في ضمان ألاّ تحمل سياستان مرئيتان من النقطة PDP نفس معرف الهوية. ويمكن تحقيق ذلك من خلال اتباع مخطط URN أو URI مسبق التحديد. وإذا اتخذ معرف هوية السياسة شكل موقع URL يمكن عندئذٍ حله.

- Version [1.0 بالتغيب]

رقم نسخة السياسة.

- RuleCombiningAlgId [إلزامي]

وهو معرف خوارزمية تجميع القواعد الذي يجب استخدامه في تجميع المكونات <Policy> و<CombinerParameters> و<RuleCombinerParameters>.

- <Description> [خياري]

وصف شكل حر للسياسة.

- <PolicyDefaults> [خياري]

يحدد مجموعة من قيم التغيب التي يمكن استخدامها في السياسة. ونطاق تطبيق العنصر <PolicyDefaults> هو السياسة العامة.

- <CombinerParameters> [خياري]

تتابع من معلمات تستخدمها خوارزمية تجميع القواعد.

- <RuleCombinerParameters> [خياري]

تتابع من معلمات تستخدمها خوارزمية تجميع القواعد.

- <Target> [إلزامي]

يحدد العنصر <Target> قابلية تطبيق عنصر <Policy> على مجموعة طلبات قرارات.

ويجوز لمستحدث العنصر <Policy> أن يفصح عن العنصر <Target> أو يمكن حسابه استناداً إلى العناصر <Target> للعناصر <Rule> المحال إليها كتقاطع أو كمجموعة.

- <VariableDefinition> [أي عدد]

تعاريف وظائف مشتركة يمكن الإحالة إليها من أي مكان في قاعدة يمكن إيجاد تعبير فيها.

- <Rule> [أي عدد]

تتابع قواعد يجب تجميعها وفقاً للنعت RuleCombiningAlgId. ويجب النظر في القواعد التي تتلاءم فيها العناصر <Target> مع طلب القرار. أما القواعد التي لا تتلاءم فيها عناصر <Target> مع طلب القرار فينبغي تجاهلها.

- <Obligations> [خياري]

تتابع ترابطي من الالتزامات التي ينبغي أن تفي بها النقطة PEP المرتبطة بقرار الترخيص.

23.4.7 العنصر <PolicyDefaults>

يحدد العنصر <PolicyDefaults> قيم التغيب التي تنطبق على العنصر <Policy>.

```
<xs:element name="PolicyDefaults" type="xacml:DefaultsType"/>
<xs:complexType name="DefaultsType">
   <xs:sequence>
         <xs:choice>
               <xs:element ref="xacml:XPathVersion" minOccurs="0"/>
         </xs:choice>
   </xs:sequence>
</xs:complexType>
```

العنصر <PolicyDefaults> هو من النمط المعقد **DefaultsType**.

ويضم العنصر <PolicyDefaults> العنصر التالي:

- <XPathVersion> [خياري]

نسخة XPath بالتغيب.

24.4.7 العنصر <CombinerParameters>

ينقل العنصر <CombinerParameters> المعلمات إلى خوارزمية تجميع سياسات أو قواعد.

وإذا وردت عدة عناصر <CombinerParameters> ضمن نفس السياسة أو المجموعة السياسية فإنها تعتبر مساوية لعنصر <CombinerParameters> واحد يضم تسلسل جميع التتابعات <CombinerParameters> التي تتضمنها جميع العناصر <CombinerParameters> المذكورة سابقاً بحيث تحافظ على ترتيب ظهور العناصر <CominberParameters> في تسلسل العناصر <CombinerParameter>.

وتجدر الإشارة إلى أن النسخة XACML 2.0 تضع معلمات أي خوارزمية تجميع محددة فيها.

```
<xs:element name="CombinerParameters" type="xacml:CombinerParametersType"/>
<xs:complexType name="CombinerParametersType">
   <xs:sequence>
         <xs:element ref="xacml:CombinerParameter" minOccurs="0"
maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>
```

العنصر <CombinerParameters> هو من النمط **CombinerParameterType**

ويضم العنصر <CombinerParameters> العنصر التالي:

- <CombinerParameter> [أي عدد]

معلمة واحدة.

وتوفير العنصر <CombinerParameters> خياري.

25.4.7 العنصر <CombinerParameter>

ينقل العنصر <CombinerParameter> معلمة واحدة لخوارزمية تجميع السياسات أو القواعد.

```
<xs:element name="CombinerParameter" type="xacml:CombinerParameterType"/>
<xs:complexType name="CombinerParameterType">
   <xs:sequence>
         <xs:element ref="xacml:AttributeValue"/>
   </xs:sequence>
   <xs:attribute name="ParameterName" type="xs:string" use="required"/>
</xs:complexType>
```

والعنصر <CombinerParameter> هو من النمط **CombinerParameterType**.

ويضم العنصر <CombinerParameter> النعتين التاليين:

- ParameterName [إلزامي]

  معرف هوية المعلمة.

- AttributeValue [إلزامي]

  قيمة المعلمة.

وتوفير العنصر <CombinerParameter> خياري.

26.4.7 العنصر <RuleCombinerParameters>

ينقل العنصر <RuleCombinerParameters> المعلمات المصاحبة لقاعدة معينة ضمن سياسة ما إلى خوارزمية تجميع قواعد.

ويجب أن يرفق كل عنصر <RuleCombinerParameters> بقاعدة تضمها نفس السياسة. وإذا أحالت عدة عناصر <RuleCombinerParameters> إلى نفس القاعدة، فإنها تعتبر وكأنها عنصر واحد <RuleCombinerParameters> يضم تسلسل جميع التتابعات <CombinerParameters> التي تضمها العناصر <RuleCombinerParameters> المذكورة سابقاً بحيث يحافظ على ترتيب ظهور العناصر <RuleCombinerParameters> في تسلسل العناصر <CombinerParameter>.

وتجدر الإشارة إلى أن النسخة XACML 2.0 لا تضع معلمات أي من خوارزميات تجميع القواعد المحددة فيها.

```
<xs:element name="RuleCombinerParameters"
type="xacml:RuleCombinerParametersType"/>
<xs:complexType name="RuleCombinerParametersType">
   <xs:complexContent>
         <xs:extension base="xacml:CombinerParametersType">
               <xs:attribute name="RuleIdRef" type="xs:string" use="required"/>
         </xs:extension>
   </xs:complexContent>
</xs:complexType>
```

ويضم العنصر <RuleCombinerParameters> العنصر التالي:

- RuleIdRef [إلزامي]

  وهو معرف العنصر <Rule> الموجود في السياسة.

وتوفير العنصر <RuleCombinerParameters> خياري إلاّ عندما لا تتوفر معلمات المجمِّع.

27.4.7 العنصر <PolicyCombinerParameters>

ينقل العنصر <PolicyCombinerParameters> المعلمات المصاحبة لسياسة ما ضمن مجموعة سياسات إلى خوارزمية تجميع السياسات.

ويجب أن يرفق كل عنصر <PolicyCombinerParameters> بسياسة تضمها نفس مجموعة السياسات. وإذا أحالت عدة عناصر <PolicyCombinerParameters> إلى نفس السياسة فإنها تعتبر عنصراً <PolicyCombinerParameters> واحداً يضم تسلسلاً من جميع التتابعات <CombinerParameters> الموجود في جميع العناصر <PolicyCombinerParameters> المذكورة آنفاً على نحو يحافظ فيه على ترتيب ظهور العناصر <PolicyCombinerParameters> في تسلسل العناصر <CombinerParameter>.

وتجدر الإشارة إلى أن النسخة XACML 2.0 لا تضع معلمات أي من خوارزميات تجميع السياسة المحددة فيها.

```
<xs:element name="PolicyCombinerParameters"
type="xacml:PolicyCombinerParametersType"/>
<xs:complexType name="PolicyCombinerParametersType">
   <xs:complexContent>
         <xs:extension base="xacml:CombinerParametersType">
               <xs:attribute name="PolicyIdRef" type="xs:anyURI"
use="required"/>
         </xs:extension>
   </xs:complexContent>
</xs:complexType>
```

والعنصر <PolicyCombinerParameters> هو من النمط المعقد **PolicyCombinerParametersType**.

ويضم العنصر <PolicyCombinerParameters> العناصر التالية:

- PolicyIdRef [إلزامي]

وهو معرف العنصر <Policy> أو قيمة العنصر <PolicyIdReference> الموجود في مجموعة السياسات.

وتوفير العنصر <PolicyCombinerParameters> خياري ما عدا عندما لا تتوفر معلمات المجمع.

28.4.7 العنصر <PolicySetCombinerParameters>

ينقل العنصر <PolicySetCombinerParameters> معلمات مصاحبة لمجموعة سياسات معينة ضمن مجموعة سياسات إلى خوارزمية تجميع السياسات.

ويجب أن يرفق كل عنصر <PolicySetCombinerParameters> بمجموعة سياسات موجودة ضمن نفس مجموعة السياسات. وإذا أحالت عدة عناصر <PolicySetCombinerParameters> إلى نفس مجموعة السياسات فإنها تعتبر عنصرا <PolicySetCombinerParameters> واحداً يضم تسلسلاً من جميع تتابعات <PolicySetCombinerParameters> الموجودة <CombinerParameters> الموجودة في جميع العناصر <PolicySetCombinerParameters> المذكورة آنفاً على نحو يحافظ على ترتيب ظهور العناصر <PolicySetCominberParameters> في تسلسل العناصر <CombinerParameter>.

وتجدر الإشارة إلى أن النسخة XACML 2.0 لا تحدد معلمات أي من خوارزميات تجميع السياسات المحددة فيها.

```
<xs:element name="PolicySetCombinerParameters"
type="xacml:PolicySetCombinerParametersType"/>
<xs:complexType name="PolicySetCombinerParametersType">
   <xs:complexContent>
         <xs:extension base="xacml:CombinerParametersType">
               <xs:attribute name="PolicySetIdRef" type="xs:anyURI"
use="required"/>
         </xs:extension>
   </xs:complexContent>
</xs:complexType>
```

والعنصر <PolicySetCombinerParameters> هو من النمط المعقد **PolicySetCombinerParametersType**.

ويضم العنصر <PolicySetCombinerParameters> العنصر التالي:

- PolicySetIdRef [إلزامي]

وهو معرف عنصر <PolicySet> أو قيمة <PolicySetIdReference> تضمها مجموعة السياسات.

وليس توفير العنصر <PolicySetCombinerParameters> خيارياً إلا في حال عدم توفر معلمات المجمع.

29.4.7 العنصر <Rule>

يحدد العنصر <Rule> القواعد المختلفة في السياسة. والمكونات الرئيسية لهذا العنصر هي العنصران <Target> و<Condition> والنعت Effect.

ويمكن تقييم عنصر <Rule>، وفي هذه الحالة يجب استعمال إجراء التقييم المحدد في الفقرة 9.6.7.

```
<xs:element name="Rule" type="xacml:RuleType"/>
<xs:complexType name="RuleType">
   <xs:sequence>
         <xs:element ref="xacml:Description" minOccurs="0"/>
         <xs:element ref="xacml:Target" minOccurs="0"/>
```

```
        <xs:element ref="xacml:Condition" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute name="RuleId" type="xs:string" use="required"/>
    <xs:attribute name="Effect" type="xacml:EffectType" use="required"/>
</xs:complexType>
```

والعنصر <Rule> هو من النمط المعقد **RuleType**.

ويضم العنصر <Rule> النعوت والعناصر التالية:

- RuleId [إلزامي]

  سلسلة تعرف هوية هذه القاعدة.

- Effect [إلزامي]

أثر القاعدة. وقيمة هذا النعت هي إما "مسموح" وإما "مرفوض".

- <Description> [خياري]

  وصف شكل حر للقاعدة.

- <Target> [خياري]

  ويعرف مجموعة طلبات القرارات التي يفترض بالعنصر <Rule> أن يقيمها. وإذا ألغي هذا العنصر فإن هدف <Rule> سيحدده العنصر <Target> المدرج في العنصر <Policy>. لمزيد من التفاصيل انظر الفقرة 6.6.7.

- <Condition> [خياري]

  يجب للإسناد الذي يتعين الوفاء بشروطه وفقاً للقاعدة أن يتحدد في القيمة Effect.

30.4.7 نمط بسيط EffectType

يعرف النمط البسيط **EffectType** القيم المسموح بها للنعت Effect في العنصر <Rule> وللنعت FulfillOn في العنصر <Obligation>.

```
<xs:simpleType name="EffectType">
    <xs:restriction base="xs:string">
        <xs:enumeration value="Permit"/>
        <xs:enumeration value="Deny"/>
    </xs:restriction>
</xs:simpleType>
```

31.4.7 العنصر <VariableDefinition>

يستخدم العنصر <VariableDefinition> في تحديد قيمة يمكن أن يحيل إليها العنصر <VariableReference>. والاسم المعطى لنعته VariableId يجب ألاّ يظهر في النعت VariableId التابع لأي عنصر <VariableDefinition> آخر ضمن السياسة المحيطة. ويجوز للعنصر <VariableDefinition> أن يضم عنصراً <VariableReference> غير محدد، غير أنه يتعين في هذه الحالة تحديد عنصر <VariableDefinition> مقابل فيما بعد في السياسة المحيطة. ويجوز تجميع العناصر <VariableDefinition> مع بعضها البعض أو يجوز وضعها قرب مرجعها في السياسة المحيطة. وقد لا يتوفر أي مرجع للعنصر <VariableDefinition> أو قد يتوفر له مرجع واحد أو أكثر.

```
<xs:element name="VariableDefinition" type="xacml:VariableDefinitionType"/>
<xs:complexType name="VariableDefinitionType">
    <xs:sequence>
        <xs:element ref="xacml:Expression"/>
    </xs:sequence>
    <xs:attribute name="VariableId" type="xs:string" use="required"/>
</xs:complexType>
```

والعنصر <VariableDefinition> هو من النمط المعقد **VariableDefinitionType**. ويضم العناصر والنعوت التالية:

- <Expression> [إلزامي]

  وهو أي عنصر من النمط المعقد **ExpressionType**.

- VariableId [إلزامي]

  اسم التعريف المتغير.

32.4.7 العنصر <VariableReference>

يستخدم العنصر <VariableReference> في الإحالة إلى قيمة محددة ضمن نفس العنصر <Policy> المحيط. ويحيل العنصر <VariableReference> إلى العنصر <VariableDefinition> من خلال تساوي سلسلة القيمة لنعتيهما VariableId. ويجب أن يوجد عنصر <VariableDefinition> واحد فقط داخل نفس العنصر <Policy> المحيط الذي يحيل إليه <VariableReference>. وقد يوجد صفر واحد أو أكثر من العناصر <VariableReference> تحيل إلى نفس العنصر <VariableReference>.

```
<xs:element name="VariableReference" type="xacml:VariableReferenceType"
substitutionGroup="xacml:Expression"/>
<xs:complexType name="VariableReferenceType">
   <xs:complexContent>
         <xs:extension base="xacml:ExpressionType">
               <xs:attribute name="VariableId" type="xs:string" use="required"/>
         </xs:extension>
   </xs:complexContent>
</xs:complexType>
```

والعنصر <VariableReference> هو من النمط المعقد **VariableReferenceType** الذي ينتمي بدوره إلى النمط المعقد **ExpressionType**. وهو جزء من مجموعة بدائل العنصر <Expression>. ويجوز أن يظهر العنصر <VariableReference> في أي مكان يظهر فيه العنصر <Expression> في المخطط.

ويضم العنصر <VariableReference> النعت التالي:

- VariableId [إلزامي]

  وهو الاسم المستخدم في الإحالة إلى القيمة المحددة في عنصر <VariableDefinition>.

33.4.7 العنصر <Expression>

لا يستخدم العنصر <Expression> مباشرة في سياسة ما. ويعني العنصر <Expression> أن عنصراً يوسع النعت **ExpressionType** ويشكل جزءاً من مجموعة بدائل العنصر <Expression> سيظهر مكانه.

```
<xs:element name="Expression" type="xacml:ExpressionType" abstract="true"/>
<xs:complexType name="ExpressionType" abstract="true"/>
```

وفيما يلي العناصر التي تضمها مجموعة بدائل العنصر <Expression>:

<Apply> و<AttributeSelector> و<AttributeValue> و<Function> و<VariableReference>؛ <ActionAttributeDesignator> و<ResourceAttributeDesignator> و<SubjectAttributeDesignator> و<EnvironmentAttributeDesignator>.

34.4.7 العنصر <Condition>

العنصر <Condition> وظيفة بولانية في نعوت الجهة المستعملة والمورد والإجراء والبيئة أو وظائف نعوت.

```
<xs:element name="Condition" type="xacml:ConditionType"/>
<xs:complexType name="ConditionType">
   <xs:sequence>
         <xs:element ref="xacml:Expression"/>
   </xs:sequence>
</xs:complexType>
```

ويضم العنصر <Condition> عنصر <Expression> واحداً شرط أن يكون نمط معطيات رجوع العنصر <Expression>: "http://www.w3.org/2001/XMLSchema#boolean".

35.4.7 العنصر <Apply>

يعني العنصر <Apply> تطبيق دالة ما على حججها (متغيرات الدالة) وبالتالي تشفير نداء وظيفة. ويمكن تطبيق العنصر <Apply> على أي تجميعة أجزاء من مجموعة بدائل العنصر <Expression>.

```
<xs:element name="Apply" type="xacml:ApplyType"
substitutionGroup="xacml:Expression"/>
<xs:complexType name="ApplyType">
   <xs:complexContent>
```

```
          <xs:extension base="xacml:ExpressionType">
                <xs:sequence>
                      <xs:element ref="xacml:Expression" minOccurs="0"
maxOccurs="unbounded"/>
                </xs:sequence>
                <xs:attribute name="FunctionId" type="xs:anyURI" use="required"/>
          </xs:extension>
   </xs:complexContent>
</xs:complexType>
```

والعنصر <Apply> هو من النمط المعقد **ApplyType**.

ويضم العنصر <Apply> النعوت والعناصر التالية:

- FunctionId [إلزامي]

وهو معرف هوية الدالة التي تطبق على الحجج. وترد الوظائف المحددة في اللغة XACML في الملحق A.

- <Expression> [خياري]

حجج الدالة التي قد تضم وظائف أخرى.

36.4.7 العنصر <Function>

يستخدم العنصر <Function> في تسمية دالة ما حجة للوظيفة التي يحددها العنصر <Apply> الأصل. وعندما يكون العنصر <Apply> الأصلي دالة سلة من مرتبة أعلى تطبق الدالة المسماة على كل عنصر في السلة أو السلال الموجودة في المتغيرات الأخرى للعنصر الأصل.

```
<xs:element name="Function" type="xacml:FunctionType"
substitutionGroup="xacml:Expression"/>
<xs:complexType name="FunctionType">
   <xs:complexContent>
          <xs:extension base="xacml:ExpressionType">
                <xs:attribute name="FunctionId" type="xs:anyURI" use="required"/>
          </xs:extension>
   </xs:complexContent>
</xs:complexType>
```

والعنصر Function هو من النمط المعقد **FunctionType**.

ويضم العنصر Function النعوت التالية:

- FunctionId [إلزامي]

وهو معرف هوية الدالة.

37.4.7 النمط المعقد AttributeDesignatorType

النمط المعقد **AttributeDesignatorType** هو نمط العناصر التي تحدد هوية النعوت من خلال الاسم. ويضم المعلومات المطلوبة لمقابلة النعوت في سياق الطلب.

ويضم أيضاً معلومات التحكم في السلوك عند عدم وجود أي نعوت مقابلة في السياق.

ويجب ألاّ تؤثر عناصر هذا النمط على دلالات التقابل في النعوت المسماة لكنها تستطيع أن تقلص مجال البحث.

```
<xs:complexType name="AttributeDesignatorType">
   <xs:complexContent>
          <xs:extension base="xacml:ExpressionType">
                <xs:attribute name="AttributeId" type="xs:anyURI"
use="required"/>
                <xs:attribute name="DataType" type="xs:anyURI" use="required"/>
                <xs:attribute name="Issuer" type="xs:string" use="optional"/>
                <xs:attribute name="MustBePresent" type="xs:boolean"
use="optional" default="false"/>
          </xs:extension>
   </xs:complexContent>
</xs:complexType>
```

ويتلاءم نعت معين مع نعت إذا تلاءمت قيم نعوتهما AttributeId وDataType وIssuer على التوالي. ويجب أن يتلاءم مبين النعت AttributeId مع AttributeId النعت من خلال تساوي المعرف URI. ويجب أن يتلاءم مبين النعت DataType مع DataType نفس النعت من خلال تساوي المعرف URI.

وإذا وجد النعت Issuer في مبين النعت يجب أن يتلاءم مع Issuer نفس النعت باستخدام الدالة: "urn:oasis:names:tc:xacml:1.0:function:string-equal". وفي حال عدم وجود Issuer في مبين النعت فإن تلاؤم النعت مع النعت المسمى يخضع للنعتين AttributeId وDataType لا غير.

ويضم العنصر <AttributeDesignatorType> النعوت التالية:

- AttributeId [إلزامي]

يحدد هذا النعت المعرف AttributeId الذي يتلاءم معه النعت.

- DataType [إلزامي]

السلة التي يعيدها العنصر <AttributeDesignator> تضم قيم نمط المعطيات هذا.

- Issuer [خياري]

يحدد هذا النعت في حال وجوده العنصر Issuer الذي يتلاءم معه النعت.

- MustBePresent [خياري]

يقرر هذا النعت ما إذا كان العنصر يعيد النعت "غير محدد" أو سلة فارغة عند عدم وجود النعت المسمى في سياق الطلب.

38.4.7 العنصر <SubjectAttributeDesignator>

يستعيد العنصر <SubjectAttributeDesignator> سلة قيم نعت لجهة مستعملة مصنفة مسماة استناداً إلى سياق الطلب. ونعت الجهة المستعملة نعت موجود ضمن عنصر <Subject> لسياق الطلب. والموضوع المصنف هو جهة يعرّفها نعت فئة الجهة المستعملة. ونعت جهة مصنفة مسماة هو نعنت جهة مسماة لجهة مصنفة معينة.

ويعيد العنصر <SubjectAttributeDesignator> سلة تضم جميع قيم نعت الجهة التي تتلاءم من خلال نعوت الجهة المصنفة المسماة. وعند عدم وجود أي نعت تلاؤم في السياق، يقرر النعت MustBePresent ما إذا كان على هذا النعت أن يعيد سلة فارغة أو معلومة "غير محدد".

ويوسع العنصر **SubjectAttributeDesignatorType** دلالات تقابل النمط **AttributeDesignatorType** بحيث يقلّص مجال البحث ليقتصر على الجهة المصنفة المحددة على نحو تتلاءم فيه قيمة النعت SubjectCategory مع قيمة النعت SubjectCategory للعنصر <Subject> في سياق الطلب.

وإذا ضم سياق الطلب عدة جهات مستعملة لها نفس النعت SubjectCategory XML توجب علاجها كما لو كانت جهة مصنفة واحدة.

وقد يظهر <SubjectAttributeDesignator> في العنصر <SubjectMatch> وينتقل إلى العنصر <Apply> على أنه حجة (متغير دالة).

```
<xs:element name="SubjectAttributeDesignator"
type="xacml:SubjectAttributeDesignatorType"
substitutionGroup="xacml:Expression"/>
<xs:complexType name="SubjectAttributeDesignatorType">
   <xs:complexContent>
          <xs:extension base="xacml:AttributeDesignatorType">
                <xs:attribute name="SubjectCategory" type="xs:anyURI"
use="optional" default="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"/>
          </xs:extension>
   </xs:complexContent>
</xs:complexType>
```

والعنصر <SubjectAttributeDesignator> هو من النمط **SubjectAttributeDesignatorType**. ويوسِّع النمط المعقد **SubjectAttributeDesignatorType** النمط المعقد **AttributeDesignatorType** بإضافة النعت SubjectCategory.

- SubjectCategory [خياري]

يحدد هذا النعت الجهة المستعملة المصنفة التي يستند إليها تقابل نعوت الجهة المستعملة. وفي حال عدم وجود النعت SubjectCategory تستخدم قيمته بالتغيب وهي "urn:oasis:names:tc:xacml:1.0:subject-category:access-subject".

39.4.7 العنصر <ResourceAttributeDesignator>

يستعيد العنصر <ResourceAttributeDesignator> سلة قيم لنعت المورد المسمى استناداً إلى سياق الطلب. ونعت المورد هو نعت مدرج في العنصر <Resource> لسياق الطلب. ونعت المورد المسمى هو نعت مسمى يقابل نعت مورد ما. ويجب اعتبار نعت مورد مسمى موجوداً إذا وجد نعت مورد واحد على الأقل يلائم المعيار المذكور أدناه. وقيمة نعت المورد هي قيمة نعت مدرج في نعت المورد.

ويعيد العنصر <ResourceAttributeDesignator> سلة تضم جميع قيم نعوت المورد التي تقابل نعت المورد المسمى. وفي حال عدم وجود نعت تقابل في السياق، يقرر النعت MustBePresent ما إذا كان يتعين على هذا العنصر إعادة سلة فارغة أو معلمة "غير محدد".

وينبغي أن يقابل نعت مورد مسمى نعت مورد حسب دلالات التقابل المحددة في النمط المعقد **AttributeDesignatorType**.

وقد يظهر <ResourceAttributeDesignator> في العنصر <ResourceMatch> وينتقل إلى العنصر <Apply> كحجة.

```
<xs:element name="ResourceAttributeDesignator"
type="xacml:AttributeDesignatorType" substitutionGroup="xacml:Expression"/>
```

والعنصر <ResourceAttributeDesignator> هو من النمط المعقد AttributeDesignatorType.

40.4.7 العنصر <ActionAttributeDesignator>

يستعيد العنصر <ActionAttributeDesignator> سلة قيم لنعت الإجراء المسمى استناداً إلى سياق الطلب. ونعت الإجراء هو نعت مدرج في العنصر <Action> لسياق الطلب. ولنعت الإجراء المسمى معيار خاص (يرد وصفه أدناه) يتلاءم معه نعت إجراء. ويجب اعتبار نعت إجراء مسمى موجوداً إذا وجد نعت إجراء واحد على الأقل متلائماً مع المعيار. وقيمة نعت الإجراء هي قيمة نعت مدرجة داخل نعت إجراء.

وينبغي أن يعيد العنصر <ActionAttributeDesignator> سلة تضم جميع قيم نعت الإجراء التي تتقابل استناداً إلى نعت الإجراء المسمى. وعند غياب أي نعت تقابل في السياق، يقرر النعت MustBePresent ما إذا كان يتعين على هذا العنصر أن يعيد سلة فارغة أو معلمة "غير محدد".

وينبغي أن يقابل نعت إجراء مسمى نعت إجراء حسب دلالات التقابل المحددة في النمط المعقد **AttributeDesignatorType**.

وقد يظهر العنصر <ActionAttributeDesignator> في العنصر <ActionMatch>. وقد ينتقل إلى العنصر <Apply> كحجة.

```
<xs:element name="ActionAttributeDesignator" type="xacml:AttributeDesignatorType"
substitutionGroup="xacml:Expression"/>
```

والعنصر <ActionAttributeDesignator> هو من النمط المعقد **AttributeDesignatorType**.

41.4.7 العنصر <EnvironmentAttributeDesignator>

يستعيد العنصر <EnvironmentAttributeDesignator> سلة قيم لنعت البيئة المسمى استناداً إلى سياق الطلب. ونعت البيئة نعت مدرج داخل العنصر <Environment> لسياق الطلب. ولنعت البيئة المسمى معيار خاص (يرد وصفه أدناه) يتلاءم معه نعت البيئة. وينبغي اعتبار نعت بيئة مسمى موجوداً إذا تلاءم نعت بيئة واحد على الأقل مع المعيار. وقيمة نعت البيئة هي قيمة نعت مدرجة داخل نعت بيئة.

ويقيم العنصر <EnvironmentAttributeDesignator> كسلة جميع قيم نعوت البيئة التي تتقابل استناداً إلى نعت البيئة المسمى. وعند عدم وجود نعت تقابل في السياق يقرر النعت MustBePresent ما إذا كان يتعين على هذا العنصر إعادة سلة فارغة أو معلومة "غير محدد".

وينبغي أن يقابل نعت بيئة مسمى نعت بيئة حسب دلالات التقابل المحددة في النمط المعقد **AttributeDesignatorType**.

وقد ينتقل العنصر <EnvironmentAttributeDesignator> إلى العنصر <Apply> كحجة.

```
<xs:element   name="EnvironmentAttributeDesignator"   type="xacml:AttributeDesignatorType"
                                                    substitutionGroup="xacml:Expression"/>
```

والعنصر <EnvironmentAttributeDesignator> هو من النمط المعقد **AttributeDesignatorType**.

42.4.7 العنصر <AttributeSelector>

يعرف العنصر <AttributeSelector> النعوت وفقاً لمواقعها في سياق الطلب. وتوفير العنصر <AttributeSelector> خياري.

ويضم النعت RequestContextPath MXL للعنصر <AttributeSelector> تعبير XPath نظامي عقدة سياقه هي العنصر <xacml-context:Request>. ويقيم العنصر AttributeSelector بأنه سلة قيم يتحدد نمط معطياتها وفقاً للنعت DataType التابع للعنصر. وإذا كان النعت DataType المحدد في AttributeSelector نمط معطيات بدائياً (معرف في W3C Schema:2001

وW3C Datatypes:2001, 3.2) يجب أن تتحول القيمة اللغوية التي يعيدها التعبير XPath إلى القيمة DataType المحددة في العنصر <AttributeSelector>. وإذا نتج خطأ من تحويل القيمة التي يعيدها التعبير XPath بحيث لا تكون القيمة حالة صالحة للنعت DataType تكون قيمة العنصر <AttributeSelector> عندئذٍ "غير محدد".

xs:string()
xs:boolean()
xs:integer()
xs:double()
xs:dateTime()
xs:date()
xs:time()
xs:hexBinary()
xs:base64Binary()
xs:anyURI()

وإذا لم يكن النعت DataType المحدد في AttributeSelector واحداً من الأنماط البدائية المعددة سابقاً فإن النعت AttributeSelector يعيد سلة حالات من النعت DataType المحدد. وإذا وقع خطأ من جراء تحويل القيم التي يعيدها التعبير XPath إلى النمط DataType المحدد فإن نتيجة AttributeSelector تكون "غير محدد".

ويجب أن تكون كل عقدة ينتقيها التعبير XPath المحدد عقدة نص أو عقدة نعت أو عقدة تعليمات معالجة أو عقدة شرح. ويجب تحويل التمثيل التسلسلي لقيمة كل عقدة إلى قيمة نعت نمط معطيات محدد ونتيجة AttributeSelector هي سلة قيم النعت الناتجة عن العقد المنتقاة.

وإذا لم تكن العقدة المنتقاة التي يحددها التعبير XPath واحدة من العقد المعددة أعلاه (أي عقدة نص أو عقدة نعت أو عقدة تعليمات معالجة أو عقدة شرح)، فإن نتيجة السياسة العامة تكون "غير محدد" مع قيمة StatusCode للتعبير "urn:oasis:names:tc:xacml:1.0:status:syntax-error".

```
<xs:element name="AttributeSelector" type="xacml:AttributeSelectorType"
substitutionGroup="xacml:Expression"/>
<xs:complexType name="AttributeSelectorType">
   <xs:complexContent>
         <xs:extension base="xacml:ExpressionType">
               <xs:attribute name="RequestContextPath" type="xs:string"
use="required"/>
               <xs:attribute name="DataType" type="xs:anyURI" use="required"/>
               <xs:attribute name="MustBePresent" type="xs:boolean"
use="optional" default="false"/>
         </xs:extension>
   </xs:complexContent>
</xs:complexType>
```

والعنصر <AttributeSelector> هو من النمط المعقد **AttributeSelectorType**.

ويضم العنصر <AttributeSelector> النعوت التالية:

- RequestContextPath [إلزامي]

وهو تعبير XPath عقدة سياقه هي العنصر <xacml-context:Request>. ويجب عدم فرض تقييدات على قواعد تركيب اللغة XPath.

- DataType [إلزامي]

يجب أن تضم السلة التي يعيدها العنصر <AttributeSelector> قيم نمط المعطيات.

- MustBePresent [خياري]

يقرر هذا النعت ما إذا كان ينبغي للعنصر أن يعيد المعلمة "غير محدد" أو السلة فارغة في ما لم ينتق التعبير XPath أي عقدة.

43.4.7 العنصر <AttributeValue>

يضم العنصر <xacml:AttributeValue> قيمة نعت حرفية.

```
<xs:element name="AttributeValue" type="xacml:AttributeValueType"
substitutionGroup="xacml:Expression"/>
<xs:complexType name="AttributeValueType" mixed="true">
   <xs:complexContent>
         <xs:extension base="xacml:ExpressionType">
               <xs:sequence>
                     <xs:any namespace="##any" processContents="lax"
minOccurs="0" maxOccurs="unbounded"/>
               </xs:sequence>
               <xs:attribute name="DataType" type="xs:anyURI" use="required"/>
               <xs:anyAttribute namespace="##any" processContents="lax"/>
         </xs:extension>
   </xs:complexContent>
</xs:complexType>
```

والعنصر <xacml:AttributeValue> هو من النمط المعقد **AttributeValueType**.

ويضم العنصر <xacml:AttributeValue> النعوت التالية:

- DataType [إلزامي]

وهو نمط معطيات قيمة النعت.

44.4.7 العنصر <Obligations>

يضم العنصر <Obligations> مجموعة عناصر <Obligation>.

وتوفير عنصر <Obligations> خياري.

```
<xs:element name="Obligations" type="xacml:ObligationsType"/>
<xs:complexType name="ObligationsType">
   <xs:sequence>
         <xs:element ref="xacml:Obligation" maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>
```

والعنصر <Obligations> هو من النمط المعقد **ObligationsType**.

ويضم العنصر <Obligations> العنصر التالي:

- <Obligation> [واحد أو أكثر]

وهو تتابع من الالتزامات.

45.4.7 العنصر <Obligation>

يضم العنصر <Obligation> معرف هوية الالتزام ومجموعة نعوت تشكل متغيرات دالة الإجراء الذي يحدده الالتزام. ويدل النعت FulfillOn على الأثر الذي يجب من أجله وفاء النقطة PEP بهذا الالتزام.

```
<xs:element name="Obligation" type="xacml:ObligationType"/>
<xs:complexType name="ObligationType">
   <xs:sequence>
         <xs:element ref="xacml:AttributeAssignment" minOccurs="0"
maxOccurs="unbounded"/>
   </xs:sequence>
   <xs:attribute name="ObligationId" type="xs:anyURI" use="required"/>
   <xs:attribute name="FulfillOn" type="xacml:EffectType" use="required"/>
</xs:complexType>
```

والعنصر <Obligation> هو من النمط المعقد **ObligationType**. ويرجى مراجعة الفقرة 14.6.7 للحصول على وصف كيفية إعادة النقطة PDP لمجموعة الالتزامات.

ويضم العنصر <Obligation> العناصر والنعوت التالية:

- ObligationId [إلزامي]

معرف هوية الالتزام. وتفسر النقطة PEP قيمة معرف هوية الالتزام.

- FulfillOn [إلزامي]

الأثر الذي يجب من أجله وفاء النقطة PEP بهذا الالتزام.

- <AttributeAssignment> [خياري]

تخصيص متغيرات دالة الالتزام. وتفسر النقطة PEP قيم متغيرات دالة الالتزام.

46.4.7 العنصر <AttributeAssignment>

يستخدم العنصر <AttributeAssignment> في إدراج متغيرات الدالة في الالتزامات. ويضم المعرف AttributeId وقيمة النعت المقابل من خلال توسيع تعريف النمط **AttributeValueType**. ويمكن استعمال العنصر <AttributeAssignment> بأي طريقة تنسجم مع قواعد تركيب المخطط الذي يتمثل في تتابع عناصر <xs:any>. وتفسر النقطة PEP القيمة المحددة التي لا تعود محددة باللغة XACML.

```
<xs:element name="AttributeAssignment" type="xacml:AttributeAssignmentType"/>
<xs:complexType name="AttributeAssignmentType" mixed="true">
   <xs:complexContent>
         <xs:extension base="xacml:AttributeValueType">
               <xs:attribute name="AttributeId" type="xs:anyURI"
use="required"/>
         </xs:extension>
   </xs:complexContent>
</xs:complexType>
```

والعنصر <AttributeAssignment> هو من النمط المعقد **AttributeAssignmentType**.

ويضم العنصر <AttributeAssignment> النعت التالي:

- AttributeId [إلزامي]

معرف هوية النعت.

5.7 قواعد تركيب السياق

مقاطع المخططات التي ترد في الفقرات التالية غير معيارية.

1.5.7 العنصر <Request>

العنصر <Request> هو عنصر عالي السوية في مخطط سياق اللغة SACML. والعنصر <Request> هو طبقة تجريد تستخدمها لغة السياسة. وتصف هذه التوصية لأغراض التبسيط تقييم اللغة من حيث عمليات السياق. غير أن نقطة تطابق PDP ليست ملزمة بتحويل السياق فعلياً إلى شكل وثيقة XML. لكنه يجب على كل نظام مطابق للغة XACML أن ينتج تماماً نفس قرارات الترخيص كما لو أن جميع المداخل تحولت إلى شكل العنصر <xacml-context:Request>.

ويضم العنصر <Request> العناصر <Subject> و<Resource> و<Action> و<Environment>. وقد يوجد عدة عناصر <Subject> وفي بعض الحالات عدة عناصر <Resource>. ويضم كل عنصر فرع تتابعاً من العناصر <xacml-context:Attribute> مرفقة بالجهة المستعملة والمورد والإجراء والبيئة على التوالي. وتشكل هذه العناصر <Attribute> جزءاً من تقييم السياسة.

```
<xs:element name="Request" type="xacml-context:RequestType"/>
<xs:complexType name="RequestType">
   <xs:sequence>
         <xs:element ref="xacml-context:Subject" maxOccurs="unbounded"/>
         <xs:element ref="xacml-context:Resource" maxOccurs="unbounded"/>
         <xs:element ref="xacml-context:Action"/>
         <xs:element ref="xacml-context:Environment"/>
   </xs:sequence>
</xs:complexType>
```

والعنصر <Request> هو من النمط المعقد **RequestType**.

ويضم العنصر <Request> العناصر التالية:

- <Subject> [واحد أو أكثر]

وهو يحدد معلومات عن موضوع سياق الطلب من خلال تعداد تتابع من عناصر <Attribute> مصاحبة للجهة المستعملة. ويسمح بعنصر <Subject> واحد أو أكثر. والجهة المستعملة هي كيان مصاحب لطلب النفاذ. فمثلاً قد تمثل إحدى الجهات المستعمل الشخصي

الذي بدأ التطبيق الذي أصدر الطلب؛ وقد تمثل جهة أخرى شفرة التطبيق القابلة للاستخدام والمسؤولة عن إصدار الطلب؛ وقد تمثل جهة ثالثة الآلة التي نُفذ فيها التطبيق؛ وتمثل جهة رابعة الكيان اللازم لاستيعاب المورد. ويجب إدراج نعوت كل من هذه الكيانات في عناصر <Subject> منفصلة.

- <Resource> [مورد واحد أو أكثر]

وهو يحدد معلومات عن المورد أو الموارد التي طلب النفاذ إليها من خلال بيان تتابع من العناصر <Attribute> المصاحبة للإجراء.

- <Action> [إلزامي]

ويحدد الإجراء المطلوب لتنفيذه في المورد من خلال بيان مجموعة العناصر <Attribute> المصاحبة للإجراء.

- <Environment> [إلزامي]

ويضم مجموعة عناصر <Attribute> خاصة بالبيئة.

2.5.7 العنصر <Subject>

يحدد العنصر <Subject> جهة مستعملة من خلال بيان تتابع من عناصر <Attribute> مصاحبة للجهة.

```
<xs:element name="Subject" type="xacml-context:SubjectType"/>
<xs:complexType name="SubjectType">
   <xs:sequence>
         <xs:element ref="xacml-context:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
   </xs:sequence>
   <xs:attribute name="SubjectCategory" type="xs:anyURI"
default="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"/>
</xs:complexType>
```

والعنصر <Subject> هو من النمط المعقد **SubjectType**.

ويضم العنصر <Subject> العناصر والنعوت التالية:

- SubjectCategory [خياري]

يدل هذا النعت على الدور الذي يؤديه العنصر <Subject> الأصل في وضع طلب النفاذ. وفي حال عدم وجود هذا النعت في عنصر <Subject> ما، يجب استعمال قيمة التغيب "urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" مع الإشارة إلى أن العنصر <Subject> الأصل يمثل الكيان المسؤول أساساً عن إصدار طلب النفاذ.

وإذا ضم أكثر من عنصر <Subject> واحد نعتاً "urn:oasis:names:tc:xacml:2.0:subject-category" يحمل نفس القيمة فإن النقطة PDP تعالج محتويات هذه العناصر إذا كانت مدرجة في نفس العنصر <Subject>.

- <Attribute> [أي عدد]

تتابع نعوت تنطبق على الجهة المستعملة.

ويضم عنصر <Subject> عادة عنصر <Attribute> مع معرف AttributeId للقيمة "urn:oasis:names:tc:xacml:1.0:subject:subject-id" يضم هوية الجهة المستعملة.

وقد يضم عنصر <Subject> عناصر <Attribute> إضافية.

3.5.7 العنصر <Resource>

يحدد العنصر <Resource> معلومات عن المورد الذي طلب النفاذ إليه وذلك من خلال بيان تتابع من العناصر <Attribute> المصاحبة للمورد. وقد يضم محتوى المورد.

```
<xs:element name="Resource" type="xacml-context:ResourceType"/>
<xs:complexType name="ResourceType">
   <xs:sequence>
         <xs:element ref="xacml-context:ResourceContent" minOccurs="0"/>
         <xs:element ref="xacml-context:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>
```

والعنصر <Resource> هو من النمط المعقد **ResourceType**.

ويضم العنصر <Resource> العنصرين التاليين:

- <ResourceContent> [خياري]

  وهو محتوى المورد.

- <Attribute> [أي عدد]

  تتابع من نعوت المورد.

وقد يضم العنصر <Resource> عنصراً <Attribute> واحداً أو أكثر مع معرف AttributeId للقيمة "urn:oasis:names:tc:xacml:2.0:resource:resource-id" وكل عنصر <Attribute> من هذا القبيل هو تمثيل مطلق وكامل لهوية مورد واحد طلب النفاذ إليه. وإذا وجد أكثر من تمثيل واحد من هذا القبيل وإذا تحدد أي عنصر <Attribute> في هذا المعرف AttributeId يتحدد عندئذ عنصر <Attribute> لكلٍ تمثيل مستقل لهوية المورد. ويجب أن تحيل جميع هذه العناصر <Attribute> إلى نفس حالة المورد الواحد. وقد تحدد مواصفات مورد معين تمثيلاً معيارياً واحداً لحالات المورد. وفي هذه الحالة يستعمل أي عنصر <Attribute> مع معرف AttributeId هذا التمثيل والواحد لا غير.

وقد يضم عنصر <Resource> عناصر <Attribute> إضافية.

4.5.7 العنصر <ResourceContent>

العنصر <ResourceContent> هو بديل مفهوم محتوى المورد. وعندما تحيل السياسة XACML إلى محتويات المورد باستعمال العنصر <AttributeSelector> يجب عندئذ إدراج العنصر <ResourceContent> في السلسلة RequestContextPath.

```
<xs:complexType name="ResourceContentType" mixed="true">
   <xs:sequence>
         <xs:any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
   </xs:sequence>
   <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>
```

والعنصر <ResourceContent> هو من النمط المعقد **ResourceContentType**.

ويسمح العنصر <ResourceContent> بعناصر ونعوت اعتباطية.

5.5.7 العنصر <Action>

يحدد العنصر <Action> الإجراء المطلوب من المورد من خلال عرض مجموعة من العناصر <Attribute> المصاحبة للإجراء.

```
<xs:element name="Action" type="xacml-context:ActionType"/>
<xs:complexType name="ActionType">
   <xs:sequence>
         <xs:element ref="xacml-context:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>
```

والعنصر <Action> هو من النمط المعقد **ActionType**.

ويضم العنصر <Action> العناصر التالية:

- <Attribute> [أي عدد]

  قائمة بنعوت الإجراء الذي يستخدم في المورد.

6.5.7 العنصر <Environment>

يضم العنصر <Environment> مجموعة نعوت البيئة.

```
<xs:element name="Environment" type="xacml-context:EnvironmentType"/>
<xs:complexType name="EnvironmentType">
   <xs:sequence>
         <xs:element ref="xacml-context:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>
```

والعنصر <Environment> هو من النمط المعقد **EnvironmentType**.

ويضم العنصر <Environment> العنصر التالي:

- <Attribute> [أي عدد]

وهو قائمة بنعوت البيئة. ونعوت البيئة هي النعوت التي لا تصاحب المورد أو الإجراء أو أي من جهات طلب النفاذ.

7.5.7 العنصر <Attribute>

العنصر <Attribute> هو التجريد المركزي لسياق الطلب. ويضم معطيات شرح النعت وقيمة نعت واحدة أو أكثر. وتضم معطيات شرح النعت معرف هوية النعت وجهة إصداره. وقد يحيل العنصران <AttributeDesignator> و<AttributeSelector> في السياسة إلى نعوت باستعمال هذه المعطيات الشرحية.

```
<xs:element name="Attribute" type="xacml-context:AttributeType"/>
<xs:complexType name="AttributeType">
   <xs:sequence>
         <xs:element ref="xacml-context:AttributeValue" maxOccurs="unbounded"/>
   </xs:sequence>
   <xs:attribute name="AttributeId" type="xs:anyURI" use="required"/>
   <xs:attribute name="DataType" type="xs:anyURI" use="required"/>
   <xs:attribute name="Issuer" type="xs:string" use="optional"/>
</xs:complexType>
```

والعنصر <Attribute> هو من النمط المعقد **AttributeType**.

ويضم العنصر <Attribute> النعوت والعناصر التالية:

- AttributeId [إلزامي]

معرف هوية النعت. عدد من معرفات الهوية مخصصة للغة XACML لتدل على النعوت المتداولة الاستعمال.

- DataType [إلزامي]

نمط معطيات محتويات العنصر <xacml-context:AttributeValue>. ويكون إما نمطاً بدائياً معرفاً في هذه التوصية أو نمطاً (بدائياً أو منظماً) معرفاً في مكان اسم يفصح عنه العنصر <xacml-context>.

- Issuer [خياري]

جهة إصدار النعت. على سبيل المثال، يمكن أن تكون قيمة النعت x500Name وهي تصل بمفتاح عمومي أو قد تكون معرف هوية آخر يتم تبادله خارج النطاق بين الجهات المنتجة والمستهلكة.

- <xacml-context:AttributeValue> [واحد أو أكثر]

قيمة نعت واحدة أو أكثر. وقد يكون لكل قيمة نعت محتويات فارغة تحدث مرة أو عدة مرات.

8.5.7 العنصر <AttributeValue>

يضم العنصر <xacml-context:AttributeValue> قيمة نعت.

```
<xs:element name="AttributeValue" type="xacml-context:AttributeValueType"/>
<xs:complexType name="AttributeValueType" mixed="true">
   <xs:sequence>
         <xs:any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
   </xs:sequence>
   <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>
```

والعنصر <xacml-context:AttributeValue> هو من النمط المعقد **AttributeValueType**.

ويجب تحديد نمط معطيات العنصر <xacml-context:AttributeValue> باستخدام النعت DataType للعنصر <Attribute> الأصل.

9.5.7 العنصر <Response>

العنصر <Response> عنصر عالي السوية في مخطط السياق XACML. والعنصر <Response> هو طبقة تجريدية تستخدمها لغة السياسة. ويجب على أي نظام ملكية يستعمل اللغة XACML أن يحول العنصر <Response> من سياق اللغة XACML إلى شكل قرار ترخيصه.

ويغلف العنصر <Response> قرار الترخيص الذي تنتجه النقطة PDP. وهو يضم تتابعاً من نتيجة واحدة أو أكثر وعنصر <Result> واحد لكل مورد مطلوب. ويمكن أن تعيد بعض التطبيقات عدة نتائج خاصة تلك التي توفر مواصفة اللغة XACML لطلبات الموارد المتعددة. وتوفير عدة نتائج أمر خياري.

```
<xs:element name="Response" type="xacml-context:ResponseType"/>
<xs:complexType name="ResponseType">
   <xs:sequence>
          <xs:element ref="xacml-context:Result" maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>
```

والعنصر <Response> هو من النمط المعقد **ResponseType**.

ويضم العنصر <Response> العنصر التالي:

- <Result> [واحد أو أكثر]

  نتيجة قرار ترخيص.

10.5.7 العنصر <Result>

يمثل العنصر <Result> نتيجة قرار ترخيص للمورد الذي يحدده النعت ResourceId.

ويضم مجموعة التزامات يتعين على النقطة PEP الوفاء بها. وإذا لم تفهم النقطة PEP الالتزامات أو لم تستطع الوفاء بها يجب عندئذ أن تعمل كما لو أن النقطة PDP رفضت النفاذ إلى المورد المطلوب.

```
<xs:complexType name="ResultType">
   <xs:sequence>
          <xs:element ref="xacml-context:Decision"/>
          <xs:element ref="xacml-context:Status" minOccurs="0"/>
          <xs:element ref="xacml:Obligations" minOccurs="0"/>
   </xs:sequence>
   <xs:attribute name="ResourceId" type="xs:string" use="optional"/>
</xs:complexType>
```

والعنصر <Result> هو من النمط المعقد **ResultType**.

ويضم العنصر <Result> النعوت والعناصر التالية:

- ResourceId [خياري]

  وهو معرف هوية المورد المطلوب. وإذا حذف هذا النعت تكون هوية المورد هي تلك التي يحددها نعت المورد "urn:oasis:names:tc:xacml:1.0:resource:resource-id" في العنصر <Request> المقابل.

- <Decision> [إلزامي]

  قرار الترخيص: "مسموح" أو "مرفوض" أو "غير محدد" أو "لا يوجد".

- <Status> [خياري]

  يدل على حدوث أخطاء أثناء تقييم طلب القرار ومع إمكانية الحصول على معلومات عن هذه الأخطاء. وإذا ضمّ العنصر <Response> عناصر <Result> ذات عناصر <Status> متماثلة وكان العنصر <Response> متواجداً في مغلف بروتوكول قادر على إرسال معلومات حالة، أمكن عندئذٍ وضع معلومات الحالة المشتركة في مغلف البروتوكول وحذف هذا العنصر <Status> من جميع العناصر <Result>.

- <Obligations> [خياري]

  قائمة من الالتزامات التي يجب أن تفي بها النقطة PEP. وإذا لم تفهم النقطة PEP إحدى هذه الالتزامات أو لم تستطع الوفاء بها، يجب عندئذٍ أن تعمل كما لو أن النقطة PDP رفضت النفاذ إلى المورد المطلوب.

11.5.7 العنصر <Decision>

يضم العنصر <Decision> نتيجة تقييم السياسة.

```
<xs:element name="Decision" type="xacml-context:DecisionType"/>
<xs:simpleType name="DecisionType">
   <xs:restriction base="xs:string">
          <xs:enumeration value="Permit"/>
          <xs:enumeration value="Deny"/>
          <xs:enumeration value="Indeterminate"/>
          <xs:enumeration value="NotApplicable"/>
   </xs:restriction>
</xs:simpleType>
```

والعنصر <Decision> هو من النمط البسيط **DecisionType**.

ويضم العنصر <Decision> المعاني التالية:

- سماح: النفاذ المطلوب مسموح.
- رفض: النفاذ المطلوب مرفوض.
- غير محدد: لا تستطيع النقطة PDP تقييم النفاذ المطلوب. ومن بين الأسباب مثل هذه النتيجة ما يلي: نعوت مفقودة، أخطاء شبكة عند استعادة السياسات، تقسيم على صفر أثناء تقييم السياسة، أخطاء قواعد تركيب في طلب القرار أو في السياسة وغير ذلك.
- غير موجود: لا تمتلك النقطة PDP أي سياسة تنطبق على طلب القرار هذا.

12.5.7 العنصر <Status>

يمثل العنصر <Status> حالة نتيجة قرار الترخيص.

```
<xs:element name="Status" type="xacml-context:StatusType"/>
<xs:complexType name="StatusType">
   <xs:sequence>
          <xs:element ref="xacml-context:StatusCode"/>
          <xs:element ref="xacml-context:StatusMessage" minOccurs="0"/>
          <xs:element ref="xacml-context:StatusDetail" minOccurs="0"/>
   </xs:sequence>
</xs:complexType>
```

العنصر <Status> هو من النمط المعقد **StatusType**.

ويضم العنصر <Status> العناصر التالية:

- <StatusCode> [إلزامي]

  شفرة الحالة.

- <StatusMessage> [خياري]

  رسالة حالة تصف شفرة الحالة.

- <StatusDetail> [خياري]

  معلومات إضافية عن الحالة.

13.5.7 العنصر <StatusCode>

يضم العنصر <StatusCode> قيمة شفرة حالة كبرى وشفرات حالة صغرى خيارية.

```
<xs:element name="StatusCode" type="xacml-context:StatusCodeType"/>
<xs:complexType name="StatusCodeType">
   <xs:sequence>
          <xs:element ref="xacml-context:StatusCode" minOccurs="0"/>
   </xs:sequence>
   <xs:attribute name="Value" type="xs:anyURI" use="required"/>
</xs:complexType>
```

والعنصر <StatusCode> هو من النمط المعقد **StatusCodeType**.

ويضم العنصر <StatusCode> النعوت والعناصر التالية:

- Value [إلزامي]

راجع الفقرة 8.B للحصول على قائمة القيم.

- <StatusCode> [أي عدد]

شفرة حالة صغرى. وتحدد شفرة الحالة هذه شفرة حالة أصلها.

14.5.7 العنصر <StatusMessage> [أي عدد]

العنصر <StatusMessage> هو وصف شكل حر لشفرة الحالة.

```
<xs:element name="StatusMessage" type="xs:string"/>
```

والعنصر <StatusMessage> هو من النمط **xs:string**.

15.5.7 العنصر <StatusDetail>

يحدد العنصر <StatusDetail> العنصر <Status> مع معلومات إضافية.

```
<xs:element name="StatusDetail" type="xacml-context:StatusDetailType"/>
<xs:complexType name="StatusDetailType">
   <xs:sequence>
         <xs:any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>
```

والعنصر <StatusDetail> هو من النمط المعقد **StatusDetailType**.

ويسمح العنصر <StatusDetail> بالمحتوى XML الاعتباطي.

وإدراج عنصر <StatusDetail> خياري. غير أن النقطة PDP تعيد إحدى قيم <StatusCode> المحددة في اللغة XACML وتدخل عنصر <StatusDetail> ثم تطبق القواعد التالية:

```
urn:oasis:names:tc:xacml:1.0:status:ok
```

ويجب ألاّ تعيد النقطة PDP عنصراً <StatusDetail> مصاحباً لقيمة الحالة "ok".

```
urn:oasis:names:tc:xacml:1.0:status:missing-attribute
```

ويجوز لنقطة PDP أن تختار عدم إعادة أي معلومات <StatusDetail> أو أن تختار إعادة عنصر <StatusDetail> يضم عنصراً <xacml-context: MissingAttributeDetail> واحداً أو أكثر.

```
urn:oasis:names:tc:xacml:1.0:status:syntax-error
```

ويجب ألاّ تعيد نقطة PDP عنصراً <StatusDetail> مرفقاً بقيمة حالة "خطأ كبير". وقد يمثل خطأ التركيب إما مشكلة في السياسة المستخدمة أو في سياق الطلب. ويمكن أن تعيد النقطة PDP عنصر <StatusMessage> يصف المشكلة.

```
urn:oasis:names:tc:xacml:1.0:status:processing-error
```

ويجب ألاّ تعيد نقطة PDP عنصر <StatusDetail> مرفقاً بقيمة حالة "خطأ معالجة". وتدل شفرة الحالة هذه على مشكلة داخلية في النقطة PDP. وقد تختار النقطة PDP لأسباب أمنية أن لا تعيد معلومات إضافية إلى النقطة PEP. أما في حالة خطأ التقسيم على صفر أو أي خطأ حسابي آخر تعيد النقطة PDP عنصر <StatusMessage> يصف طبيعة الخطأ.

16.5.7 العنصر <MissingAttributeDetail>

ينقل العنصر <MissingAttributeDetail> معلومات عن النعوت اللازمة لتقييم السياسة المفقودة من سياق الطلب.

```
<xs:element name="MissingAttributeDetail" type="xacml-
context:MissingAttributeDetailType"/>
<xs:complexType name="MissingAttributeDetailType">
<xs:sequence>
<xs:element ref="xacml-context:AttributeValue" minOccurs="0"
maxOccurs="unbounded"/>
</xs:sequence>
<xs:attribute name="AttributeId" type="xs:anyURI" use="required"/>
<xs:attribute name="DataType" type="xs:anyURI" use="required"/>
   <xs:attribute name="Issuer" type="xs:string" use="optional"/>
</xs:complexType>
```

والعنصر <MissingAttributeDetail> هو من النمط المعقد **MissingAttributeDetailType**.

ويضم العنصر <MissingAttributeDetal> النعوت والعناصر التالية:

- AttributeValue [خياري]

  القيمة المطلوبة للنعت المفقود.

- <AttributeId> [إلزامي]

  معرف هوية النعت المفقود.

- <DataType> [إلزامي]

  نمط المعطيات للنعت المفقود.

- Issuer [خياري]

  يحدد هذا النعت في حال توفره القيمة Issuer المطلوبة للنعت المفقود.

وإذا ضمت النقطة PDP العناصر <xacml-context:AttributeValue> في العنصر <MissingAttributeDetail>. دلّ ذلك على القيم المقبولة لذلك النعت. وإلاّ فإن ذلك يدل على أسماء النعوت التي أخفقت النقطة PDP في حلها أثناء تقييمها. وتكون قائمة النعوت جزئية أو كاملة. ولا تضمن النقطة PDP أن توفير القيم أو النعوت المفقودة سيكفي للوفاء بتلبية احتياجات السياسة.

6.7 المتطلبات الوظيفية للغة XACML

تحدد هذه الفقرة بعض المتطلبات الوظيفية غير المرتبطة مباشرة بإنتاج أو استهلاك عنصر XACML خاص.

1.6.7 نقطة تفعيل السياسة

تصف هذه الفقرة المتطلبات في النقطة PDP.

تعمل التطبيقات في دور النقطة PEP إذا احتفظت بالنفاذ إلى مجموعة الموارد وطلبت من النقطة PDP قرار ترخيص. ويجب أن تتقيد النقطة PEP بقرارات ترخيص النقطة PDP.

1.1.6.7 النقطة PEP الأساسية

إذا جاء القرار بنتيجة "مسموح" فإن النقطة PEP تسمح بالنفاذ. وإذا صاحبت القرار التزامات ما، لا تسمح النقطة PEP بالنفاذ إلاّ إذا فهمت هذه الالتزامات وكانت قادرة على الوفاء بها.

أما إذا جاء القرار بنتيجة "مرفوض"، فإن النقطة PEP ترفض النفاذ. وإذا صاحبت القرار بعض الالتزامات فإن النقطة PEP لا ترفض النفاذ إلاّ إذا فهمت هذه الالتزامات وكانت قادرة على الوفاء بها.

وإذا كانت نتيجة القرار "غير موجود"ن يكون سلوك النقطة PEP غير محدد.

وإذا كانت نتيجة القرار "غير محدد" يكون سلوك النقطة PEP غير محدد.

2.1.6.7 النقطة PEP تميل إلى الرفض

إذا كانت نتيجة القرار "مسموح"، تسمح النقطة PEP بالنفاذ. وإذا صاحبت القرار بعض الالتزامات فإن النقطة PEP لا تسمح بالنفاذ إلاّ إذا فهمت هذه الالتزامات وكانت قادرة على الوفاء بها.

وينتج عن جميع القرارات الأخرى رفض النفاذ.

وينتج عن جميع القرارات الأخرى سماح النفاذ.

ملاحظة – الإجراءات الأخرى مثل استشارة نقاط PDP إضافية أو إعادة صياغة/إعادة تقديم طلب القرار أو غيرها إجراءات غير ممنوعة.

3.1.6.7 النقطة PEP تميل إلى السماح

إذا كانت نتيجة القرار "مرفوض"، ترفض النقطة PEP النفاذ. وإذا صاحبت القرار بعض الالتزامات فإن النقطة PEP لا ترفض النفاذ إلاّ إذا فهمت هذه الالتزامات وكانت قادرة على الوفاء بها.

ملاحظة – الإجراءات الأخرى مثل استشارة نقاط PDP إضافية أو إعادة صياغة/تقديم طلب القرار وغير ذلك، إجراءات غير ممنوعة.

2.6.7 تقييم النعت

تمثل إدارة السياق النعوت في سياق الطلب بغض النظر عن ظهورها في طلب القرار الأصلي ويحال إليها في السياسة من خلال مؤشرات ومنتقيات نعوت الجهة المستعملة والموارد والإجراءات والبيئة. والنعت المسمى هو المصطلح المستخدم في المعيار الذي تستخدمه مؤشرات ومنتقيات النعوت المحددة للجهة المستعملة والمورد والإجراء والبيئة في الإحالة إلى نعوت خاصة في عناصر جهة سياق الطلب ومواردها وإجراءاتها وبيئتها على التوالي.

1.2.6.7 النعوت المبنينة

يضم العنصران <xacml:AttributeValue> و<xacml-context:AttributeValue> حالة من نمط المعطيات XML المبنينة مثل <ds:KeyInfo>. وتقدم هذه التوصية عدة طرق لمقارنة المحتويات مع عناصر من هذا القبيل.

1) يمكن في بعض الحالات مقارنة هذه العناصر باستخدام إحدى وظائف السلسلة XACML مثل "string-regexp-match" الواردة أدناه. ويتطلب ذلك إعطاء العنصر نمط المعطيات "http://www.w3.org/2001/XMLSchema#string". على سبيل المثال، يظهر نمط المعطيات المبنينة المؤلف فعلياً من **ds:KeyInfo/KeyName** في السياق على الشكل التالي:

```
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
   &lt;ds:KeyName&gt;jhibbert-key&lt;/ds:KeyName&gt;
</AttributeValue>
```

ولا تصلح هذه الطريقة عموماً إلاّ إذا كان نمط المعطيات المبنينة بسيطاً.

2) يمكن استعمال عنصر <AttributeSelector> لانتقاء محتويات عصر فرعي ورقي لنمط معطيات مبنينة عن طريق تعبير XPath. ويمكن عندئذٍ مقارنة تلك القيمة باستعمال إحدى الوظائف XACML المناسبة المتوفرة لأغراض نمط معطياتها البدائي. وتتطلب هذه الطريقة توفير النقطة PDP لخصائص التعابير XPath الخيارية.

3) يمكن استعمال عنصر <AttributeSelector> لانتقاء أي عقدة في نمط المعطيات المبنينة باستعمال تعبير XPath. ويمكن عندئذٍ مقارنة هذه العقدة باستخدام إحدى الوظائف القائمة على اللغة XPath والواردة في الفقرة A.3. وتتطلب هذه الطريقة توفير النقطة PDP للخصائص الخيارية للتعابير والوظائف XPath.

2.2.6.7 سلال النعوت

تحدد اللغة XACML مجموعات ضمنية لأنماط معطياتها. وتسمى اللغة XACML مجموعة قيم من نمط معطيات واحد سلة. وسلال أنماط المعطيات ضرورية لأن انتقاء العقد من مورد XML أو من سياق طلب XACML قد يعيد أكثر من قيمة واحدة.

ويستعمل العنصر <AttributeSelector> تعبير XPath من أجل تحديد انتقاء معطيات من مورد XML. وتسمى نتيجة التعبير XPath مجموعة عقد، وهي تضم جميع العقد الورقية من المورد XML الذي يتواءم مع العبارة المنطقية في التعبير XPath. واستناداً إلى وظائف الفهرسة المختلفة الواردة في المعيار W3C XPath:1999، ينبغي افتراض أن مجموعة العقد الناتجة هي مجموعة العقد المتقابلة. وتعرف هذه التوصية أيضاً العنصر <AttributeDesignator> للحصول على نفس منهجية التقابل بين النعوت في سياق الطلب XACML.

والقيم في الحيبة غير مرتبة وقد تتضاعف بعض القيم. ويجب عدم وجود مفهوم سلة تضم حقائب أو سلة تضم قيم من أنماط مختلفة (أي أن لا تحتوي سلة في اللغة XACML إلاّ على قيم من نفس نمط المعطيات).

3.2.6.7 نعوت متعددة القيم

إذا ضم عنصر <Attribute> واحد في سياق طلب ما عدة عناصر فرعية <xacml-context:AttributeValue>، يجب عندئذٍ أن تكون سلة القيم الناجمة عن تقييم العنصر <Attribute> مماثلة لسلة القيم الناجمة عن تقييم سياق يظهر فيه كل عنصر <xacml-context:AttributeValue> في عنصر <Attribute> مستقل يحمل معطيات شرح مماثلة.

4.2.6.7 تقابل النعوت

يتضمن النعت المسمى معياراً محدداً من أجل مقابلة النعوت في السياق. ويحدد النعت المعرف AttributeId والنمط DataType ويحدد النعت المسمى أيضاً جهة الإصدار Issuer. ويقابل نعت مسمى نعتاً إذا تقابلت قيم نعوتها AttributeId وDataType وIssuer الاختياري مع نظيراتها في كل عنصر جهة مستعملة ومورد وإجراء وبيئة محددة في السياق. وينبغي أن يتلاءم المعرف AttributeId للنعت المسمى مع المعرف AttributeId لنعت السياق المقابل من خلال تساوي المعرف URI. وينبغي أن يتلاءم النمط DataType للنعت المسمى مع النمط DataType لنعت السياق المقابل من خلال تساوي المعرف URI. وإذا توفر النعت Issuer في النعت المسمى فينبغي أن يتلاءم مع Issuer نعت السياق المقابل عند استخدام الوظيفة urn:oasis:names:tc:xacml:1.0:function:string-equal. أما في حال عدم توفره في النعت المسمى فإن تقابل نعت السياق مع النعت المسمى لا يخضع إلاّ للنعتين AttributeId وDataType بغض النظر عن وجود أو غياب أو حقيقة قيمة Issuer في نعت السياق المقابل. وفي حال منتقي النعت يخضع تقابل النعت والنعت المسمى للتعبير XPath وDataType.

5.2.6.7 استعادة النعت

تطلب النقطة PDP قيم نعوت سياق الطلب من إدارة السياق. وتحيل النقطة PDP إلى النعوت كما لو أنها كانت في وثيقة مادية لسياق الطلب، لكن إدارة السياق هي المسؤولة عن الحصول على القيم المطلوبة وتوفيرها بأي وسيلة تراها مناسبة. وتعيد إدارة السياق قيم النعوت التي تتلاءم مع مؤشر النعت أو منتقي النعت ويحولها إلى سلة قيم ذات نمط معطيات محدد. وفي حال عدم تلاؤم أي نعت من سياق الطلب يعتبر النعت مفقوداً. وإذا فقد النعت يتحكم النعت MustBePresent في إعادة مؤشر النعت أو منتقي النعت لسلة فارغة أو نتيجة "غير محددة". وإذا كان النعت MustBePresent "صحيحاً" فإن النعت المفقود ينتج القيمة "غير محدد". ويجب تناول هذه النتيجة "غير محدد" بالتوافق مع مواصفة التعابير والقواعد والسياسات ومجموعات السياسات الشاملة. وإذا كانت النتيجة "غير محدد"، يمكن عندئذٍ بيان AttributeId وDataType و Issuerللنعت في قرار الترخيص. غير أن نقطة PDP قد تختار عدم إعادة مثل هذه المعلومات لأسباب أمنية.

6.2.6.7 نعوت البيئة

إذا توفرت قيمة لأحد هذه النعوت في طلب القرار، تستعمل إدارة السياق تلك القيمة. وإلاّ فإن إدارة السياق تقدم قيمة ما. وفي حالة نعوت التاريخ والساعة تتخذ القيمة الموفرة دلالات "التاريخ والساعة المنطبقان على طلب القرار".

3.6.7 تقييم التعبير

تحدد اللغة XACML تعابير على شكل العناصر المعددة أدناه، والتي غالباً ما يؤلف فيها العنصران <Apply> و<Con<Apply>dition> معظم التعابير. وينبغي أن تكون التعابير الصالحة من النمط الصحيح مما يعني أن أنماط كل نمط موجود داخل العنصرين <Apply> و<Condition> ستقبل أنماط متغيرات الدالة المقابلة للوظيفة التي يسميها النعت FunctionId. وينبغي أن يكون النمط الناتج للعنصر <Apply> أو العنصر <Condition> النمط الناتج للوظيفة، مما يمكن اختصاره إلى نمط معطيات بدائي أو سلة نمط معطيات بدائي باستعمال توحيد النمط. وتحدد اللغة XACML نتيجة التقييم "غير محدد" التي تعادل نتيجة تعبير غير صالح أو خطأ تشغيلي يقع أثناء تقييم التعبير.

وتحدد اللغة XACML العناصر التالية لتصفها في مجموعة بدائل العنصر <Expression>:

- <xacml:AttributeValue>
- <xacml:SubjectAttributeDesignator>
- <xacml:ResourceAttributeDesignator>
- <xacml:ActionAttributeDesignator>
- <xacml:EnvironmentAttributeDesignator>
- <xacml:AttributeSelector>
- <xacml:Apply>
- <xacml:Condition>
- <xacml:Function>
- <xacml:VariableReference>

4.6.7 التقييم الحسابي

يحدد المعيار IEEE 754 كيفية تقييم الدالات الحسابية في سياق ما، مما يحدد قيم التغيب للتقريب أو للجبر أو غيرها. وتستعمل اللغة XACML هذه المواصفة لتقييم جميع الدالات الصحيحة والمضاعفة استناداً إلى السياق الموسع بالتغيب. المحسّن مع تمثيل مزدوج الدقة:

- الأعلام: موضوعة جميعها على 0؛
- منشطات القطع: موضوعة جميعها على 0 باستثناء منشط قطع "القسمة على صفر" الذي ينبغي أن يتخذ القيمة 1؛
- الدقة: تضبط على التمثيل مزدوج الدقة المشار إليه؛
- الجبر: يضبط على جبر نصف زوجي.

5.6.7 تقييم التقابل

تظهر عناصر تقابل النعوت في العنصر <Target> من القواعد والسياسات ومجموعات السياسة. وهي التالية:

- <SubjectMatch>
- <ResourceMatch>
- <ActionMatch>
- <EnvironmentMatch>

وتمثل هذه العناصر تعابير بولانية في نعوت الجهة المستعملة والمورد والإجراء والبيئة على التوالي. ويضم عنصر التقابل النعت MatchId الذي يحدد الوظيفة الواجب استعمالها في إجراء تقييم التقابل، والعنصرين <xacml:AttributeValue> و<AttributeDesignator> أو <AttributeSelector> الذي يحدد نعت السياق الذي ينبغي مقابلته مع القيمة المحددة.

ويحدد النعت MatchId وظيفة تقارن بين حجتين ويعيد نمط نتيجة "http://www.w3.org/2001/XMLSchema#boolean". وينبغي توفير قيمة النعت المحددة في عنصر التقابل من أجل الوظيفة MatchId على أنها حجتها الثانية، كما يرد أدناه. ويتقابل DataType العنصر <xacml:AttributeValue> مع نمط معطيات الحجة الأولى التي تتوقعها الوظيفة MatchId. ويتقابل DataType العنصر <AttributeDesignator> أو <AttributeSelector> مع نمط معطيات الحجة الثانية التي تنتظرها الوظيفة MatchId.

وفيما يلي وظائف اللغة XACML المعيارية التي تفي بمتطلبات استعمال قيمة النعت MatchId:

```
urn:oasis:names:tc:xacml:2.0:function:-type-equal
urn:oasis:names:tc:xacml:2.0:function:-type-greater-than
urn:oasis:names:tc:xacml:2.0:function:-type-greater-than-or-equal
urn:oasis:names:tc:xacml:2.0:function:-type-less-than
urn:oasis:names:tc:xacml:2.0:function:-type-less-than-or-equal
urn:oasis:names:tc:xacml:2.0:function:-type-match
```

علاوة على ذلك، قد تظهر الوظائف الموجودة تماماً داخل توسيع اللغة للغة XACML كقيمة للنعت MatchId. وقد تستعمل هذه الوظائف أنماط المعطيات التي هي بدورها توسيعات طالما أعادت وظيفة التوسيع نتيجة بولانية واتخذت نمطين أساسيين وحيدين كمدخلاتها. وينبغي أن تكون الوظيفة المستخدمة كقيمة للنعت MatchId سهلة الفهرسة. وقد يعيق استعمال الوظائف غير المفهرسة أو المعقدة التقييم الصحيح لطلبات القرار.

ودلالات التقييم لعنصر التقابل هي التالية. إذا وقع خطأ تشغيلي أثناء تقييم العنصر <AttributeDesignator> أو <AttributeSelector> كانت نتيجة التعبير الكامل "غير محدد". وإذا عمل العنصر <AttributeDesignator> أو <AttributeSelector> على تقييم سلة فارغة كانت نتيجة التعبير "خطأ". وإلاّ فإنه ينبغي تطبيق الوظيفة MatchId بين العنصر <xacml:AttributeValue> وكل عنصر في السلة المعادة من العنصر <AttributeDesignator> أو <AttributeSelector>. وإذا كانت نتيجة واحدة على الأقل من تطبيقات الوظائف هذه "صحيح" فإن نتيجة كامل التعبير تكون "صحيح". وإذا أعطت واحدة على الأقل من تطبيقات الوظائف النتيجة "غير محدد" فإن النتيجة تكون "غير محدد". وأخيراً إذا أعطت جميع تطبيقات الوظائف القيمة "خطأ"، فإن نتيجة التعبير بكامله تكون "خطأ".

ومن الممكن أيضاَ التعبير عن دلالة عنصر تقابل الهدف في حالة، مثال: يمكن التعبير عن تقابل الهدف الذي يقارن "اسم الموضوع" الذي يبدأ بالاسم "John" على النحو التالي:

```
<SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
       John.*
    </AttributeValue>
    <SubjectAttributeDesignator
          AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
          DataType="http://www.w3.org/2001/XMLSchema#string"/>
</SubjectMatch>
```

ومن ناحية أخرى، يمكن التعبير عن نفس دلالة التقابل كعنصر <Apply> في حالة ما باستخدام الوظيفة "urn:oasis:names:tc:xacml:1.0:function:any-of" على النحو التالي:

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
    <Function
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"/>
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        John.*
    </AttributeValue>
    <SubjectAttributeDesignator
         AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
         DataType="http://www.w3.org/2001/XMLSchema#string"/>
</Apply>
```

6.6.7 تقييم الهدف

تكون قيمة الهدف "تقابل" إذا كانت الجهات المستعملة والموارد والإجراءات والبيئات المحددة في الهدف تتلاءم جميعها مع قيم سياق الطلب. أما إذا كانت قيمة أي جهة أو مورد أو إجراء أو بيئة محددة في الهدف "غير محدد"، فإن الهدف سيكون عندئذٍ "غير محدد". وإلاّ فيكون الهدف "لا تقابل". ويظهر جدول مقابلة الأهداف في الجدول 7-1.

الجدول X.1142/1-7 – جدول مقابلة الأهداف

قيمة الجهة المستعملة	قيمة المورد	قيمة الإجراء	قيمة البيئة	قيمة الهدف
"تقابل"	"تقابل"	"تقابل"	"تقابل"	"تقابل"
"لا تقابل"	"تقابل" أو "لا تقابل"	"تقابل" أو "لا تقابل"	"تقابل" أو "لا تقابل"	"لا تقابل"
"تقابل" أو "لا تقابل"	"لا تقابل"	"تقابل" أو "لا تقابل"	"تقابل" أو "لا تقابل"	"لا تقابل"
"تقابل" أو "لا تقابل"	"تقابل" أو "لا تقابل"	"لا تقابل"	"تقابل" أو "لا تقابل"	"لا تقابل"
"تقابل" أو "لا تقابل"	"تقابل" أو "لا تقابل"	"تقابل" أو "لا تقابل"	"لا تقابل"	"لا تقابل"
"غير محدد"	غير هام	غير هام	غير هام	"غير محدد"
غير هام	"غير محدد"	غير هام	غير هام	"غير محدد"
غير هام	غير هام	"غير محدد"	غير هام	"غير محدد"
غير هام	غير هام	غير هام	"غير محدد"	"غير محدد"

وينبغي مقابلة الجهات المستعملة والموارد والإجراءات والبيئات مع قيم سياق الطلب إذا كان تقابل واحد على الأقل من العناصر <Subject> أو <Resource> أو <Action> أو <Environment> على التوالي مع قيمة سياق طلب. ويظهر جدول مقابلة الجهات المستعمل في الجدول 7-2. وجداول مقابلة الموارد والإجراءات والبيئات مماثلة.

الجدول X.1142/2-7 – جدول مقابلة الجهات المستعملة

القيم <Subject>	القيمة <Subjects>
"تقابل" واحد على الأقل	"تقابل"
لا تقابل وواحد على الأقل "غير محدد"	"غير محدد"
"لا تقابل" في جميع القيم	"لا تقابل"

وتقابل الجهة المستعملة أو المورد أو الإجراء أو البيئة قيمة ما في سياق الطلب إذا كانت قيمة جميع العناصر <SubjectMatch> أو <ResourceMatch> أو <ActionMatch> أو <EnvironmentMatch> على التوالي "صح".

ويظهر جدول مقابلة الجهات المستعملة في الجدول 7-3. وجداول المورد والإجراء والبيئة مماثلة.

الجدول X.1142/3-7 – جدول مقابلة الجهات المستعملة

قيم <SubjectMatch>	قيمة <Subject>
جميعها "صح"	"تقابل"
لا يوجد "خطأ" وقيمة واحدة على الأقل "غير محدد"	"غير محدد"
قيمة واحدة على الأقل "خطأ"	"لا تقابل"

7.6.7 تقييم VariableReference

يحيل العنصر <VariableReference> إلى عنصر <VariableDefinition> واحد مدرج في نفس العنصر <Policy>. ويسمى عنصر <VariableReference> لا يحتوي على عنصر <VariableDefinition> داخل العنصر <Policy> الشامل مرجعاً غير محدد. والسياسات التي تحتوي على إحالات غير محددة سياسات غير صالحة.

ويؤثر العنصر <VariableReference> أينما حلّ كما لو أن نص العنصر <Expression> المحدد في العنصر <VariableDefinition> يحل محل العنصر <VariableReference>. وأي نظام تقييم يحافظ على هذه الدلالة مقبول. ويمكن تقييم التعبير الوارد في العنصر <VariableDefinition> مثلاً بقيمة معينة وحفظ إحالات عدة في الذاكرة دون عواقب (أي تبقى قيمة العنصر <Expression> ذاتها في تقييم كامل السياسة). وهذه الخاصة هي إحدى مزايا اللغة XACML باعتبارها لغة تصريح.

8.6.7 تقييم الحالة

تكون قيمة الحالة "صح" في حال عدم وجود العنصر <Condition> أو في حالة تقييمه بالقيمة "صح". وتكون قيمته "خطأ" إذا كانت قيمة العنصر <Condition> "خطأ". وتكون قيمة الحالة "غير محدد" إذا كانت قيمة التعبير المدرج في العنصر <Condition> "غير محدد".

9.6.7 تقييم القاعدة

للقاعدة قيمة يمكن حسابها من خلال تقييم محتوياتها. وينطوي تقييم القاعدة على تقييم منفصل لهدف القاعدة وحالتها. ويظهر جدول قيم القواعد في الجدول 7-4.

الجدول X.1142/4-7 – جدول قيم القواعد

الهدف	الحالة	قيمة القاعدة
"تقابل"	"صح"	تأثير
"تقابل"	"خطأ"	"غير صالحة"
"تقابل"	"غير محدد"	"غير محدد"
"لا تقابل"	غير هام	"غير صالحة"
"غير محدد"	غير هام	"غير محدد"

إذا كانت قيمة الهدف "لا تقابل" أو "غير محدد" فإن قيمة القاعدة تكون "غير صالح" أو "غير محدد" على التوالي، بغض النظر عن قيمة الحالة. وفي هاتين الحالتين لا حاجة لتقييم الحالة.

وإذا كانت قيمة الهدف "تقابل" وقيمة الحالة "صح"، فإن التأثير المحدد في العنصر <Rule> الشامل يحدد قيمة القاعدة.

10.6.7 تقييم السياسة

ينبغي تقييم هدف السياسة من أجل تحديد قابلية تطبيق السياسة. وإذا كانت قيمة الهدف "لا تقابل" فإن قيمة السياسة عندئذٍ تكون "غير صالح للتطبيق". أما إذا كانت قيمة الهدف "غير محدد" فإن قيمة السياسة تكون "غير محدد".

ويظهر جدول قيم السياسة في الجدول 7-5.

الجدول X.1142/5-7 – جدول قيم السياسة

الهدف	قيم القاعدة	قيمة السياسة
"تقابل"	قيمة قاعدة واحدة على الأقل هي تأثيرها	تحددها خوارزمية تجميع القاعدة
"تقابل"	جميع قيم القاعدة "غير صالحة للتطبيق"	"غير صالح"
"تقابل"	قيمة قاعدة واحدة على الأقل هي "غير محددة"	تحددها خوارزمية تجميع القاعدة
"لا تقابل"	غير هام	"غير صالح"
"غير محدد"	غير هام	"غير محدد"

تعني قيمة القاعدة "قيمة قاعدة واحدة على الأقل هي تأثيرها" أن العنصر <Rule> غير موجود أو أن قاعدة واحدة أو أكثر مدرجة في السياسة صالحة للتطبيق في طلب القرار (أي تعود مع قيمة "تأثيرها"). وينبغي استخدام القيمة "جميع قيم القاعدة" "غير صالحة للتطبيق" إذا لم تضم السياسة قاعدة قابلة للتطبيق في الطلب، وإذا لم تعد أي قاعدة مدرجة في السياسة قيمة "غير محدد". وفي حال عدم وجود أي قاعدة في السياسة قابلة للتطبيق على الطلب لكن قاعدة واحدة أو أكثر تعود مع القيمة "غير محدد"، تتخذ القواعد عندئذٍ القيمة "قيمة قاعدة واحدة على الأقل هي "غير محدد".

وإذا كانت قيمة الهدف "لا تقابل" أو "غير محدد"، تكون قيمة السياسة "غير صالح للتطبيق" أو "غير محدد" على التوالي، بغض النظر عن قيمة القواعد. وفي هاتين الحالتين لا حاجة لتقييم القواعد.

وإذا كانت قيمة الهدف "تقابل" وقيمة القاعدة "قيمة قاعدة واحدة على الأقل هي تأثيرها" أو "قيمة قاعدة واحدة على الأقل هي "غير محدد"، فإن خوارزمية تجميع القاعدة المحددة في السياسة هي التي تضع قيمة السياسة.

ويجدر بالذكر أن أياً من خوارزميات تجميع القاعدة المحددة في هذه التوصية لا تتخذ معلمات. غير أنه يمكن لخوارزميات التجميع غير المعيارية اتخاذ المعلمات.

وفي مثل هذه الحالة، يجب أن تراعى قيم هذه المعلمات المصاحبة للقواعد عند تقييم السياسة. وينبغي تعريف المعلمات وأنماطها في مواصفة خوارزمية التجميع. وفي حال توفير التنفيذ لمعلمات المجمع ووجود معلمات المجمع في السياسة، يجب توفير قيم المعلمات عندئذٍ من أجل تنفيذ خوارزمية التجميع.

11.6.7 تقييم مجموعة السياسات

تتحدد قيمة مجموعة السياسات من خلال محتوياتها في ضوء علاقتها مع محتويات سياق الطلب. ويجب تحديد قيمة مجموعة السياسات عن طريق تقييم هدف مجموعة السياسات والسياسات ومجموعات السياسات وفقاً للخوارزمية المحددة لتجميع السياسة. وإذا كانت قيمة الهدف "لا تقابل"، تكون قيمة مجموعة السياسة "غير قابلة للتطبيق". وإذا كانت قيمة الهدف "غير محدد"، يجب ضبط قيمة مجموعة السياسة على "غير محدد".

ويظهر جدول قيم مجموعة السياسة في الجدول 7-6.

الجدول X.1142/6-7 – جدول قيم مجموعة السياسات

هدف	قيم السياسة	قيم مجموعة السياسات
"تقابل"	قيمة سياسة واحدة على الأقل هي قرارها	تحددها خوارزمية تجميع السياسة
"تقابل"	جميع قيم السياسة "غير صالحة للتطبيق"	"غير صالح للتطبيق"
"تقابل"	قيمة سياسة واحدة على الأقل هي "غير محدد"	تحددها خوارزمية تجميع السياسة
"لا تقابل"	غير هام	"غير صالح للتطبيق"
"غير محدد"	غير هام	"غير محدد"

يجب استعمال قيمة السياسات "قيمة سياسة واحدة على الأقل هي قرارها" في حال عدم وجود سياسات أو مجموعة سياسات أو عدم الإحالة إليها، أو إذا كانت سياسة واحدة أو أكثر أو مجموعة سياسات واحدة أو أكثر تحتوي عليها مجموعة السياسات أو تحيل إليها قابلة للتطبيق على طلب القرار (أي تعيد قيمة تحددها خوارزمية التجميع). وتستعمل قيمة السياسات "جميع قيم السياسة غير صالحة للتطبيق" إذا لم تكن أي سياسة أو أي مجموعة سياسات تحتوي عليها مجموعة السياسة أو تحيل إليها قابلة للتطبيق على الطلب وإذا لم تعد أي سياسة أو مجموعة سياسات تحتوي عليها مجموعة السياسات أو تحيل إليها، القيمة "غير محدد". وإذا لم تكن أي سياسة أو مجموعة سياسات تحتوي عليها مجموعة السياسات قابلة للتطبيق على الطلب ولكن سياسة أو مجموعة سياسات واحدة أو أكثر تعيد قيمة "غير محدد"، فإن قيمة السياسات عندئذٍ تكون "قيمة سياسة واحدة على الأقل هي غير محدد".

إذا كانت قيمة الهدف "لا تقابل" أو "غير محدد" تكون قيمة مجموعة السياسات، "غير صالح للتطبيق" أو غير "محدد"، على التوالي مهما كانت قيمة السياسات. وفي هذه الحالة لا حاجة لتقييم السياسات.

إذا كانت قيمة الهدف "تقابل" وقيمة السياسات "قيمة سياسة واحدة على الأقل هي قرارها" أو "قيمة سياسة واحدة على الأقل "غير محدد" فإن خوارزمية تجميع السياسة المحددة في مجموعة السياسات تحدد عندئذٍ قيمة مجموعة السياسات.

ومن الجدير بالذكر أن خوارزميات تجميع السياسة المحددة في النسخة XACML 2.0 تتخذ معلمات. كما أن خوارزميات التجميع غير المعيارية تتخذ معلمات أيضاً. وفي مثل هذه الحالة، يجب مراعاة قيم هذه المعلمات المصاحبة للسياسات عند تقييم مجموعة السياسات وينبغي تعريف المعلمات وأنماطها في مواصفة خوارزمية التجميع. وإذا قدم التنفيذ معلمات المجمِّع وإذا توفرت معلمات المجمِّع في السياسة فإنه يجب توفير قيم المعلمات لتنفيذ خوارزمية التجميع.

12.6.7 موارد تراتبية

غالباً ما تنتظم الموارد وفق تراتب ما (مثل نظام الملفات، وثائق XML). وتوفر اللغة XACML عدة آليات خيارية لدعم الموارد التراتبية وفق أحكام هذه التوصية.

13.6.7 قرار الترخيص

تحدد خوارزمية تجميع السياسة ومجموعة السياسات و/أو مجموعات السياسات النقطة PDP فيما يتعلق بطلب قرار خاص. ويجب أن تعيد النقطة PDP سياق استجابة كما لو أنها قيمت مجموعة سياسات واحدة تتألف من خوارزمية تجميع السياسة هذه ومجموعة السياسات و/أو مجموعات السياسات.

ويجب أن تقيم النقطة PDP مجموعة السياسات كما يرد في الفقرتين 4.7 و6.7. ويجب أن تعيد النقطة PDP سياق الإجابة مع عنصر <Decision> واحد قيمته "مسموح" أو "مرفوض" أو "غير محدد" أو "غير صالح للتطبيق".

وإذا لم تستطع النقطة PDP اتخاذ قرار يجب إعادة عنصر <Decision> قيمته "غير محدد".

14.6.7 التزامات

قد تضم السياسة أو مجموعة السياسات التزاماً واحداً أو أكثر. وعند تقييم مثل هذه السياسة أو مجموعة السياسات، يجب عدم نقل الالتزام إلى السوية الأعلى من التقييم (السياسة الشاملة أو المحال إليها أو مجموعة السياسات أو قرار الترخيص) إلا إذا كان تأثير السياسة أو مجموعة السياسات التي يجري تقييمها متلائماً مع قيمة النعت FulfillOn للالتزام.

وينتج عن هذا الإجراء عدم إعادة أي التزام إلى النقطة PEP إذا لم تكن السياسة أو مجموعة السياسات المأخوذة منها مقيمة أو إذا كانت قيمتها "غير محدد" أو "غير صالح للتطبيق" أو إذا كان القرار الناتج عن تقييم السياسة أو مجموعة السياسات لا يلائم القرار الناتج عن تقييم مجموعة سياسات شاملة.

وإذا عُرض تقييم النقطة PDP على شكل شجرة مجموعات سياسات وسياسات تعيد كل منها القيمة "مسموح" أو "مرفوض" فإن مجموعة الالتزامات التي تعيدها النقطة PDP إلى النقطة PEP لن تضم إلاّ الالتزامات المصاحبة لتلك المسارات حيث التأثير في كل سوية تقييم هو نفس التأثير الذي تعيده النقطة PDP. وفي الحالات التي لا تقبل أي نقص بالتحديد ينبغي استعمال خوارزمية تجميع حتمي مثل خوارزميات بأولويات رفض منظم.

15.6.7 معالجة الاستثناء

تحدد اللغة XACML سلوك النقطة PDP في الحالات التالية.

1.15.6.7 وظائف غير متوفرة

إذا حاولت النقطة PDP تقييم مجموعة سياسات أو سياسة تضم نمط عنصر خياري أو وظيفة لا تتوفر في النقطة PDP يجب أن تعيد هذه النقطة قيمة "غير محدد" للعنصر <Decision>. وإذا أُعيد أيضاً عنصر <StatusCode> تكون قيمته "urn:oasis:names:tc:xacml:1.0:status:syntax-error" في حال عدم توفر نمط العنصر و"urn:oasis:names:tc:xacml:1.0:status:processing-error" في حال عدم توفر الوظيفة.

2.15.6.7 أخطاء قواعد وأنماط

إذا قيمت النقطة XACML PDP سياسة تضم قاعدة تركيب خاطئة حين استقبال طلب قرار، فإن نتيجة تلك السياسة تكون "غير محدد" مع قيمة معلمة StatusCode كالتالي:

```
"urn:oasis:names:tc:xacml:1.0:status:syntax-error"
```

إذا قيمت النقطة XACML PDP سياسة تضم أنماط معطيات إحصائية خاطئة حين استقبال طلب قرار، فإن نتيجة تلك السياسة تكون "غير محدد" مع القيمة StatusCode التالية:

```
"urn:oasis:names:tc:xacml:1.0:status:processing-error"
```

3.15.6.7 نعوت مفقودة

يؤدي غياب نعوت التقابل في سياق طلب أي مؤشرات أو منتقيات نعوت موجودة في السياسة إلى عنصر <Decision> قيمته "غير محدد". وإذا توفرت شفرة حالة في هذه الحالة، فإن القيمة:

```
"urn:oasis:names:tc:xacml:1.0:status:missing-attribute"
```

تستخدم للدلالة على الحاجة إلى مزيد من المعلومات من أجل الحصول على قرار نهائي. وقد يعدد العنصر <Status> في هذه الحالة أسماء وأنماط معطيات كل نعوت الجهات والموارد والإجراءات والبيئة التي تحتاج إليها النقطة PDP في توضيح قرارها. وقد تعيد النقطة PEP تقديم سياق طلب جهة مستعملة في إجابة على محتويات عنصر <Decision> قيمته "غير محدد" بشفرة حالة كالتالي:

```
"urn:oasis:names:tc:xacml:1.0:missing-attribute"
```

وذلك بإضافة قيم نعوت إلى أسماء النعوت التي ورد تعدادها في الإجابة المذكورة سابقاً. وعندما تعيد النقطة PDP محتويات عنصر <Decision> قيمته "غير محدد" مع شفرة الحالة التالية:

```
"urn:oasis:names:tc:xacml:1.0:missing-attribute"
```

فإنه يجب عدم تعداد أسماء أو أنماط معطيات أي نعت للموضوع أو المورد أو الإجراء أو البيئة التي تتوفر بشأنها القيم في الطلب الأصلي. ويلاحظ أن هذا الشرط يلزم النقطة PDP بإعادة قرار ترخيص بقيمة "مسموح" أو "مرفوض" أو "غير محدد" حسب الاقتضاء، مع بعض شفرات الحالة رداً على الطلبات التي يتم توضيحها على شكل مثالٍ.

7.7 نقاط توسيع اللغة XACML

تصف هذه الفقرة النقاط الواقعة في النموذج والمخطط XACML والتي يمكن فيها إضافة التوسيعات. وترد هذه الفقرة على سبيل الإعلام.

1.7.7 أنماط النعوت XML القابلة للتوسيع

قيم النعوت XML التالية هي معرفات URI. ويمكن توسيعها من خلال استحداث معرفات URI جديد مرفقة بدلالات جديدة لهذه النعوت.

- AttributeId;
- DataType;
- FunctionId;
- MatchId;
- ObligationId;
- PolicyCombiningAlgId;
- RuleCombiningAlgId;
- StatusCode;
- SubjectCategory.

2.7.7 النعوت المنينة

قد يضم العنصران <xacml:AttributeValue> و<xacml-context:AttributeValue> حالة من نمط المعطيات XML المبنينة. وفيما يلي بعض التقنيات التي تتطلب توسيعات XACML.

1) يمكن أن يحدد جماعة مستعملي اللغة XACML لأغراض نمط معطيات مبنينة معرفات نعوت جديدة لكل عنصر فرعي ورقي لنمط المعطيات المبنينة ذات النمط المطابق لأحد أنماط المعطيات البدائية المحددة في اللغة XACML. وباستعمال معرفات النعوت الجديدة هذه تستطيع النقاط PEP أو إدارات السياق التي تستخدمها هذه الجماعة من المستعملين أن تسوي حالات نمط المعطيات المبنينة وتحولها إلى تتابع من العناصر <Attribute> المتفرقة. ويمكن مقارنة كل عنصر <Attribute> باستعمال الوظائف المحددة في اللغة XACML. وعند استعمال هذه الطريقة لا يظهر نمط المعطيات المبنينة ذاته أبداً في عنصر <xacml-context:AttributeValue>.

2) يمكن أن تحدد جماعة مستعملي اللغة XACML وظيفة جديدة تستعمل لمقارنة قيمة نمط معطيات مبنينة بقيمة أخرى. ولا تستخدم هذه الطريقة إلاّ في النقاط PDP التي توفر الوظيفة الجديدة.

8.7 المطابقة

تحدد اللغة XACML عدداً من الوظائف ذات التطبيق الخاص بعض الشيء، والتي لا يُطلب توفيرها في تطبيق يزعم المطابقة مع هذه التوصية.

وتعدد هذه الفقرة أجزاء هذه التوصية التي يتوجب إدراجها في تطبيق نقطة PDP تزعم المطابقة مع النسخة XACML v2.0.

ملاحظة - "M" تعني إلزامي للتطبيق، و"O" تعني خياري.

1.8.7 عناصر المخطط

يجب أن يوفر التطبيق عناصر المخطط المشار إليها بالحرف "M".

اسم العنصر	M/O
xacml-context:Action	M
xacml-context:Attribute	M
xacml-context:AttributeValue	M
xacml-context:Decision	M
xacml-context:Environment	M
xacml-context:MissingAttributeDetail	M
xacml-context:Obligations	O
xacml-context:Request	M
xacml-context:Resource	M
xacml-context:ResourceContent	O
xacml-context:Response	M
xacml-context:Result	M
xacml-context:Status	M
xacml-context:StatusCode	M
xacml-context:StatusDetail	O
xacml-context:StatusMessage	O
xacml-context:Subject	M
xacml:Action	M
xacml:ActionAttributeDesignator	M

اسم العنصر	M/O
xacml:ActionMatch	M
xacml:Actions	M
xacml:Apply	M
xacml:AttributeAssignment	O
xacml:AttributeSelector	O
xacml:AttributeValue	M
xacml:CombinerParameters	O
xacml:CombinerParameter	O
xacml:Condition	M
xacml:Description	M
xacml:Environment	M
xacml:EnvironmentMatch	M
xacml:EnvironmentAttributeDesignator	M
xacml:Environments	M
xacml:Expression	M
xacml:Function	M
xacml:Obligation	O
xacml:Obligations	O
xacml:Policy	M
xacml:PolicyCombinerParameters	O
xacml:PolicyDefaults	O
xacml:PolicyIdReference	M
xacml:PolicySet	M
xacml:PolicySetDefaults	O
xacml:PolicySetIdReference	M
xacml:Resource	M
xacml:ResourceAttributeDesignator	M
xacml:ResourceMatch	M
xacml:Resources	M
xacml:Rule	M
xacml:RuleCombinerParameters	O
xacml:Subject	M
xacml:SubjectMatch	M
xacml:Subjects	M
xacml:Target	M
xacml:VariableDefinition	M
xacml:VariableReference	M
xacml:XPathVersion	O

2.8.7 سوابق معرفات الهوية

فيما يلي سوابق معرفات الهوية المحجوزة للغة XACML.

معرف الهوية
urn:oasis:names:tc:xacml:2.0
urn:oasis:names:tc:xacml:2.0:conformance-test
urn:oasis:names:tc:xacml:2.0:context
urn:oasis:names:tc:xacml:2.0:example
urn:oasis:names:tc:xacml:1.0:function
urn:oasis:names:tc:xacml:2.0:function
urn:oasis:names:tc:xacml:2.0:policy
urn:oasis:names:tc:xacml:1.0:subject
urn:oasis:names:tc:xacml:1.0:resource
urn:oasis:names:tc:xacml:1.0:action
urn:oasis:names:tc:xacml:1.0:environment
urn:oasis:names:tc:xacml:1.0:status

3.8.7 الخوارزميات

يجب أن يدرج التطبيق خوارزميات تجميع القاعدة والسياسة مع معرفات الهوية التالية المشار إليها بالحرف "M".

الخوارزمية	M/O
urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides	M
urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides	M
urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides	M
urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides	M
urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable	M
urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:first-applicable	M
urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:only-one-applicable	M
urn:oasis:names:tc:xacml:1.1:rule-combining-algorithm:ordered-deny-overrides	M
urn:oasis:names:tc:xacml:1.1:policy-combining-algorithm:ordered-deny-overrides	M
urn:oasis:names:tc:xacml:1.1:rule-combining-algorithm:ordered-permit-overrides	M
urn:oasis:names:tc:xacml:1.1:policy-combining-algorithm:ordered-permit-overrides	M

4.8.7 شفرات الحالة

توفير التطبيقات للعنصر <StatusCode> خياري لكن في حال توفيره، يجب توفير شفرات الحالة التالية واستعمالها حسب الطريقة التي تحددها اللغة XACML.

معرف الهوية	M/O
urn:oasis:names:tc:xacml:1.0:status:missing-attribute	M
urn:oasis:names:tc:xacml:1.0:status:ok	M
urn:oasis:names:tc:xacml:1.0:status:processing-error	M
urn:oasis:names:tc:xacml:1.0:status:syntax-error	M

5.8.7 النعوت

يجب أن توفر التطبيقات النعوت المصاحبة للمعرفات التالية كما تحددها اللغة XACML. وفي حال عدم وجود قيم هذه النعوت في طلب القرار يجب أن توفر إدارة السياق هذه القيم. وعلى عكس معظم النعوت الأخرى، لا تظهر دلالاتها للنقطة PDP.

معرف الهوية	M/O
urn:oasis:names:tc:xacml:1.0:environment:current-time	M
urn:oasis:names:tc:xacml:1.0:environment:current-date	M
urn:oasis:names:tc:xacml:1.0:environment:current-dateTime	M

6.8.7 معرفات الهوية

يجب أن تستخدم التطبيقات النعوت المصاحبة لمعرفات الهوية التالية حسب الطريقة المحددة في اللغة XACML. ويستهدف هذا الشرط خاصة النقطة PAP أو PEP التي تستخدم اللغة XACML طالما كانت دلالات النعوت ظاهرة للنقطة PDP.

معرف الهوية	M/O
urn:oasis:names:tc:xacml:1.0:subject:authn-locality:dns-name	O
urn:oasis:names:tc:xacml:1.0:subject:authn-locality:ip-address	O
urn:oasis:names:tc:xacml:1.0:subject:authentication-method	O
urn:oasis:names:tc:xacml:1.0:subject:authentication-time	O
urn:oasis:names:tc:xacml:1.0:subject:key-info	O
urn:oasis:names:tc:xacml:1.0:subject:request-time	O
urn:oasis:names:tc:xacml:1.0:subject:session-start-time	O
urn:oasis:names:tc:xacml:1.0:subject:subject-id	O
urn:oasis:names:tc:xacml:1.0:subject:subject-id-qualifier	O
urn:oasis:names:tc:xacml:1.0:subject-category:access-subject	M
urn:oasis:names:tc:xacml:1.0:subject-category:codebase	O
urn:oasis:names:tc:xacml:1.0:subject-category:intermediary-subject	O
urn:oasis:names:tc:xacml:1.0:subject-category:recipient-subject	O
urn:oasis:names:tc:xacml:1.0:subject-category:requesting-machine	O
urn:oasis:names:tc:xacml:1.0:resource:resource-location	O
urn:oasis:names:tc:xacml:1.0:resource:resource-id	M
urn:oasis:names:tc:xacml:1.0:resource:simple-file-name	O
urn:oasis:names:tc:xacml:1.0:action:action-id	O
urn:oasis:names:tc:xacml:1.0:action:implied-action	O

7.8.7 أنماط المعطيات

يجب أن توفر التطبيقات أنماط المعطيات المصاحبة لمعرفات الهوية التالية المشار إليها بالحرف "M".

نمط المعطيات	M/O
http://www.w3.org/2001/XMLSchema#string	M
http://www.w3.org/2001/XMLSchema#boolean	M
http://www.w3.org/2001/XMLSchema#integer	M
http://www.w3.org/2001/XMLSchema#double	M
http://www.w3.org/2001/XMLSchema#time	M
http://www.w3.org/2001/XMLSchema#date	M
http://www.w3.org/2001/XMLSchema#dateTime	M
urn:oasis:names:tc:xacml:2.0:data-types:dayTimeDuration	M
urn:oasis:names:tc:xacml:2.0:data-types:yearMonthDuration	M
http://www.w3.org/2001/XMLSchema#anyURI	M
http://www.w3.org/2001/XMLSchema#hexBinary	M
http://www.w3.org/2001/XMLSchema#base64Binary	M
urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name	M
urn:oasis:names:tc:xacml:1.0:data-type:x500Name	M

8.8.7 الوظائف

يجب أن تعالج التطبيقات جيداً الوظائف المصاحبة لمعرفات الهوية المشار إليها بالحرف "M".

الوظيفة	M/O
urn:oasis:names:tc:xacml:1.0:function:string-equal	M
urn:oasis:names:tc:xacml:1.0:function:boolean-equal	M
urn:oasis:names:tc:xacml:1.0:function:integer-equal	M
urn:oasis:names:tc:xacml:1.0:function:double-equal	M
urn:oasis:names:tc:xacml:1.0:function:date-equal	M
urn:oasis:names:tc:xacml:1.0:function:time-equal	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-equal	M
urn:oasis:names:tc:xacml:1.0:function:dayTimeDuration-equal	M
urn:oasis:names:tc:xacml:1.0:function:yearMonthDuration-equal	M
urn:oasis:names:tc:xacml:1.0:function:anyURI-equal	M
urn:oasis:names:tc:xacml:1.0:function:x500Name-equal	M
urn:oasis:names:tc:xacml:1.0:function:rfc822Name-equal	M
urn:oasis:names:tc:xacml:1.0:function:hexBinary-equal	M
urn:oasis:names:tc:xacml:1.0:function:base64Binary-equal	M
urn:oasis:names:tc:xacml:1.0:function:integer-add	M
urn:oasis:names:tc:xacml:1.0:function:double-add	M
urn:oasis:names:tc:xacml:1.0:function:integer-subtract	M
urn:oasis:names:tc:xacml:1.0:function:double-subtract	M
urn:oasis:names:tc:xacml:1.0:function:integer-multiply	M
urn:oasis:names:tc:xacml:1.0:function:double-multiply	M
urn:oasis:names:tc:xacml:1.0:function:integer-divide	M
urn:oasis:names:tc:xacml:1.0:function:double-divide	M
urn:oasis:names:tc:xacml:1.0:function:integer-mod	M
urn:oasis:names:tc:xacml:1.0:function:integer-abs	M
urn:oasis:names:tc:xacml:1.0:function:double-abs	M
urn:oasis:names:tc:xacml:1.0:function:round	M
urn:oasis:names:tc:xacml:1.0:function:floor	M
urn:oasis:names:tc:xacml:1.0:function:string-normalize-space	M
urn:oasis:names:tc:xacml:1.0:function:string-normalize-to-lower-case	M
urn:oasis:names:tc:xacml:1.0:function:double-to-integer	M
urn:oasis:names:tc:xacml:1.0:function:integer-to-double	M
urn:oasis:names:tc:xacml:1.0:function:or	M
urn:oasis:names:tc:xacml:1.0:function:and	M
urn:oasis:names:tc:xacml:1.0:function:n-of	M
urn:oasis:names:tc:xacml:1.0:function:not	M
urn:oasis:names:tc:xacml:1.0:function:integer-greater-than	M

الوظيفة	M/O
urn:oasis:names:tc:xacml:1.0:function:integer-greater-than-or-equal	M
urn:oasis:names:tc:xacml:1.0:function:integer-less-than	M
urn:oasis:names:tc:xacml:1.0:function:integer-less-than-or-equal	M
urn:oasis:names:tc:xacml:1.0:function:double-greater-than	M
urn:oasis:names:tc:xacml:1.0:function:double-greater-than-or-equal	M
urn:oasis:names:tc:xacml:1.0:function:double-less-than	M
urn:oasis:names:tc:xacml:1.0:function:double-less-than-or-equal	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-add-dayTimeDuration	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-add-yearMonthDuration	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-subtract-dayTimeDuration	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-subtract-yearMonthDuration	M
urn:oasis:names:tc:xacml:1.0:function:date-add-yearMonthDuration	M
urn:oasis:names:tc:xacml:1.0:function:date-subtract-yearMonthDuration	M
urn:oasis:names:tc:xacml:1.0:function:string-greater-than	M
urn:oasis:names:tc:xacml:1.0:function:string-greater-than-or-equal	M
urn:oasis:names:tc:xacml:1.0:function:string-less-than	M
urn:oasis:names:tc:xacml:1.0:function:string-less-than-or-equal	M
urn:oasis:names:tc:xacml:1.0:function:time-greater-than	M
urn:oasis:names:tc:xacml:1.0:function:time-greater-than-or-equal	M
urn:oasis:names:tc:xacml:1.0:function:time-less-than	M
urn:oasis:names:tc:xacml:1.0:function:time-less-than-or-equal	M
urn:oasis:names:tc:xacml:2.0:function:time-in-range	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-greater-than	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-greater-than-or-equal	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-less-than	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-less-than-or-equal	M
urn:oasis:names:tc:xacml:1.0:function:date-greater-than	M
urn:oasis:names:tc:xacml:1.0:function:date-greater-than-or-equal	M
urn:oasis:names:tc:xacml:1.0:function:date-less-than	M
urn:oasis:names:tc:xacml:1.0:function:date-less-than-or-equal	M
urn:oasis:names:tc:xacml:1.0:function:string-one-and-only	M
urn:oasis:names:tc:xacml:1.0:function:string-bag-size	M
urn:oasis:names:tc:xacml:1.0:function:string-is-in	M
urn:oasis:names:tc:xacml:1.0:function:string-bag	M
urn:oasis:names:tc:xacml:1.0:function:boolean-one-and-only	M
urn:oasis:names:tc:xacml:1.0:function:boolean-bag-size	M
urn:oasis:names:tc:xacml:1.0:function:boolean-is-in	M
urn:oasis:names:tc:xacml:1.0:function:boolean-bag	M
urn:oasis:names:tc:xacml:1.0:function:integer-one-and-only	M
urn:oasis:names:tc:xacml:1.0:function:integer-bag-size	M
urn:oasis:names:tc:xacml:1.0:function:integer-is-in	M
urn:oasis:names:tc:xacml:1.0:function:integer-bag	M
urn:oasis:names:tc:xacml:1.0:function:double-one-and-only	M
urn:oasis:names:tc:xacml:1.0:function:double-bag-size	M
urn:oasis:names:tc:xacml:1.0:function:double-is-in	M
urn:oasis:names:tc:xacml:1.0:function:double-bag	M
urn:oasis:names:tc:xacml:1.0:function:time-one-and-only	M
urn:oasis:names:tc:xacml:1.0:function:time-bag-size	M
urn:oasis:names:tc:xacml:1.0:function:time-is-in	M
urn:oasis:names:tc:xacml:1.0:function:time-bag	M
urn:oasis:names:tc:xacml:1.0:function:date-one-and-only	M
urn:oasis:names:tc:xacml:1.0:function:date-bag-size	M
urn:oasis:names:tc:xacml:1.0:function:date-is-in	M
urn:oasis:names:tc:xacml:1.0:function:date-bag	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-one-and-only	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-bag-size	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-is-in	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-bag	M
urn:oasis:names:tc:xacml:1.0:function:anyURI-one-and-only	M

الوظيفة	M/O
urn:oasis:names:tc:xacml:1.0:function:anyURI-bag-size	M
urn:oasis:names:tc:xacml:1.0:function:anyURI-is-in	M
urn:oasis:names:tc:xacml:1.0:function:anyURI-bag	M
urn:oasis:names:tc:xacml:1.0:function:hexBinary-one-and-only	M
urn:oasis:names:tc:xacml:1.0:function:hexBinary-bag-size	M
urn:oasis:names:tc:xacml:1.0:function:hexBinary-is-in	M
urn:oasis:names:tc:xacml:1.0:function:hexBinary-bag	M
urn:oasis:names:tc:xacml:1.0:function:base64Binary-one-and-only	M
urn:oasis:names:tc:xacml:1.0:function:base64Binary-bag-size	M
urn:oasis:names:tc:xacml:1.0:function:base64Binary-is-in	M
urn:oasis:names:tc:xacml:1.0:function:base64Binary-bag	M
urn:oasis:names:tc:xacml:1.0:function:dayTimeDuration-one-and-only	M
urn:oasis:names:tc:xacml:1.0:function:dayTimeDuration-bag-size	M
urn:oasis:names:tc:xacml:1.0:function:dayTimeDuration-is-in	M
urn:oasis:names:tc:xacml:1.0:function:dayTimeDuration-bag	M
urn:oasis:names:tc:xacml:1.0:function:yearMonthDuration-one-and-only	M
urn:oasis:names:tc:xacml:1.0:function:yearMonthDuration-bag-size	M
urn:oasis:names:tc:xacml:1.0:function:yearMonthDuration-is-in	M
urn:oasis:names:tc:xacml:1.0:function:yearMonthDuration-bag	M
urn:oasis:names:tc:xacml:1.0:function:x500Name-one-and-only	M
urn:oasis:names:tc:xacml:1.0:function:x500Name-bag-size	M
urn:oasis:names:tc:xacml:1.0:function:x500Name-is-in	M
urn:oasis:names:tc:xacml:1.0:function:x500Name-bag	M
urn:oasis:names:tc:xacml:1.0:function:rfc822Name-one-and-only	M
urn:oasis:names:tc:xacml:1.0:function:rfc822Name-bag-size	M
urn:oasis:names:tc:xacml:1.0:function:rfc822Name-is-in	M
urn:oasis:names:tc:xacml:1.0:function:rfc822Name-bag	M
urn:oasis:names:tc:xacml:2.0:function:string-concatenate	M
urn:oasis:names:tc:xacml:2.0:function:uri-string-concatenate	M
urn:oasis:names:tc:xacml:1.0:function:any-of	M
urn:oasis:names:tc:xacml:1.0:function:all-of	M
urn:oasis:names:tc:xacml:1.0:function:any-of-any	M
urn:oasis:names:tc:xacml:1.0:function:all-of-any	M
urn:oasis:names:tc:xacml:1.0:function:any-of-all	M
urn:oasis:names:tc:xacml:1.0:function:all-of-all	M
urn:oasis:names:tc:xacml:1.0:function:map	M
urn:oasis:names:tc:xacml:1.0:function:x500Name-match	M
urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match	M
urn:oasis:names:tc:xacml:1.0:function:string-regexp-match	M
urn:oasis:names:tc:xacml:2.0:function:anyURI-regexp-match	M
urn:oasis:names:tc:xacml:2.0:function:ipAddress-regexp-match	M
urn:oasis:names:tc:xacml:2.0:function:dnsName-regexp-match	M
urn:oasis:names:tc:xacml:2.0:function:rfc822Name-regexp-match	M
urn:oasis:names:tc:xacml:2.0:function:x500Name-regexp-match	M
urn:oasis:names:tc:xacml:1.0:function:xpath-node-count	O
urn:oasis:names:tc:xacml:1.0:function:xpath-node-equal	O
urn:oasis:names:tc:xacml:1.0:function:xpath-node-match	O
urn:oasis:names:tc:xacml:1.0:function:string-intersection	M
urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of	M
urn:oasis:names:tc:xacml:1.0:function:string-union	M
urn:oasis:names:tc:xacml:1.0:function:string-subset	M
urn:oasis:names:tc:xacml:1.0:function:string-set-equals	M
urn:oasis:names:tc:xacml:1.0:function:boolean-intersection	M
urn:oasis:names:tc:xacml:1.0:function:boolean-at-least-one-member-of	M
urn:oasis:names:tc:xacml:1.0:function:boolean-union	M
urn:oasis:names:tc:xacml:1.0:function:boolean-subset	M
urn:oasis:names:tc:xacml:1.0:function:boolean-set-equals	M
urn:oasis:names:tc:xacml:1.0:function:integer-intersection	M
urn:oasis:names:tc:xacml:1.0:function:integer-at-least-one-member-of	M

الوظيفة	M/O
urn:oasis:names:tc:xacml:1.0:function:integer-union	M
urn:oasis:names:tc:xacml:1.0:function:integer-subset	M
urn:oasis:names:tc:xacml:1.0:function:integer-set-equals	M
urn:oasis:names:tc:xacml:1.0:function:double-intersection	M
urn:oasis:names:tc:xacml:1.0:function:double-at-least-one-member-of	M
urn:oasis:names:tc:xacml:1.0:function:double-union	M
urn:oasis:names:tc:xacml:1.0:function:double-subset	M
urn:oasis:names:tc:xacml:1.0:function:double-set-equals	M
urn:oasis:names:tc:xacml:1.0:function:time-intersection	M
urn:oasis:names:tc:xacml:1.0:function:time-at-least-one-member-of	M
urn:oasis:names:tc:xacml:1.0:function:time-union	M
urn:oasis:names:tc:xacml:1.0:function:time-subset	M
urn:oasis:names:tc:xacml:1.0:function:time-set-equals	M
urn:oasis:names:tc:xacml:1.0:function:date-intersection	M
urn:oasis:names:tc:xacml:1.0:function:date-at-least-one-member-of	M
urn:oasis:names:tc:xacml:1.0:function:date-union	M
urn:oasis:names:tc:xacml:1.0:function:date-subset	M
urn:oasis:names:tc:xacml:1.0:function:date-set-equals	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-intersection	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-at-least-one-member-of	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-union	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-subset	M
urn:oasis:names:tc:xacml:1.0:function:dateTime-set-equals	M
urn:oasis:names:tc:xacml:1.0:function:anyURI-intersection	M
urn:oasis:names:tc:xacml:1.0:function:anyURI-at-least-one-member-of	M
urn:oasis:names:tc:xacml:1.0:function:anyURI-union	M
urn:oasis:names:tc:xacml:1.0:function:anyURI-subset	M
urn:oasis:names:tc:xacml:1.0:function:anyURI-set-equals	M
urn:oasis:names:tc:xacml:1.0:function:hexBinary-intersection	M
urn:oasis:names:tc:xacml:1.0:function:hexBinary-at-least-one-member-of	M
urn:oasis:names:tc:xacml:1.0:function:hexBinary-union	M
urn:oasis:names:tc:xacml:1.0:function:hexBinary-subset	M
urn:oasis:names:tc:xacml:1.0:function:hexBinary-set-equals	M
urn:oasis:names:tc:xacml:1.0:function:base64Binary-intersection	M
urn:oasis:names:tc:xacml:1.0:function:base64Binary-at-least-one-member-of	M
urn:oasis:names:tc:xacml:1.0:function:base64Binary-union	M
urn:oasis:names:tc:xacml:1.0:function:base64Binary-subset	M
urn:oasis:names:tc:xacml:1.0:function:base64Binary-set-equals	M
urn:oasis:names:tc:xacml:1.0:function:dayTimeDuration-intersection	M
urn:oasis:names:tc:xacml:1.0:function:dayTimeDuration-at-least-one-member-of	M
urn:oasis:names:tc:xacml:1.0:function:dayTimeDuration-union	M
urn:oasis:names:tc:xacml:1.0:function:dayTimeDuration-subset	M
urn:oasis:names:tc:xacml:1.0:function:dayTimeDuration-set-equals	M
urn:oasis:names:tc:xacml:1.0:function:yearMonthDuration-intersection	M
urn:oasis:names:tc:xacml:1.0:function:yearMonthDuration-at-least-one-member-of	M
urn:oasis:names:tc:xacml:1.0:function:yearMonthDuration-union	M
urn:oasis:names:tc:xacml:1.0:function:yearMonthDuration-subset	M
urn:oasis:names:tc:xacml:1.0:function:yearMonthDuration-set-equals	M
urn:oasis:names:tc:xacml:1.0:function:x500Name-intersection	M
urn:oasis:names:tc:xacml:1.0:function:x500Name-at-least-one-member-of	M
urn:oasis:names:tc:xacml:1.0:function:x500Name-union	M
urn:oasis:names:tc:xacml:1.0:function:x500Name-subset	M
urn:oasis:names:tc:xacml:1.0:function:x500Name-set-equals	M
urn:oasis:names:tc:xacml:1.0:function:rfc822Name-intersection	M
urn:oasis:names:tc:xacml:1.0:function:rfc822Name-at-least-one-member-of	M
urn:oasis:names:tc:xacml:1.0:function:rfc822Name-union	M
urn:oasis:names:tc:xacml:1.0:function:rfc822Name-subset	M
urn:oasis:names:tc:xacml:1.0:function:rfc822Name-set-equals	M

8 صفات التحكم في النفاذ القائم على الدور المركزي والتراتبي

تعرف هذه الفقرة مواصفات لاستعمال اللغة XACML بهدف الوفاء بمتطلبات التحكم في النفاذ القائم على الدور (RBAC) "المركزي" و"التراتبي".

1.8 معلومات أساسية عن التحكم RBAC

ترد هذه الفقرة على سبيل الإعلام.

وتعرف هذه الفقرة مواصفة تستعمل مع اللغة XACML من أجل الوفاء بمتطلبات التحكم في النفاذ القائم على الدور "المركزي" و"التراتبي" (RBAC).

ملاحظة – للحصول على معلومة عن التحكم RBAC راجع المرجع (RBAC).

1.1.8 نطاق التطبيق

يتيح التحكم في النفاذ القائم على الدور للسياسات أن تتحدد تبعاً لأدوار الجهات المستعملة بدلاً من هوياتها الفردية، وذلك هام لأغراض القياس والإدارة في أنظمة التحكم بالنفاذ.

والسياسات المحددة في هذه المواصفة قادرة على الإجابة على ثلاثة أنواع من الأسئلة هي:

1) إذا كان للجهة المستعملة أدوار R_1، R_2، ... R_n نشطة، هل تتمكن الجهة X من النفاذ إلى مورد معين باستعمال إجراء معين؟
2) هل من المسموح للجهة المستعملة X أن يكون لها دور R_i منشط؟
3) إذا كان للجهة المستعملة أدوار R_1، R_2، ... R_n منشطة، هل يعني ذلك أنها ستحصل على تراخيص مصاحبة للدور 'R'؟ وفي هذه الحالة، هل الدور 'R مساوٍ للأدوار R_1، R_2، ... R_n أو *أصغر (junior)* منها؟

ولا تجيب الأسئلة المحددة في هذه المواصفة على السؤال "ما هي مجموعة أدوار الموضوع X؟". ويجب معالجة هذا السؤال من طرف سلطة تنشيط وليس مباشرة من طرف النقطة XACML PDP. ويمكن لمثل هذا الكيان أن يستخدم السياسات XACML ولكنه سيحتاج إلى معلومات إضافية لذلك.

وتضطلع السياسات المحددة في هذه المواصفة بجميع الأدوار التي نشطتها جهة مستعملة معينة عند طلب قرار الترخيص. وهي لا تتعامل مع بيئة يجب فيها تنشيط الأدوار دينامياً استناداً إلى مورد أو إجراءات تحاول جهة ما الحصول عليها أو القيام بها. ولهذا السبب لا تعالج السياسات المحددة في هذه المواصفة "فصل المهام" السكوني أو الدينامي. وقد تتناول مواصفة أخرى متطلبات هذا النوع من البيئة.

2.1.8 الدور

يعبر عن الأدوار في هذه التوصية على أنها نعوت جهة مستعملة XACML. وثمة استثناءان هما حالة تخصيص الدور في العنصر <PolicySet> أو <Policy> وحالة <Policy> HasPrivilegesOfRole، حيث يظهر الدور كنعت مورد.

ويمكن التعبير عن نعوت الدور بإحدى طريقتين تبعاً لمتطلبات بيئة التطبيق. ففي بعض البيئات يوجد عدد ضئيل من "نعوت الدور" حيث يكون اسم كل نعت منها هو اسم ما يدل على "دور" وحيث قيمة كل نعت منها يدل على اسم الدور القائم. على سبيل المثال في أول نوع بيئة يوجد "نعت دور" واحد له AttributeId و"&role;" (توصي هذه المواصفة باستعمال هذا المعرف). والمواضيع الممكنة هي قيم هذا النعت الواحد، التي قد تكون "&roles;officer" و"&roles;manager" و"&roles;employee". وتعمل طريقة التعبير هذه على نحو أفضل مع الطريقة XACML لسياسات التعبير. كما أن هذه الطريقة لتحديد الأدوار أكثر ملاءمة لقابلية التشغيل البيني.

ومن ناحية أخرى يوجد في بيئات تطبيق أخرى عدد من معرفات هويات النعوت المختلفة يدل كل منها على دور مختلف. ففي هذا النوع من البيئة مثلاً، قد يوجد ثلاثة معرفات نعت هي: "urn:someapp:attributes:officer-role"، "urn:someapp:attributes:manager-role" و"urn:someapp:attributes:employee-role". وقد تكون قيمة النعت في هذه الحالة فارغة أو قد تضم معلمات مختلفة مصاحبة للدور. وتستطيع السياسات XACML الاضطلاع بالأدوار المعبر عنها بهذه الطريقة ولكن ليس بنفس القدر من السهولة المتوفرة في الطريقة الأولى.

وتدعم اللغة XACML عدة جهات مستعملة لكل طلب نفاذ وتشير إلى كيانات مختلفة قد تدخل في صياغة الطلب. فهناك عادة على سبيل المثال شخص مستعمل يبدأ الطلب بشكل غير مباشر على الأقل. وهناك عادة تطبيق واحد أو أكثر أو قاعدة شفرات واحدة أو أكثر تولد طلب النفاذ منخفض السوية الفعلي إنابةً عن المستعمل. وهناك بعض جهاز حاسوبي يُنفذ فيه التطبيقات أو قواعد الشفرة، وقد يكون لهذا الجهاز هوية كعنوان IP مثلاً. وتحدد اللغة XACML كل جهة من هذا القبيل باستعمال نعت xml SubjectCategory يدل على نوع الجهة الموصوفة. فمثلاً، يكون للشخص المستعمل نعت SubjectCategory بالقيمة &subject-category؛ access-subject (وهي

فئة التغيب)؛ وللتطبيق الذي يولد طلب النفاذ الفئة SubjectCategory للعنصر subject-category&؛ codebase وهكذا دواليك. ويمكن في هذه المواصفة إرفاق نعت دور بأي فئة جهة منخرطة في صياغة طلب النفاذ.

3.1.8 السياسات

تحدد هذه التوصية أربعة أنواع من السياسات هي:

1) **دور** <PolicySet> أو **RPS**: وهي <PolicySet> تجمع بين حملة نعت دور معين وقيمة رخصة <PolicySet> تضم الرخص الفعلية المصاحبة للدور المعين. ويحد العنصر <Target> للدور <PolicySet> من قابلية تطبيق <PolicySet> على جهات تحمل نعت الدور المصاحب وقيمته. ويحيل كل دور <PolicySet> إلى رخصة <PolicySet> مقابلة واحدة ولكنه لا يضم أي عنصر <Policy> أو <PolicySet> آخر ولا يحيل إليه.

2) **رخصة** <PolicySet> أو **PPS**: وهي <PolicySet> تضم الرخص الفعلية المصاحبة لدور معين. وتضم عناصر <Policy> و<Rules> تصف الموارد والإجراءات المسموح للجهات بالنفاذ إليها مرفقةً بجميع الشروط الإضافية بأن ذلك النفاذ مثل تحديد ساعات الاستعمال. وقد تضم رخصة <PolicySet> أيضاً إحالات إلى رخصة <PolicySet> مصاحبة لأدوار أخرى تابعة للدور المعين متيحة بذلك للرخصة <PolicySet> أن ترث الرخص المصاحبة للدور الذي تحيل إليه الرخصة <PolicySet>. ويجب ألا يقتصر العنصر <Target> للرخصة <PolicySet> في حال وجوده على الجهات التي ينطبق عليها العنصر <PolicySet>.

3) **توزيع الأدوار** <Policy> أو <PolicySet>: وهي <Policy> أو <PolicySet> تحدد الأدوار التي يمكن تفعيلها أو توزيعها على الجهات المحددة. وقد تحدد أيضاً التقييدات المفروضة على تجميع الأدوار أو مجموع عدد الأدوار الموزعة على جهة ما أو المنشَّطة من أجله. وتستخدم سلطة التنشيط هذا النوع من السياسة. أما استعمال تخصيص <Policy> أو <PolicySet> فهو أمر خياري.

4) العنصر <Policy> **HasPrivilegesOfRole**: وهو سياسة <Policy> ضمن رخصة <PolicySet> تتولى معالجة الطلبات من خلال طرح سؤال لمعرفة ما إذا كانت جهة ما تتمتع بامتيازات مرفقة بدور معين. فإذا توفر هذا النوع من الطلب توجب عندئذٍ إدراج HasPrivilegesOfRole <Policy> في كل رخصة <PolicySet>. وتوفير هذا النمط من السياسات أي معرفة ما إذا كانت جهة ما تتمتع بامتيازات مرفقة بدورها، أمر خياري.

وينبغي تخزين حالات رخصة <PolicySet> في مستودع السياسة على نحو يتعذر فيه استعمالها كسياسة أولية لنقطة XACML PDP؛ وينبغي ألاّ يكون النفاذ إلى حالات رخصة <PolicySet> إلاّ من خلال الدور المقابل <PolicySet>. وذلك لأنه من أجل توفير أدوار تراتبية يجب أن تنطبق رخصة <PolicySet> على كل جهة. وترتبط الرخصة <PolicySet> بالدور المقابل لها <PolicySet> من أجل ضمان عدم السماح إلاّ لحملة نعت الدور المقابل بالنفاذ إلى الحيز المسموح في رخصة <PolicySet> معينة.

ويتيح استعمال حالات دور <PolicySet> ورخصة <PolicySet> منفصلة توفير التحكم RBAC التراتبي حيث يتمكن الدور *الأكبر* من الحصول على رخص من الدور *الأصغر*. ويمكن لرخصة <PolicySet> لا تحيل إلى عناصر رخصة <PolicySet> أخرى أن تكون بالحقيقة <Policy> XACML وليس <PolicySet>. غير أن اشتراط أن تكون <PolicySet> يتيح للدور المصاحب أن يصبح جزءاً من تراتب الأدوار في وقت لاحق دون أن يستدعي ذلك أي تغيير في السياسات الأخرى.

4.1.8 رخص متعددة الأدوار

من الممكن في هذه المواصفة الكلام عن سياسات يتعين على المستعمل فيها أن يتزود بعدة أدوار في نفس الوقت من أجل التوصل إلى النفاذ إلى بعض الرخص. على سبيل المثال، يتطلب تغيير التعليمات الطبية لمريض في المستشفى أن يكون للشخص الذي يضطلع بالإجراء دور الطبيب ودور الموظف في آن واحد.

ويمكن الكلام عن هذه السياسات باستعمال دور <PolicySet> حيث يتطلب العنصر <Target> من الجهات المستعملة Subject أن تزوده بجميع نعوت الأدوار الضرورية. وذلك ممكن من خلال استعمال عنصر <Subject> واحد يحتوي على عدة عناصر <SubjectMatch>. وينبغي أن تحدد الرخصة <PolicySet> المصاحبة عناصر Subjects الرخصة المصاحبة للجهات المستعملة المزودة بجميع الأدوار المحددة النشطة معاً.

وقد تحيل الرخصة <PolicySet> المصاحبة لسياسة متعددة الأدوار إلى حالات الرخصة <PolicySet> المصاحبة لأدوار أخرى مما قد ينتج تلقي رخص من أدوار أخرى. وقد يمنح دور آخر للرخص المصاحبة لعنصر <PolicySet> متعدد الأدوار معين إذا ضم الدور الآخر إحالة إلى الرخصة <PolicySet> المصاحبة للسياسة متعددة الأدوار في رخصتها الخاصة <PolicySet>.

2.8 مثال للتحكم RBAC

ترد هذه الفقرة على سبيل الإعلام.

وتقدم هذه الفقرة مثالاً كاملاً لأنواع السياسات المصاحبة للتحكم في النفاذ القائم على الدور (RBAC).

لنفترض أن تنظيماً ما يؤدي دورين: إداري (manager) وموظف (employee). ويعبر عن الدورين في هذا المثال بأنهما قيمتان لنعت XACML واحد مع AttributeId "&role;". وقيمتا النعت &role؛ المقابلتان للدورين المذكورين هما "&roles;employee" و"&roles;manager". ويسمح للموظف باستحداث أمر شراء. ويسمح للإداري بتوقيع أمر الشراء إضافةً لأي رخصة مصاحبة لدور الموظف. وبالتالي يكون دور الإداري أكبر من دور الموظف ودور الموظف أصغر من دور الإداري.

ووفقاً لهذه المواصفة توجد حالتا "سماح" <PolicySet> : واحدة لدور الإداري والأخرى لدور الموظف. وستعطي "سماح" الإداري <PolicySet> لأي موضوع Subject السماح الخاص ليوقع أمر شراء وحيل إلى "سماح" الموظف <PolicySet> لكي يتلقى ما تبقى له من قيم سماح. وسيعطي سماح الموظف <PolicySet> لأي موضوع Subject سماحاً لاستصدار أمر شراء.

ووفقاً لهذه المواصفة، ستوجد أيضاً حالتا دور <PolicySet>: واحدة لدور الإداري والأخرى لدور الموظف. وسيضم دور الإداري <PolicySet> عنصر <Target> يتطلب إعطاء الجهة المستعملة نعت &role؛ مع القيمة "&roles;manager". وستحيل إلى رخصة الإداري <PolicySet>. وسيضم دور الموظف <PolicySet> عنصر <Target> يتطلب إعطاء الجهة المستعملة النعت &role مع القيمة "&roles;employee. وستحيل هذه القيمة إلى رخصة الموظف <PolicySet>.

1.2.8 رخصة <PolicySet> لدور الإداري

تضم رخصة <PolicySet> التالية الرخص المصاحبة لدور الإداري. ويجب ترتيب استعادة السياسة في النقطة PDP بحيث يتعذر النفاذ إلى هذه المجموعة <PolicySet> إلاّ من خلال إحالة صادرة عن دور الإداري <PolicySet>، (انظر الجدول 8-1).

الجدول X.1142/1-8 – رخصة <PolicySet> للإداريين

```
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
PolicySetId="PPS:manager:role"
PolicyCombiningAlgId="&policy-combine;permit-overrides">

<!-- Permissions specifically for the manager role -->
<Policy PolicyId="Permissions:specifically:for:the:manager:role"
    RuleCombiningAlgId="&rule-combine;permit-overrides">
    <!-- Permission to sign a purchase order -->
    <Rule RuleId="Permission:to:sign:a:purchase:order" Effect="Permit">
                <Target>
                      <Resources>
                            <Resource>
                                  <ResourceMatch MatchId="&function;string-equal">
                                     <AttributeValue
                                          DataType="&xml;string">purchase
order</AttributeValue>
                                  <ResourceAttributeDesignator
AttributeId="&resource;resource-id"
                                          DataType="&xml;string"/>
                            </ResourceMatch>
                            </Resource>
                      </Resources>
                      <Actions>
                            <Action>
                                  <ActionMatch MatchId="&function;string-equal">
                                    <AttributeValue
                                       DataType="&xml;string">sign</AttributeValue>
                                       ActionAttributeDesignator
                                       AttributeId="&action;action-id"
                                       DataType="&xml;string"/>
                                  </ActionMatch>
                            </Action>
                      </Actions>
                </Target>
          </Rule>
</Policy>
<!-- Include permissions associated with employee role -->
<PolicySetIdReference>PPS:employee:role</PolicySetIdReference>
</PolicySet>
```

2.2.8 رخصة <PolicySet> لدور الموظف

تضم رخصة <PolicySet> التالية الرخص المصاحبة لدور الموظف (انظر الجدول 8-2). ويجب أن ترتب استعادة السياسة في النقطة PDP بحيث لا يمكن النفاذ إلى هذا العنصر <PolicySet> إلاّ بالإحالة الصادرة عن دور الموظف <PolicySet> أو عن دور إداري <PolicySet> أكبر باستعمال رخصة الإداري <PolicySet>.

الجدول X.1142/2-8 – رخصة <PolicySet> للموظفين

```
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
   PolicySetId="PPS:employee:role"
   PolicyCombiningAlgId="&policy-combine;permit-overrides">
   <!-- Permissions specifically for the employee role -->
   <Policy PolicyId="Permissions:specifically:for:the:employee:role"
          RuleCombiningAlgId="&rule-combine;permit-overrides">
   <!-- Permission to create a purchase order -->
          <Rule RuleId="Permission:to:create:a:purchase:order" Effect="Permit">
                 <Target>
                        <Resources>
                               <Resource>
                                      <ResourceMatch MatchId="&function;string-equal">
                                        <AttributeValue
                                        DataType="&xml;string">purchase
order</AttributeValue>
                                        <ResourceAttributeDesignator
AttributeId="&resource;resource-id"
                                        DataType="&xml;string"/>
                                      </ResourceMatch>
                               </Resource>
                        </Resources>
                        <Actions>
                               <Action>
                                      <ActionMatch MatchId="&function;string-equal">
                                        <AttributeValue
DataType="&xml;string">create</AttributeValue>
                                        <ActionAttributeDesignator
AttributeId="&action;action-id"
                                        DataType="&xml;string"/>
                                      </ActionMatch>
                               </Action>
                        </Actions>
                 </Target>
          </Rule>
   </Policy>
</PolicySet>
```

3.2.8 دور <PolicySet> في دور الإداري

لا يطبق الدور <PolicySet> التالي وفقاً لعنصره <Target> إلاّ على الجهات المزودة بالنعت &role؛ (انظر الجدول 8-3) مع قيمة نعت "&roles;manager". والعنصر <PolicySetIdReference> مسدد إلى الرخصة <PolicySet> المصاحبة لدور الإداري.

الجدول X.1142/3-8 – دور <PolicySet> للإداريين

```
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
   PolicySetId="RPS:manager:role"
   PolicyCombiningAlgId="&policy-combine;permit-overrides">
   <Target>
          <Subjects>
                 <Subject>
                        <SubjectMatch MatchId="&function;anyURI-equal">
                               <AttributeValue
DataType="&xml;anyURI">&roles;manager</AttributeValue>
                               <SubjectAttributeDesignator AttributeId="&role;"
                                      DataType="&xml;anyURI"/>
                        </SubjectMatch>
                 </Subject>
          </Subjects>
   </Target>
<!-- Use permissions associated with the manager role -->
   <PolicySetIdReference>PPS:manager:role</PolicySetIdReference>
</PolicySet>
```

4.2.8 دور <PolicySet> في دور "الموظف"

لا يطبق الدور <PolicySet> التالي وفقاً لعنصره <Target> إلاّ على الجهات المزودة بالنعت role&؛ (انظر الجدول 8-4) مع قيمة نعت "&roles;employee". والعنصر <PolicySetIdReference> مسدد إلى الرخصة <PolicySet> المصاحبة لدور الموظف.

الجدول X.1142/4-8 – دور <PolicySet> للموظفين

```
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
   PolicySetId="RPS:employee:role"
   PolicyCombiningAlgId="&policy-combine;permit-overrides">
   <Target>
          <Subjects>
                 <Subject>
                        <SubjectMatch MatchId="&function;anyURI-equal">
                               <AttributeValue
DataType="&xml;anyURI">&roles;employee</AttributeValue>
                               <SubjectAttributeDesignator AttributeId="&role;"
DataType="&xml;anyURI"/>
                        </SubjectMatch>
                 </Subject>
          </Subjects>
   </Target>
<!-- Use permissions associated with the employee role -->
<PolicySetIdReference>PPS:employee:role</PolicySetIdReference>
</PolicySet>
```

5.2.8 سياسات وطلبات الدور HasPrivilegesOfRole

يمكن لنظام XACML RBAC أن يختار توفير أسئلة من النوع "هل تتمتع هذه الجهة بامتيازات الدور X؟". وفي هذه الحالة يجب أن تضم كل رخصة <PolicySet> المعلمة <Policy> HasPrivilegesOfRole. وفيما يتعلق بالرخصة <PolicySet> للإداريين فإن المعلمة <Policy> HasPrivilegesOfRole تتخذ الشكل المبين في الجدول 8-5.

الجدول X.1142/5-8 – رخصة <PolicySet> للإداريين

```
<!-- HasPrivilegesOfRole Policy for manager role -->
<Policy PolicyId="Permission:to:have:manager:role:permissions"
   RuleCombiningAlgId="&rule-combine;permit-overrides">
<!-- Permission to have manager role permissions -->
   <Rule RuleId="Permission:to:have:manager:permissions" Effect="Permit">
          <Condition>
                 <Apply FunctionId="&function;and">
                        <Apply FunctionId="&function;anyURI-is-in">
                               <AttributeValue
DataType="&xml;anyURI">&roles;manager</AttributeValue>
                               <ResourceAttributeDesignator AttributeId="&role;"
DataType="&xml;anyURI"/>
                        </Apply>
                               <Apply FunctionId="&function;anyURI-is-in">
                               <AttributeValue

   DataType="&xml;anyURI">&actions;hasPrivilegesofRole</AttributeValue>
                               <ActionAttributeDesignator AttributeId="&action;action-
id"
                                      DataType="&xml;anyURI"/>
                        </Apply>
                 </Apply>
          </Condition>
   </Rule>
</Policy>
```

أما فيما يتعلق بالرخصة <PolicySet> للموظفين فإن المعلمة <Policy> HasPrivilegesOfRole تتخذ الشكل المبين في الجدول 8-6.

الجدول X.1142/6-8 – رخصة <PolicySet> للموظفين

```
<!-- HasPrivilegesOfRole Policy for employee role -->
<Policy PolicyId="Permission:to:have:employee:role:permissions"
   RuleCombiningAlgId="&rule-combine;permit-overrides">
<!-- Permission to have employee role permissions -->
   <Rule RuleId="Permission:to:have:employee:permissions" Effect="Permit">
         <Condition>
               <Apply FunctionId="&function;and">
                     <Apply FunctionId="&function;anyURI-is-in">
                           <AttributeValue
DataType="&xml;anyURI">&roles;employee</AttributeValue>
                           <ResourceAttributeDesignator AttributeId="&role;"
                                 DataType="&xml;anyURI"/>
                     </Apply>
                     <Apply FunctionId="&function;anyURI-is-in">
                     <AttributeValue
DataType="&xml;anyURI">&actions;hasPrivilegesofRole
                     </AttributeValue>
                     <ActionAttributeDesignator AttributeId="&action;action-id"
                           DataType="&xml;anyURI"/>
                     </Apply>
               </Apply>
         </Condition>
   </Rule>
</Policy>
```

ويتخذ طلب معرفة ما إذا كانت الجهة Anne تتمتع بالامتيازات المصاحبة للدور &roles;manager الشكل المبين في الجدول 8-7.

الجدول X.1142/7-8 – طلب سؤال عن جهة

```
<Request>
   <Subject>
         <Attribute AttributeId="&subject;subject-id" DataType="&xml;string">
               <AttributeValue>Anne</AttributeValue>
         </Attribute>
   </Subject>
   <Resource>
         <Attribute AttributeId="&role;" DataType="&xml;anyURI">
               <AttributeValue>&roles;manager</AttributeValue>
               </Attribute>
   </Resource>
   <Action>
         <Attribute AttributeId="&action;action-id"

   DataType="&xml;anyURI">&actions;hasPrivilegesOfRole</AttributeValue>
         </Attribute>
   </Action>
</Request>
```

ويجب أن يضم <Request> الأدوار الصريحة للجهة Anne (وفي هذه الحالة &roles;employee) أو أنه يجب أن تكون إدارة سياق النقطة PDP قادراً على العثور عليها. فالسياسات HasPrivilegesOfRole لا تقوم بربط الأدوار مع الجهات المستعملة.

3.8 تخصيص نعوت الأدوار وتفعيلها

ترد هذه الفقرة على سبيل الإعلام.

إن تخصيص نعوت أدوار مختلفة للمستعملين وتفعيل هذه النعوت أثناء الجلسة لا يدخل في نطاق تطبيق النقطة XACML PDP. ويتعين وجود كيان منفصل واحد أو أكثر يحيل إلى سلطات تفعيل الدور من أجل القيام بهذه الوظائف. وتفترض هذه المواصفة أن وجود نعت دور مستعمل ما (جهة) في سياق الطلب XACML تخصيص صالح عند طلب قرار النفاذ.

ومن أين تأتي نعوت دور جهة مستعملة ما؟ وما هي مواصفات سلطة تفعيل الأدوار؟ وتتوقف الإجابة على التطبيق، لكن ثمة إمكانيات يمكن اقتراحها.

فقد تأتي نعوت الأدوار في بعض الحالات، من خدمة إدارة هويات تحتفظ بالمعلومات عن المستعمل بما فيها الأدوار المخصصة أو المتاحة لهذه الجهة؛ وتقوم خدمة إدارة الهويات بدور سلطة تفعيل الأدوار. وقد تخزن هذه الخدمة نعوت الأدوار الساكنة في دليل LDAP، ويمكن لإدارة سياق النقطة PDP أن تستعيدها من هناك. وقد تجيب هذه الخدمة على طلبات معرفة نعوت أدوار جهة ما التي تردها من إدارة سياق نقطة PDP حيث تتخذ الطلبات شكل أسئلة عن نعوت اللغة SAML.

ويمكن لسلطات تفعيل الأدوار أن تستعمل تخصيص دور XACML <Policy> أو <PolicySet> من أجل تحديد إمكانية حصول جهة ما على نعت دور معين وقيمة منشطة. ويجيب تخصيص دور <Policy> أو <PolicySet> على السؤال "هل الجهة X مخولة للحصول على دور R_i منشط؟". ولا يجيب على السؤال "ما هي مجموعة الأدوار التي يسمح للجهة X بتفعيلها؟" ويجب أن يكون لسلطة تفعيل الأدوار وسيلة ما لمعرفة الدور (أو الأدوار) الذي يجب تقديم الطلب له. مثال: قد تحتفظ سلطة تفعيل الأدوار بقائمة بجميع الأدوار الممكنة وعندما تتلقى سؤالاً عن الأدوار المعطاة لجهة معينة تقوم بطلب سياسات تخصيص الأدوار لكل دور مرشح.

وتختلف مجموعة سياسات توزيع الأدوار في هذه المواصفة عن حالات مجموعة <PolicySet> لدور الرخصة المستخدمة في تحديد رخص النفاذ المصاحبة لكل دور. ولا تستعمل سياسات تخصيص الأدوار إلا عندما يأتي الطلب XACML من سلطة تفعيل الأدوار. ويمكن إدارة هذا الفصل بطرق متعددة مثل استعمال نقاط PDP مختلفة مع ذاكرات مختلفة للسياسات أو طلب العناصر <Request> لأغراض طلبات تفعيل الدور من أجل إدراج العنصر <Subject> في النعت SubjectCategory للمعلمة "&subject-category;role-enablement-authority".

وليس هناك شكل ثابت لعنصر <Policy> لتخصيص الدور. ويوضح المثال التالي (الجدول 8-8) شكلاً ممكناً واحداً. وهو يضم عنصرين XACML <Rule>. تنص القاعدة <Rule> الأولى على أن Anne وSeth وYassir مخولون للحصول على الدور "&roles;employee" المنشط من الساعة 9 صباحاً إلى الساعة 5 بعد الظهر. أما القاعدة <Rule> الثانية فتقضي بأن Steve له الدور "&roles;manager" المنشط دون أي تقييد في الساعات.

الجدول X.1142/8-8 – مثال توزيع الأدوار

```
<POLICY XMLNS="URN:OASIS:NAMES:TC:XACML:2.0:POLICY:SCHEMA:OS"
    POLICYID="ROLE:ASSIGNMENT:POLICY"
    RULECOMBININGALGID="&RULE-COMBINE;PERMIT-OVERRIDES">
<!-- EMPLOYEE ROLE REQUIREMENTS RULE -->
    <RULE RULEID="EMPLOYEE:ROLE:REQUIREMENTS" EFFECT="PERMIT">
        <TARGET>
            <SUBJECTS>
                <SUBJECT>
                    <SUBJECTMATCH MATCHID="&FUNCTION;STRING-EQUAL">
                        <ATTRIBUTEVALUE DATATYPE="&XML;STRING">SETH</ATTRIBUTEVALUE>
                        <SUBJECTATTRIBUTEDESIGNATOR ATTRIBUTEID="&SUBJECT;SUBJECT-ID"
                            DATATYPE="&XML;STRING"/>
                    </SUBJECTMATCH>
                </SUBJECT>
                <SUBJECT>
                    <SUBJECTMATCH MATCHID="&FUNCTION;STRING-EQUAL">
                        <ATTRIBUTEVALUE DATATYPE="&XML;STRING">ANNE</ATTRIBUTEVALUE>
                        <SUBJECTATTRIBUTEDESIGNATOR ATTRIBUTEID="&SUBJECT;SUBJECT-ID"
                            DATATYPE="&XML;STRING"/>
                    </SUBJECTMATCH>
                </SUBJECT>
            </SUBJECTS>
        <RESOURCES>
            <RESOURCE>
                <RESOURCEMATCH MATCHID="&FUNCTION;ANYURI-EQUAL">
                    <ATTRIBUTEVALUE
DATATYPE="&XML;ANYURI">&ROLES;EMPLOYEE</ATTRIBUTEVALUE>
                        <RESOURCEATTRIBUTEDESIGNATOR ATTRIBUTEID="&ROLE;"
                            DATATYPE="&XML;ANYURI"/>
                    </RESOURCEMATCH>
                    </RESOURCE>
                </RESOURCES>
                <ACTIONS>
                <ACTION>
                    <ACTIONMATCH MATCHID="&FUNCTION;ANYURI-EQUAL">
                        <ATTRIBUTEVALUE DATATYPE="&XML;ANYURI">&ACTIONS;
                            ENABLEROLE</ATTRIBUTEVALUE>
                        <ACTIONATTRIBUTEDESIGNATOR ATTRIBUTEID="&ACTION;ACTION-ID"
                            DATATYPE="&XML;ANYURI"/>
                    </ACTIONMATCH>
                </ACTION>
            </ACTIONS>
        </TARGET>
        <CONDITION>
            <APPLY FUNCTIONID="&FUNCTION;AND">
                <APPLY FUNCTIONID="&FUNCTION;TIME-GREATER-THAN-OR-EQUAL">
```

الجدول X.1142/8-8 – مثال توزيع الأدوار

```
                    <APPLY FUNCTIONID="&FUNCTION;TIME-ONE-AND-ONLY">
                        <ENVIRONMENTATTRIBUTEDESIGNATOR
ATTRIBUTEID="&ENVIRONMENT;CURRENT-TIME"
                            DATATYPE="&XML;TIME"/>
                    </APPLY>
                    <ATTRIBUTEVALUE DATATYPE="&XML;TIME">9H</ATTRIBUTEVALUE>
                </APPLY>
                <APPLY FUNCTIONID="&FUNCTION;TIME-LESS-THAN-OR-EQUAL">
                    <APPLY FUNCTIONID="&FUNCTION;TIME-ONE-AND-ONLY">
                        <ENVIRONMENTATTRIBUTEDESIGNATOR
                            ATTRIBUTEID="&ENVIRONMENT;CURRENT-TIME"
DATATYPE="&XML;TIME"/>
                    </APPLY>
                    <ATTRIBUTEVALUEDATATYPE="&XML;TIME">17H</ATTRIBUTEVALUE>
                </APPLY>
        </APPLY>
    </CONDITION>
</RULE>
<!-- MANAGER ROLE REQUIREMENTS RULE -->
    <RULE RULEID="MANAGER:ROLE:REQUIREMENTS" EFFECT="PERMIT">
        <TARGET>
            <SUBJECTS>
                <SUBJECT>
                    <SUBJECTMATCH MATCHID="&FUNCTION;STRING-EQUAL">
                        <ATTRIBUTEVALUE DATATYPE="&XML;STRING">STEVE</ATTRIBUTEVALUE>
                        <SUBJECTATTRIBUTEDESIGNATOR ATTRIBUTEID="&SUBJECT;SUBJECT-ID"
                            DATATYPE="&XML;STRING"/>
                    </SUBJECTMATCH>
                </SUBJECT>
            </SUBJECTS>
            <RESOURCES>
                <RESOURCE>
                    <RESOURCEMATCH MATCHID="&FUNCTION;ANYURI-EQUAL">
                        <ATTRIBUTEVALUE
                            DATATYPE="&XML;ANYURI">&ROLES;:MANAGER</ATTRIBUTEVALUE>
                        <RESOURCEATTRIBUTEDESIGNATOR ATTRIBUTEID="&ROLE;"
                            DATATYPE="&XML;ANYURI"/>
                    </RESOURCEMATCH>
                </RESOURCE>
            </RESOURCES>
        <ACTIONS>
            <ACTION>
                <ACTIONMATCH MATCHID="&FUNCTION;ANYURI-EQUAL">
                    <ATTRIBUTEVALUE
                        DATATYPE="&XML;ANYURI">&ACTIONS;ENABLEROLE</ATTRIBUTEVALUE>
                        <ACTIONATTRIBUTEDESIGNATOR ATTRIBUTEID="&ACTION;ACTION-ID"
                            DATATYPE="&XML;ANYURI"/>
                </ACTIONMATCH>
            </ACTION>
        </ACTIONS>
    </TARGET>
</RULE>
</POLICY>
```

4.8 تطبيق نموذج التحكم RBAC

ترد هذه الفقرة على سبيل الإعلام.

وتصف الفقرات التالية كيفية استعمال السياسات XACML من أجل تطبيق مختلف مكونات النموذج RBAC (انظر المرجع [RBAC]).

1.4.8 التحكم RBAC الرئيسي

يشتمل التحكم RBAC الرئيسي على خمسة عناصر معطيات أساسية هي:

- يستفيد المستعمل باستعماله للنعوت Subjects XACML. ويمكن استعمال كل قيمة من القيم SubjectCategory XACML، حسب الاقتضاء.

- يعبر عن الأدوار باستعمال نعت واحد أو أكثر لجهة مستعملة XACML. ومجموعة الأدوار محددة جداً بمجال التطبيق والسياسة ومن الهام جداً عدم خلط استعمالات مختلفة للأدوار. ولهذه الأسباب لا تحاول هذه الواصفة أن تحدد أي مجموعة معايير لقيم الأدوار على الرغم من أنها توصي باستعمال قيمة مشتركة للمعرف AttributeId هي: "urn:oasis:names:tc:xacml:2.0:subject:role". ويوصى بأن يوافق كل مجال تطبيق أو سياسة على مجموعة وحيدة من القيم AttributeId والقيم DataType والقيم <AttributeValue> التي سيستعملها في مختلف الأدوار ذات الصلة بهذا المجال وينشرها.
- يتم التعبير عن الأغراض باستعمال الموارد XACML.
- يتم التعبير عن العمليات باستعمال الإجراءات XACML.
- يتم التعبير عن الرخص باستعمال حالتي <PolicySet> XACML Role و<PolicySet> Permission وفقاً لوصفهما الوارد في الفقرات السابقة.

ويتطلب التحكم RBAC الرئيسي توفير عدة مستعملين للدور وعدة أدوار للمستعمل وعدة رخص للدور وعدة أدوار للرخصة. ويمكن الوفاء بكل من هذه المتطلبات باستعمال السياسات XACML القائمة على هذه المواصفة على النحو التالي. ويجدر بالذكر أن التوزيع الفعلي للأدوار على المستعملين لا يدخل في نطاق النقطة XACML PDP.

وتتيح اللغة XACML لعدة جهات مستعملة أن ترفق دوراً معيناً بالنعت وستنطبق المجموعات <PolicySet>s للدور في اللغة XACML المعرفة من حيث الحصول على <Attribute> دور معين و<AttributeValue> دوره في سياق الطلب XACML.

وتتيح اللغة XACML لعدة نعوت أدوار أو قيم نعوت أدوار مصاحبة جهة مستعملة Subject معينة. وإذا كان للجهة المستعملة عدة أدوار منشطة، يمكن تقييم أي حالة <PolicySet> للدور مطبقة على أي من هذه الأدوار ويسمح بالرخص الموجودة في العنصر المقابل <PolicySet>. كما يمكن تحديد سياسات تتطلب من جهة مستعملة معينة أن تتزود بعدة نعوت أو قيم أدوار منشطة في نفس الوقت. ولا تنطبق الرخص المصاحبة لمتطلبات الدور المتعدد في هذه الحالة على الجهة المستعملة التي تمتلك جميع نعوت وقيم الأدوار اللازمة في الوقت الذي يُقدم فيه سياق الطلب XACML إلى النقطة PDP للتقييم.

وقد تسمح الرخصة <PolicySet> المصاحبة لدور ما بالنفاذ إلى موارد متعددة باستعمال إجراءات متعددة. وللغة XACML مجموعة غنية من أدوات بناء الرخص أي هناك طرق متعددة يمكن التعبير من خلالها عن الأدوار متعددة الرخص. ويمكن لأي دور A أن يصاحب رخصة <PolicySet> B بإدراج عنصر <PolicySetIdReference> في رخصة <PolicySet> B في الرخص <PolicySet> المصاحبة للدور A. وبهذه الطريقة يمكن إرفاق نفس مجموعة الرخص بأكثر من دور واحد.

وإضافة إلى متطلبات التحكم RBAC المركزي الأساسي يمكن للسياسات XACML التي تستخدم هذه المواصفة أن تطلق أيضاً شروطاً اعتباطية بشأن تطبيق رخص خاصة مرفقة بدور ما. وقد تضم هذه الشروط قصر صلاحية الرخص على فترة زمنية محددة في اليوم أو على أصحاب الدور المزودين ببعض النعوت الأخرى أكانت نعوت أدوار أم لا.

2.4.8 التحكم RBAC التراتبي

يوسع التحكم RBAC التراتبي التحكم RBAC المركزي ليشمل مقدرة تحديد علاقات الإرث بين الأدوار. فمثلاً يمكن تحديد الدور A بأنه يرث جميع الرخص المصاحبة للدور B. ويعتبر الدور A في هذه الحالة أكبر من الدور B في تراتب الأدوار. وإذا كان الدور B بدوره وريثاً للرخص المصاحبة للدور C، يرث الدور A أيضاً هذه الرخص باعتباره أكبر من الدور B.

وتستطيع السياسات XACML التي تستخدم هذه المواصفة تنفيذ إرث الأدوار بإدراج العنصر <PolicySetIdReference> في الرخصة <PolicySet> المصاحبة لدور واحد داخل الرخصة <PolicySet> المصاحبة لدور آخر. وسيرث الدور الذي يضم العنصر <PolicySetIdReference> عندئذٍ الرخص المصاحبة للدور المذكور.

وتنظم هذه المواصفة سياسات بحيث يمكن إضافة خواص الإرث إلى دور ما في أي وقت دون طلب تغيير الحالات <PolicySet> المصاحبة لأي دور آخر. وقد لا تستعمل جهة ما تراتب الأدوار في بداية الأمر لكنها تقرر فيما بعد استعمال هذه الوظائف دون الاضطرار إلى إعادة صياغة السياسات القائمة.

5.8 المواصفة

تناقش هذه الفقرة الأدوار ونعوت الأدوار وتخصيص الأدوار والتحكم بالنفاذ.

1.5.8 الأدوار ونعوت الأدوار

يعبر عن الأدوار باستخدام نعت XACML واحد أو أكثر. ويحدد كل مجال تطبيق يستخدم هذه المواصفة لأغراض التحكم في النفاذ القائم على الدور قيمة AttributeId واحدة أو أكثر أو سيوافق عليها من أجل استخدامها في نعوت الأدوار. وستصاحب كل قيمة AttributeId من هذا القبيل مجموعة من القيم المسموح بها مع المعلمات DataTypes التابعة لها. وستكون لكل قيمة مسموح بها لهذه المعلمة AttributeId دلالات محددة جيداً لاستخدام القيمة المقابلة لها في السياسات.

وتوصي هذه المواصفة باستخدام القيمة AttributeId "urn:oasis:names:tc:xacml:2.0:subject:role" في جميع نعوت الأدوار. وينبغي تزويد حالات هذا النعت نمط المعطيات "http://www.w3.org/2001/XMLSchema#anyURI".

2.5.8 تخصيص الدور أو تنشيطه

تستخدم سلطة تنشيط الأدوار المسؤولة عن تخصيص الأدوار للمستعملين وتنشيطها للاستخدام أثناء جلسة الاستخدام، العنصر <Policy> أو <PolicySet> لتخصيص الأدوار XACML من أجل تحديد المستعملين المؤهلين والأدوار المسموح تنشيطها والشروط الملازمة. ولا يوجد شكل إلزامي لعنصر <Policy> أو <PolicySet>. ويوصى بالتعبير عن الأدوار في <Policy> أو <PolicySet> لتخصيص الأدوار على شكل نعوت موارد حيث المعلمة AttributeId هي &role; والعنصر <AttributeValue> هو معرف URI لقيمة الدور ذي الصلة. كما يوصى بالتعبير عن إجراء تخصيص أو تنشيط الدور على شكل نعت إجراء حيث المعلمة AttributeId هي &action;action-id, والمعلمة DataType هي &xml;anyURI, و<AttributeValue> هو &actions;enableRole.

3.5.8 التحكم في النفاذ

يمكن تنفيذ التحكم في النفاذ القائم على الدور باستخدام نوعين من العناصر :s<PolicySet> هما <PolicySet> الدور و<PolicySet> الرخصة. وفيما يلي الوظائف والمتطلبات المحددة لهذين النوعين من العناصر s<PolicySet>.

يتحدد لكل دور عنصر <PolicySet> Role واحد يضم عنصر <Target> يجعل العنصر <PolicySet> قابلاً للتطبيق على المواضيع المزودة بالنعت XACML المصاحب للدور المعين؛ ولا يحد العنصر <Target> من الموارد أو الإجراء أو البيئة. ويضم كل دور <PolicySet> عنصراً <PolicySetIdReference> واحداً يحيل إلى رخصة <PolicySet> واحدة مصاحبة للدور. ولا يضم الدور <PolicySet> أي عناصر أخرى من عناصر <Policy> أو <PolicySet> أو <PolicyIdReference> أو <PolicySetIdReference>.

ويتحدد لكل دور عنصر <PolicySet> واحد للرخصة يضم عنصري <Policy> و<Rule> يحددان أنماط النفاذ المسموحة إلى المواضيع التي تحتوي على الدور المعني. ولا يحد العنصر <Target> في <PolicySet> وعناصره ,<PolicySet> و<Policy> و<Rule> من المواضيع التي تطبق عليها مجموعة سياسات الرخصة.

وإذا كان دور ما يرث رخصاً من واحد أو أكثر أصغر منه، فينبغي أن يضم عنصر <PolicySet> الرخصة للدور المعني (الأكبر) العنصر <PolicySetIdReference> لكل دور أصغر. ويجب أن يحيل هذا العنصر <PolicySetIdReference> إلى الرخصة <PolicySet> المصاحبة للدور الأصغر الذي يرث منه الدور الأكبر.

وقد يضم عنصر الرخصة <PolicySet> المعلمة <Policy> HasPrivilegesOfRole. التي ينبغي لها أن تضم عنصر <Rule> مع التأثير "مسموح". وتتيح هذه القاعدة لأي جهة مستعملة أن تقوم بإجراء له نعت فيه معرف AttributeId للإجراء &action;action-id وDataType للمعرف &xml;anyURI وعنصر <AttributeValue> بقيمة &actions;hasPrivilegesOfRole في مورد له نعت ينطبق على دوره الرخصة <PolicySet> (مثل AttributeId للدور &role; وDataType للمعرف &xml;anyURI و<AttributeValue> قيمته المعرف URI لقيمة الدور المحدد). ويجدر بالذكر أن نعت الدور وهو نعت موضوع العنصر <Target> للدور <PolicySet>، يعالج على أنه نعت مورد في السياسة HasPrivilegesOfRole <Policy>.

وسيضمن تنظيم أي مستودع مستخدم للسياسات والتشكيلات في النقطة PDP أن هذه النقطة لا تستطيع أبداً استعمال <PolicySet> على أنها سياسة أولية للنقطة PDP.

6.8 معرفات الهوية

فيما يلي المعرفات URN التي تحددها هذه المواصفة.

1.6.8 معرف هوية المواصفة

يستخدم المعرف التالي كمعرف هوية هذه المواصفة عندما يشترط معرف على شكل URI.

```
urn:oasis:names:tc:xacml:2.0:profiles:rbac:core-hierarchical
```

2.6.8 نعت الدور

يمكن استخدام المعرف التالي كمعرف AttributeId لنعوت الدور.

```
urn:oasis:names:tc:xacml:2.0:subject:role
```

3.6.8 المعلمة SubjectCategory (فئة الجهة المستعملة)

يمكن استخدام المعرف التالي على أنه SubjectCategory لنعوت الجهة المستعملة التي تحدد ما إذا كان الطلب صادر عن سلطة تنشيط الأدوار.

```
urn:oasis:names:tc:xacml:2.0:subject-category:role-enablement-authority
```

4.6.8 قيم نعوت الإجراء

يمكن استخدام معرف الهوية التالي على أنه عنصر <AttributeValue> للنعت &action;action-id في <Policy> HasPrivilegesOfRole.

```
urn:oasis:names:tc:xacml:2.0:actions:hasPrivilegesOfRole
```

ويمكن استخدام المعرف التالي على أنه <AttributeValue> للنعت &action;action-id في تخصيص الدور <Policy>.

```
urn:oasis:names:tc:xacml:2.0:actions:enableRole
```

9 مواصفة تعدد الموارد في اللغة XACML

يتحدد تقييم السياسة الذي تقوم به نقطة إقرار السياسة أو PDP في اللغة XACML على أنها مورد مطلوب واحد مع قرار ترخيص يتضمن عنصر <Result> واحد في سياق الاستجابة. غير أن نقطة تعزيز السياسات أو PEP قد تود تقديم سياق طلب واحد من أجل النفاذ إلى موارد متعددة وتبغي الحصول على سياق استجابة واحد يتضمن قرار ترخيص منفصل (عنصر <Result>) لكل مورد مطلوب. وقد يستخدم سياق طلب من هذا القبيل بغية تجنب إرسال عدة رسائل طلب قرار ما بين النقطتين PEP وPDP مثلاً. ومن ناحية أخرى قد ترغب النقطة PEP في تقديم سياق طلب واحد لجميع العقد الموجودة في تراتب ما وقد تريد الحصول على قرار ترخيص واحد (عنصر <Result>) يدل على ما إذا كان النفاذ مسموحاً لجميع العقد المطلوبة. وقد يستخدم سياق طلب من هذا القبيل عندما يريد الطالب نفاذاً إلى كامل الوثيقة XML أو إلى كامل شجرة فرعية من العناصر في هذه الوثيقة أو على كامل دليل نظام الملفات مع جميع تفرعاته وملفاته مثلاً.

وتصف هذه التوصية ثلاث طرائق يمكن أن تطلب فيها النقطة PEP قرارات ترخيص لعدة موارد في سياق طلب واحد وهي تصف كيفية عرض نتيجة كل قرار ترخيص منها في سياق استجابة واحدة يعاد إلى النقطة PEP.

كما تصف هذه التوصية طريقتين يمكن أن تطلب فيهما النقطة PEP قرار ترخيص واحد رداً على طلب جميع العقد الموجودة في تراتب ما.

أما توفير كل من الآليات الموصوفة في هذه المواصفة فخيار يعود إلى التطبيقات التي تمتثل للغة XACML.

وتختصر نعوت الموارد المنتشرة الاستعمال على النحو التالي:

- النعت "resource-id": نعت مورد مع معرف AttributeId:
"urn:oasis:names:tc:xacml:1.0:resource:resource-id"
- النعت "scope": نعت مورد مع معرف AttributeId:
"urn:oasis:names:tc:xacml:2.0:resource:scope"

ولمزيد من المعلومات عن هذا النعت راجع الفقرة 3.9.

1.9 طلبات موارد متعددة

هذه الفقرة معيارية ولكنها خيارية.

يمكن أن يقدم سياق طلب XACML واحد طلباً للنفاذ إلى موارد متعددة مع قرار ترخيص منفصل لكل مورد. وتتحدد قواعد تركيب هذه الطلبات والاستجابات ودلالاتها في هذه الفقرة.

ويجب أن تكون العناصر <Result> الناتجة عن تقييم طلب ما للنفاذ إلى موارد متعددة مماثلة للعناصر التي قد تنتج عن سلسلة من الطلبات التي يطلب كل منها النفاذ إلى مورد واحد من هذه الموارد. ويسمى مثل هذا المورد مورداً فردياً. ويسمى سياق الطلب النظري الذي يقابل كل عنصر <Result> طلب موردٍ فردي. ويجب أن تكون قيمة المعرف ResourceId في العنصر <Result> القيمة <AttributeValue> للنعت "resource-id" في طلب المورد الفردي المقابل. ويمكن لإدارة السياق المحددة في هذه التوصية أن تقوم بهذا التقابل بين سياق الطلب الأصلي الذي يضم عدة طلبات قرارات ترخيص مع طلبات الموارد الفردية والتقابل المقابل بين قرارات الترخيص المتعددة والعناصر <Result> المتعددة في سياق استجابة واحدة. ولا تتطلب هذه المواصفة أن يتطابق تنفيذ تقييم طلب نفاذ ما إلى عدة موارد مع النموذج السابق أو أن تتشكل طلبات موارد فردية فعلية. ولا تتطلب المواصفة سوى أن تكون العناصر <Result> هي نفسها التي كانت قد نتجت لو استعمل النموذج السابق.

وتقدم الفقرات التالية وصفاً لثلاث طرائق لتحديد طلبات النفاذ إلى موارد متعددة. وتصف كل طريقة منها طلبات موارد فردية تقابل العناصر <Result> في سياق الاستجابة.

ويمكن لسياق طلب XACML واحد تقدمه نقطة PEP أن يستخدم أكثر من طريقة لطلب النفاذ إلى موارد متعددة في عناصر <Resource> متعددة.

1.1.9 العقد المعرفة في المعلمة "scope"

هذه الفقرة معيارية ولكنها خيارية.

يصف هذا النص استخدام قيمتين لنعت المورد "scope" من أجل تحديد طلب نفاذ إلى عدة موارد في تراتب ما. ويمكن استخدام هذه القواعد مع مورد تراتبي بغض النظر عما إذا كانت الوثيقة وثيقة XML أم لا.

1.1.1.9 المعرفات URI في المواصفة

يُستخدم المعرفان URI التاليان كمعرفات URI للوظائف المحددة في هذا الجزء من هذه المواصفة. ويستخدم المعرف الأول عندما تتوفر الوظائف لأغراض الموارد XML ويستخدم المعرف الثاني عندما تتوفر الوظائف لأغراض الوثائق غير الوثائق XML:

```
urn:oasis:names:tc:xacml:2.0:profile:multiple:scope:xml
urn:oasis:names:tc:xacml:2.0:profile:multiple:scope:non-xml
```

2.1.1.9 قواعد تركيب سياق الطلب الأصلي

يجب أن يضم العنصر <Resource> لسياق الطلب XACML الأصلي النعت "scope" مع القيمة "Children" (أبناء) أو "Descendants" (أحلاف). وإذا كانت الموارد المطلوبة مدرجة في وثيقة XML فإن العنصر <ResourceContent> يجب أن يكون موجوداً وأن يتضمن كامل الوثيقة XML التي تشكل العناصر المطلوبة جزءاً منها. وإذا كانت الموارد المطلوبة مدرجة أيضاً في وثيقة XML يجب أن يتساوى التعبير XPath المستخدم كقيمة النعت "resource-id" مع مجموعة العقد التي تضم عقدة واحدة بالضبط.

3.1.1.9 الدلالات

يفسر سياق طلب بأنه طلب نفاذ إلى مجموعة عقد في تراتب ما تتصل بالعقدة الوحيدة المحددة في النعت "resource-id". وإذا كانت قيمة النعت "scope" هي "Children" فإن كل مورد فردي هو العقدة التي يدل عليها النعت "resource-id" (أو النعوت عندما يكون للمورد الواحد عدة معرفات هوية معيارية) وجميع العقد المتفرعة عنها مباشرة. وإذا كانت قيمة النعت "scope" هي "Descendants"، يكون المورد الفردي العقدة الواحدة التي يدل عليها النعت "resource-id" وجميع عقدها الأخلاف.

ويجب أن يكون كل طلب موردٍ فردي مماثلاً لسياق الطلب الأصلي باستثناء أمرين: أن النعت "scope" غير موجود وأن العنصر <Resource> يمثل مورداً فردياً واحداً. ويضم هذا العنصر <Resource> نعتاً واحداً على الأقل "resource-id"، وتكوِّن جميع قيم هذا النعت هويات فريدة معيارية للمورد الفردي. وإذا ضمَّ النعت "resource-id" في سياق الطلب الأصلي جهة مصدرة توجب أن تضم النعوت "resource-id" في طلب المورد الفردي نفس الجهة المصدرة. وإذا كان العنصر <ResourceContent> موجوداً في سياق الطلب الأصلي توجب إدراج نفس العنصر <ResourceContent> في كل طلب لمورد فردي.

ولا تحدد اللغة XACML ولا هذه المواصفة كيفية حصول إدارة السياق على المعلومات المطلوبة من أجل تحديد العقد الأبناء والعقد الأخلاف في عقدة معينة ما عدا في حالة وثيقة XML حيث يتم الحصول على المعلومات من العنصر <ResourceContent>.

2.1.9 العقد المعرفة في اللغة XPath

هذه الفقرة معيارية ولكنها خيارية.

تصف هذه الفقرة استعمال تعبير XPath في النعت "resource-id" مع قيمة "XPath-expression" في النعت "scope" من أجل تحديد طلب نفاذ إلى عقد متعددة في وثيقة XML. ويجب استخدام هذه القواعد مع وثائق XML لا غير.

1.2.1.9 المعرفات URI للمواصفة

يستخدم المعرف URI للوظائف التي يحددها هذا الجزء من هذه المواصفة:

```
urn:oasis:names:tc:xacml:2.0:profile:multiple:xpath-expression
```

2.2.1.9 سياق الطلب الأصلي

يضم العنصر <Resource> لسياق الطلب XACML الأصلي العنصر <ResourceContent> والنعت "resource-id" مع نمط المعطيات "urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression" يجب أن يكون <AttributeValue> للنعت "resource-id" تعبيراً XPath يعادل مجموعة عقد تمثل عقداً متعددة في العنصر <ResourceContent>. ويضم العنصر <Resource> النعت "scope" مع القيمة "XPath-expression".

3.2.1.9 الدلالات

يفسر سياق طلب من هذا القبيل على أنه طلب نفاذ إلى عقد متعددة في مجموعة العقد التي يمثلها العنصر <AttributeValue> للنعت "resource-id". وتمثل كل عقدة مورداً فردياً.

ويكون كل طلب مورد فردي مماثلاً لسياق الطلب الأصلي باستثناء أمرين هما: عدم وجود النعت "scope" وضرورة أن تكون قيمة النعت "resource-id" تعبيراً XPath يساوي عقدة واحدة في العنصر <ResourceContent>. وتكون تلك العقدة المورد الفردي. وإذا ضم النعت "resource-id" في سياق الطلب الأصلي جهة مصدرة فإن النعت "resource-id" في طلب المورد الفردي سيضم نفس الجهة المصدرة.

3.1.9 عناصر <Resource>

هذه الفقرة معيارية لكنها خيارية.

تصف هذه الفقرة استعمال عناصر <Resource> متعددة في سياق طلب من أجل تحديد طلب نفاذ إلى موارد متعددة. ويمكن استعمال هذه القواعد مع أي مورد أو موارد بغض النظر عما إذا كانت وثائق XML أم لا وبغض النظر عما إذا كانت موارد تراتبية أم لا.

1.3.1.9 عناصر URI

يستعمل المعرف URI التالي كمعرف URI للوظيفة التي يحددها هذا الجزء من المواصفة:

```
    urn:oasis:names:tc:xacml:2.0:profile:multiple:multiple-resource-
elements
```

2.3.1.9 سياق الطلب الأصلي

يضم سياق الطلب XACML عدة عناصر <Resource>.

3.3.1.9 الدلالات

يفسر سياق طلب من هذا القبيل على أنه طلب نفاذ إلى جميع الموارد المحددة في العنصر <Resource> مورداً فردياً واحداً شريطة ألا يستخدم ذلك العنصر الآليات الأخرى التي يرد وصفها في هذه المواصفة.

ويستحدث لكل عنصر <Resource> طلب مورد فردي واحد. ويكون هذا الطلب مماثلاً لسياق الطلب الأصلي بفارق واحد هو وجود عنصر <Resource> واحد. وإذا ضم هذا العنصر <Resource> نعت "scope" له قيمة مختلفة عن "Immediate"، تعين معالجة طلب المورد الفردي وفقاً للجزء المقابل من هذه المواصفة. وقد تفترض هذه المعالجة تفكيك طلب المورد الفردي الواحد إلى طلبات موارد فردية أخرى قبل تقييم النقطة PDP لها.

2.9 طلبات لكامل التراتب

هذه الفقرة معيارية ولكنها خيارية.

المورد تراتبي في بعض الحالات لكن الغرض من طلب قرار الترخيص هو طلب النفاذ إلى جميع العقد داخل المورد أو إلى كامل تراتب فرعي للعقد ضمن ذلك المورد. وقد تكون هذه هي الحالة عند طلب النفاذ إلى وثيقة XML لأغراض إجراء نسخة من كامل الوثيقة أو عند طلب النفاذ إلى كامل دليل نظام الملفات مع أدلته الفرعية وملفاته. والمطلوب هو عنصر <Result> واحد يدل على ما إذا كان من المسموح للطالب النفاذ إلى كامل مجموعة العقد.

ويجب أن يكون العنصر <Result> الناتج عن تقييم طلب النفاذ مماثلاً لذلك الناجم عن المعالجة التالية. تقيّم سلسلة من سياقات الطلبات التي يطلب كل منها نفاذاً إلى عقدة واحدة تماماً من التراتب. ويكون <Decision> في <Result> الوحيدة الراجعة إلى النقطة PEP "مسموح" (Permit) في حالة واحدة هي إذا كانت جميع العناصر <Result> الناجمة عن تقييم العقد الفردية تضم <Decision> "Permit". وإلاّ يكون <Decision> الذي <Result> النتيجة الوحيدة المعادة إلى النقطة PEP هو "مرفوض" (Deny). ولا تتطلب هذه المواصفة أن يكون تنفيذ تقييم طلب النفاذ إلى موارد تراتبية من هذا القبيل مطابقاً للنموذج السابق أو أن تكون سياقات الطلبات الفعلية المقابلة للعقد الفردية في التراتب مبنية ولا تتطلب هذه المواصفة إلا أن يكون العنصر <Result> هو نفسه كما لو استخدم النموذج السابق.

وتتحدد في الفقرات التالية قاعدتان لهذه الوظيفة إحداهما للاستخدام في موارد الوثائق XML والأخرى في موارد غير الوثائق XML.

1.2.9 الموارد باللغة XML

هذه الفقرة معيارية ولكنها خيارية.

تصف هذه الفقرة قاعدة طلب النفاذ إلى كامل وثيقة XML أو إلى عنصر ما في تلك الوثيقة مع جميع عناصره الفرعية.

1.1.2.9 المعرف URI للمواصفة

يستعمل المعرف URI التالي كمعرف للوظائف التي يحددها هذا الجزء من هذه المواصفة:

```
urn:oasis:names:tc:xacml:2.0:profile:multiple:entire-hierarchy:xml
```

2.1.2.9 سياق الطلب الأصلي

يضم العنصر <Resource> في سياق الطلب الأصلي النعت "scope" مع القيمة "EntireHierarchy".

ويضم العنصر <Resource> في سياق الطلب الأصلي نعتاً واحداً "resource-id" مع نمط معطيات "urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression"، بحيث يكافئ العنصر <AttributeValue> مجموعة عقد تمثل تماماً عقدة واحدة في العنصر <ResourceContent>.

وقد يضم العنصر <Resource> في سياق الطلب الأصلي نعوتاً أخرى.

3.1.2.9 الدلالات

يجب أن تكون <Result> الطلب مساوية لتلك الناتجة عن المعالجة التالية. تستحدث إدارة السياق لكل عقدة في التراتب المطلوب سياق طلب جديد يضم عنصراً واحداً <Resource> له نعت "resource-id" مع نمط معطيات "urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression" وقيمة هي تعبير XPath تساوي مجموعة العقد التي تضم تماماً تلك العقدة الواحدة في العنصر <ResourceContent>. وتقدم إدارة السياق كل سياق طلب جديد إلى النقطة PDP لتقييمه، وتتتبع أثر العنصر <Decision> (القرار) في العناصر <Result> ذات الصلة. وإذا كانت نتيجة جميع سياقات الطلبات الجديدة حصراً "مسموح" (Permit) توضع <Result> واحدة تضم <Decision> قيمته "مسموح" في سياق الاستجابة المعادة إلى النقطة PEP. وإذا كانت نتيجة أي سياق طلب جديد "مرفوض" (Deny) أو "غير محدد" (Indeterminate) أو "غير قابل للتطبيق" (NotApplicable)، توضع نتيجة <Result> واحدة فيها قرار <Decision> "مرفوض" (Deny) في سياق الاستجابة المرسلة إلى النقطة PEP.

2.2.9 الموارد بغير اللغة XML

هذه الفقرة معيارية ولكنها خيارية.

تصف هذه الفقرة قواعد طلب النفاذ إلى كامل تراتب العقد في مورد تراتبي ما مختلف عن الوثائق XML.

1.2.2.9 المعرف URI

يستخدم المعرف URI التالي كمعرف الوظائف التي يحددها هذا الجزء من المواصفة:

```
urn:oasis:names:tc:xacml:2.0:profile:multiple:entire-hierarchy:non-xml
```

2.2.2.9 سياق الطلب الأصلي

يضم العنصر <Resource> في سياق الطلب الأصلي النعت "scope" مع القيمة "EntireHierarchy".

ويضم العنصر <Resource> في سياق الطلب الأصلي نعتاً واحداً "resource-id" يمثل عقدة واحدة في مورد تراتبي.

وقد يضم العنصر <Resource> في سياق الطلب الأصلي نعوتاً أخرى.

ويمكن استخدام تمثيل العقد في مورد تراتبي محدد في المواصفة XACML للموارد التراتبية في هذه التوصية من أجل تمثيل هوية العقدة الواحدة.

3.2.2.9 الدلالات

يجب أن تكون نتيجة <Result> هذا الطلب مساوية لتلك الناجمة عن المعالجة التالية. تستحدث كل إدارة سياق لكل عقدة في التراتب المطلوب، سياق طلب جديد يضم عنصر <Resource> واحداً مع النعت "resource-id" بقيمة هي هوية تلك العقدة الواحدة في التراتب. وتقدم إدارة السياق كل سياق طلب جديد إلى النقطة PDP للتقييم، وتتتبع أثر العنصر <Decision> في العناصر <Result> ذات الصلة. وإذا كانت نتيجة جميع سياقات الطلبات الجديدة حصراً "مسموح" (Permit) توضع نتيجة <Result> واحدة تضم "قرار" <Decision>"مسموح" (Permit) في سياق الاستجابة المرسلة إلى النقطة PEP. أما إذا كانت نتيجة أحد سياقات الطلبات الجديدة "مرفوض" (Deny)، أو "غير محدد" (Indeterminate)، أو "غير قابل للتطبيق" (NotApplicable)، فإن عنصر <Result> واحداً يضم <Decision> قيمته (مرفوض) (Deny) يوضع في سياق الاستجابة التي ترسل إلى النقطة PEP.

ولا تحدد اللغة XACML أو هذه المواصفة كيفية حصول إدارة السياق على المعلومات اللازمة لتحديد العقد إلا خلاف للعقدة المحددة في الأصل أو كيفية تمثيل هوية كل عقدة. ويمكن استخدام تمثيل العقد في مورد تراتبي محدد في المواصفة XACML للموارد التراتبية في هذه التوصية من أجل تمثيل هوية كل عقدة من هذا القبيل.

3.9 معرفات هوية النعت الجديد

يستخدم معرف الهوية التالي كمعرف AttributeId لنعت مورد يدل على نطاق (attribute "scope") ("النعت" (scope)) طلب نفاذ في عنصر واحد <Resource> في سياق الطلب.

```
urn:oasis:names:tc:xacml:2.0:resource:scope
```

ويجب أن يكون للنعت نمط المعطيات "http://www.w3.org/2001/XMLSchema#string".

وترد القيم الصالحة لهذا النعت لاحقاً في الفقرة 5.7. ويمكن أن يوفر تطبيق ما أي مجموعة فرعية من هذه القيم بما فيها المجموعة الفارغة.

- "فوري" (Immediate) – يحيل العنصر <Resource> إلى مورد وحيد غير تراتبي أو إلى عقدة وحيدة في مورد تراتبي. وهذه هي قيمة التغيب في حال عدم وجود نعت "scope". وتتم معالجة العنصر<Resource> بموجب الفقرة 7.
- "فروع" (Children) – يحيل العنصر <Resource> إلى عدة موارد في التراتب. وتتألف مجموعة الموارد من عقدة واحدة يرد وصفها في نعت المورد "resource-id" ومن جميع العقد الفروع المباشرة في التراتب. وتتم معالجة العنصر <Resource> وفقاً للفقرة 1.1.9 من هذه المواصفة.
- "أخلاف" (Descendants) – يحيل العنصر <Resource> إلى عدة موارد في التراتب. وتتألف مجموعة الموارد من عقدة وحيدة يصفها نعت المورد "resource-id" ومن جميع العقد الأخلاف في التراتب. وتتم معالجة العنصر <Resource> وفقاً للفقرة 1.1.9 من هذه المواصفة.
- "تعبير XPath" (XPath-expression) – يحيل العنصر <Resource> إلى عدة موارد في التراتب. وتتألف مجموعة الموارد من العقد ومجموعة عقد يصفها نعت المورد "resource-id". وتوجد كل من هذه العقد في العنصر <ResourceContent> من العنصر <Resource> وتتم معالجة العنصر<Resource> وفقاً للفقرة 2.1.9 من هذه المواصفة.
- "تراتب كامل" (EntireHierarchy) – يحيل العنصر <Resource> إلى مورد وحيد. ويتألف المورد من عقدة يصفها نعت المورد "resource-id" ومن جميع تلك العقد الأخلاف. وجميع العقد عقد في وثيقة XML مدرجة في العنصر <ResourceContent> من العنصر <Resource> وتتم معالجة العنصر <Resource> وفقاً للفقرة 2.9.

4.9 معرفات هوية مواصفة جديدة

تستخدم قيم المعرفات URI التالية كمعرفات URI للوظائف التي تحددها الفقرات المختلفة من هذه المواصفة:

- نعت "scope" التابع لـ "children" أو "descendants" في العنصر <Resource>: موارد XML

```
urn:oasis:names:tc:xacml:2.0:profile:multiple:scope:xml
```

- نعت "scope" التابع لـ "children" أو "descendants" في العنصر <Resource> : موارد غير XML

```
urn:oasis:names:tc:xacml:2.0:profile:multiple:scope:non-xml
```

- تعبير XPath في النعت "resource-id"

```
urn:oasis:names:tc:xacml:2.0:profile:multiple:xpath-expression
```

- عناصر <Resource> متعددة

```
urn:oasis:names:tc:xacml:2.0:profile:multiple:multiple-resource-
elements
```

- طلبات من تراتب كامل: موارد XML

```
urn:oasis:names:tc:xacml:2.0:profile:multiple:entire-hierarchy:xml
```

- طلبات لتراتب كامل: موارد غير XML

```
urn:oasis:names:tc:xacml:2.0:profile:multiple:entire-hierarchy:non-
xml
```

10 النسخة SAML 2.0 للمواصفة XACML

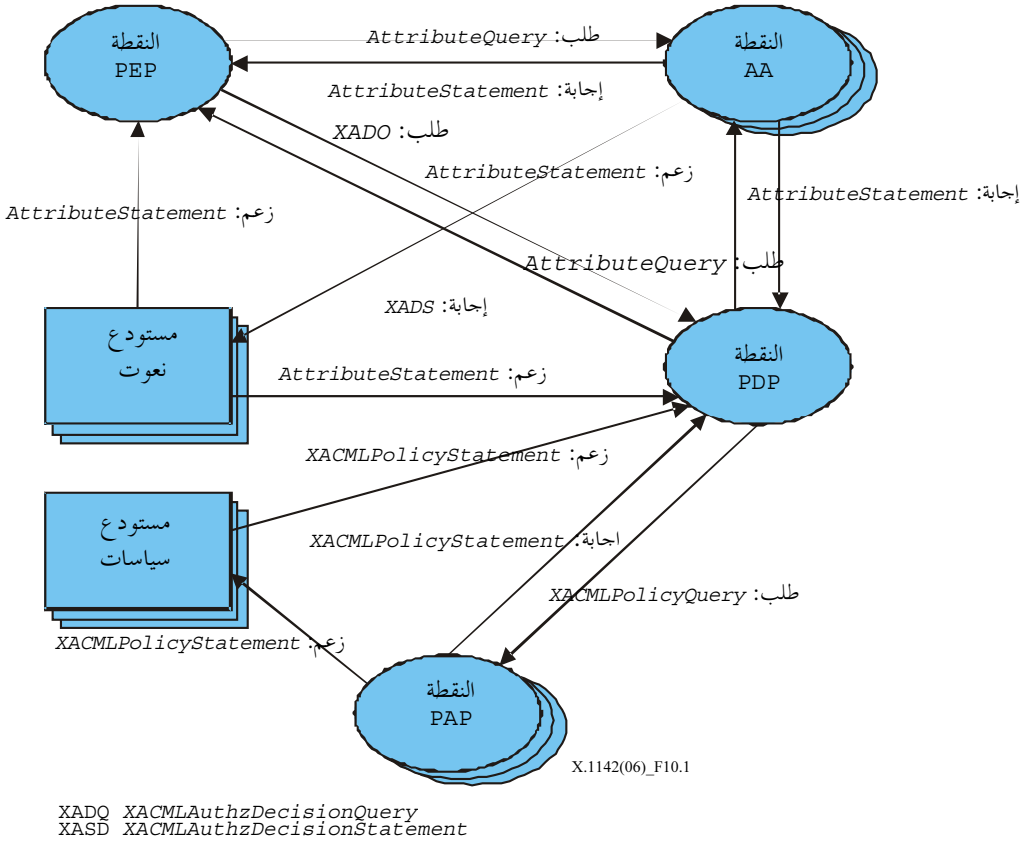
تحدد هذه الفقرة مواصفة بشأن كيفية استخدام النسخة SAML 2.0 (انظر التوصية ITU-T X.1141) من أجل حماية حالات النظام XACML ونقلها وطلبها ومعلومات أخرى يحتاجها تطبيق النظام XACML.

واللغة SAML هي إطار عمل قائم على اللغة XML لتبادل معلومات الأمن. ويعبر عن معلومات الأمن هذه في شكل مزاعم بشأن الجهات المستعملة. والجهة المستعملة كيان (إنسان أو آلة) له هوية تندرج في مجال أمن ما. وقد يضم زعم واحد عدة بيانات داخلية عن الاستيقان والترخيص والنعوت. وتعرف اللغة SAML بروتوكولاً يتمكن الزبائن من خلاله أن يطلبوا المزاعم من السلطات المعنية بالنظام SAML وأن يحصلوا على إجابة منها. ويمكن ضم هذا البروتوكول المكوَّن من أنساق رسائل طلب واستجابة قائمة على اللغة XML إلى بروتوكولات كثيرة مختلفة تتعلق بالاتصالات والنقل؛ وتحدد اللغة SAML عموماً وصلة مع البروتوكول SOAP في البروتوكول HTTP. وتستطيع سلطات النظام SAML عند استحداث استجاباتها استخدام موارد مختلفة للمعلومات مثل المخازن الخارجية للسياسات والمزاعم التي وصلت، في الطلبات الداخلة. وتحدد اللغة SAML عناصر المزاعم والجهات المستعملة والشروط والنصائح والبيانات.

وثمة ستة أنواع من الاستفسارات والبيانات المستخدمة في هذه الفقرة وهي:

1) AttributeQuery: طلب لغة SAML معياري يستعمل لطلب نعت واحد أو أكثر من سلطة النعوت.
2) AttributeStatement: بيان SAML معياري يضم نعتاً واحداً أو أكثر ويستخدم هذا البيان في إجابة SAML تصدر عن سلطة نعوت أو قد تستخدم كنسق للمزاعم SAML من أجل تخزين النعوت في مستودع نعوت.
3) XACMLPolicyQuery: توسيع طلب SAML محدد في هذه المواصفة ويستخدم في طلب سياسة واحدة أو أكثر من نقطة إدارة السياسة.
4) XACMLPolicyStatement: توسيع بيان SAML محدد في هذه المواصفة. ويستخدم في إجابة SAML صادرة عن نقطة إدارة السياسات أو في نسق المزاعم SAML من أجل تخزين السياسات في مستودع سياسات.
5) XACMLAuthzDecisionQuery: توسيع طلب SAML محدد في هذه المواصفة. وتستخدمه النقطة PEP في طلب قرار ترخيص من نقطة XACML PDP.
6) XACMLAuthzDecisionStatement: توسيع بيان SAML محدد في هذه المواصفة. ويمكن استخدامه في إجابة SAML تصدر عن نقطة XACML PDP. ويستخدم أيضاً في مزاعم SAML مستعملة كاعتمادات، ولكن هذا أمر لا يدخل في إطار نموذج استعمال XACML المحدد حالياً.

ويوضح الشكل التالي (10-1) نموذج استعمال اللغة XACML والرسائل المستخدمة في الاتصالات بين المكونات المختلفة. ولا تستخدم جميع المكونات في كل تطبيق.



الشكل X.1142/1-10 – نموذج استخدام اللغة XACML

وتصف هذه الفقرة جميع هذه الاستفسارات وعناصر مخطط البيان وكذلك كيفية استخدامها. كما تصف بعض الجوانب الأخرى لاستخدام اللغة SAML مع اللغة XACML. ولا تتطلب هذه التوصية أي تغيير أو توسيع للغة XACML، لكنها تحدد توسيعات للغة SAML.

وحرصاً على تحسين قابلية قراءة اللغة XML تفترض الأمثلة الواردة في هذه المواصفة استعمال التصريحات التالية للكيان الداخلي XML:

```
^lt;!ENTITY saml "urn:oasis:names:tc:SAML:2.0:assertion"
^lt;!ENTITY samlp "urn:oasis:names:tc:SAML:2.0:protocol"
^lt;!ENTITY xacml "urn:oasis:names:tc:xacml:2.0:"
^lt;!ENTITY xacml-context "urn:oasis:names:tc:xacml:2.0:context:schema:os"
^lt;!ENTITY xml "http://www.w3.org/2001/XMLSchema#"
^lt;!ENTITY subject-id "urn:oasis:names:tc:xacml:1.0:subject:subject-id"
^lt;!ENTITY resource "urn:oasis:names:tc:xacml:1.0:resource:"
^lt;!ENTITY resource-id "urn:oasis:names:tc:xacml:1.0:resource:resource-id"
^lt;!ENTITY action-id "urn:oasis:names:tc:xacml:1.0:action:action-id"
^lt;!ENTITY environment "urn:oasis:names:tc:xacml:1.0:environment:"
^lt;!ENTITY current-dateTime
    "urn:oasis:names:tc:xacml:1.0:environment:current-dateTime"
```

مثال: التعبير "&xml;#string" يعادل http://www.w3.org/2001/XMLSchema#string. ومكان الاسم المصاحب للمخطط XACML الذي يوسع مخطط مزعم اللغة SAML هو:

```
xacml-saml="urn:oasis:names:tc:xacml:2.0:saml:assertion:schema:os"
```

ومكان الاسم المصاحب للمخطط XACML الذي يوسع مخطط البروتوكول SAML هو:

```
xacml-samlp="urn:oasis:names:tc:xacml:2.0:saml:protocol:schema:os"
```

1.10 تقابل بين النعوت SAML والنعوت XACML

يحدد مخطط مزاعم اللغة SAML مزاعم نعت ما. ويحدد مخطط البروتوكول SAML معلمة AttributeQuery تستخدم في طلب حالات مزاعم النعت وإجابة تضم الحالات المطلوبة. وقد تستخدم الأنظمة المستعملة للغة XACML حالات من النعوت SAML لإرسال وتخزين هذه العناصر SAML. وقد تستخدم الأنظمة XACML بروتوكول AttributeQuery في طلب حالات نعوت SAML. ويجب إجراء تقابل بين النعوت SAML والنعوت XACML لكي يمكن استعمال النعوت SAML في سياق طلب XACML.

ومزعم نعت SAML هو حالة <saml:Assertion> تضم حالة <saml:AttributeStatement> واحدة أو أكثر تضم كل منها حالة <saml:Attribute> واحدة أو أكثر.

ويجب على كل نعت XACML في مزعم نعت SAML من أجل استعماله في سياق طلب SAML أن يتمثل لمواصفة النعوت *XACML Attribute profile* مكان الاسم urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML الواردة في التوصية ITU-T. X.1141.

ويوضع العنصر <xacml-context:Attribute> استناداً إلى العنصر <saml:Attribute> المقابل في مزعم النعت SAML على النحو التالي:

- النعت XACML AttributeId XML
  - تستعمل القيمة المقدرة كاملة للنعت Name XML <saml:Attribute>.
- النعت XACML DataType XML
  - تستعمل القيمة المقدرة كاملة للنعت DataType XML <saml:Attribute> وإذا فُقد النعت DataType XML <saml:Attribute> يصبح النعت DataType XACML XML http://www.w3.org/2001/XMLSchema#string.
- النعت XACML Issuer XML
  - تستعمل قيمة السلسلة للعنصر <saml:Issuer> من مزعم النعت SAML.
- العنصر <xacml-context:AttributeValue>
  - تستعمل القيمة <saml:AttributeValue> كقيمة للعنصر <xacml-context:AttributeValue>.

ويتم تقابل كل حالة <saml:Attribute> مع عنصر <xacml-context:Attribute> واحد. ولا تحتاج جميع حالات <saml:Attribute> في مزعم نعت SAML إلى التقابل؛ ويجوز انتقاء حالات النعت SAML التي تحتاج إلى التقابل باستعمال آلية ليست محددة هنا. ويستعمل النعت Issuer (الجهة المنتجة) للعنصر <saml:Assertion> كجهة منتجة لكل عنصر <xacml-context:Attribute> مستحدث.

ويوضع العنصر <xacml-context:Attribute> المستحدث استناداً إلى <saml:Assertion> في العنصر <xacml-context:Resource> أو <xacml-context:Subject> أو <xacml-context:Action> أو <xacml-context:Environment> الذي يناظر الكيان <saml:Subject> في مزعم النعت SAML. وعلى سبيل المثال، إذا كانت الجهة المستعملة لمزعم النعت SAML تضم عنصر <saml:NameIdentifier> وكانت قيمة NameIdentifier متوائمة مع القيمة <xacml-context:Attribute> التي تحتوي على معرف AttributeId للنعت &resource;resource-id، فإن حالات <xacml-context:Attribute> المستحدثة استناداً إلى حالات <saml:Attribute> في مزعم ذلك النعت SAML يجب وضعها في العنصر <xacml-context:Resource>. وإذا وضع العنصر <xacml-context:Attribute> في عنصر <xacml-context:Subject> يجب أيضاً أن يكون النعت XACML SubjectCategory XML متسقاً مع الكيان الذي يشكل موضوع العنصر <saml:Assertion>.

يتعين على الكيان الذي يقوم بعملية التقابل أنه تم التقيد بالدلالات التي تحددها اللغة SAML للعناصر في <saml:Assertion>. ولا حاجة لكيان التقابل أن يجري بنفسه عمليات التحقق من الدلالات هذه، لكن عليه أن يتأكد من أن إجراء هذه العمليات قد تم قبل استعمال النقطة XACML PDP لأي عنصر <xacml:Attribute> استحدث من <saml:Assertion>. وتضم عمليات التحقق من الدلالة في جملة أمور أخرى ما يلي:

- ينبغي أن تكون كل النعوت NotBefore وXML NotOnOrAfter في العنصر <saml:Assertion> صالحة فيما يتعلق بالعنصر <xacml:Request> الذي يضم <xacml:Attribute> المشتق من SAML والمستخدم. وذلك يعني أن قيم النعت NotBefore وXML NotOnOrAfter ينبغي أن تكون متسقة مع القيم &environment;current-time و&environment;current-date و&environment:current-dateTime <xacml:Attribute> المصاحبة للعنصر <xacml:Request>.

- ينبغي أن يتأكد الكيان الذي يقوم بالتقابل من التقيد بالدلالات التي تحددها اللغة SAML لكل عنصر <saml:AudienceRestrictionCondition> أو <saml:DoNotCacheCondition>.
- إذا ظهر عنصر <ds:Signature> في <saml:Assertion> فإنه يجب على الكيان الذي يقوم بالتقابل أن يتأكد من صلاحية التوقيع ومن اتساق العنصر <Issuer> SAML مع القيمة <ds:X509IssuerName> الموجودة في التوقيع. وينبغي التقيد بالخطوط التوجيهية الواردة في التوصية ITU-T X.1141 فيما يتعلق بالتواقيع الرقمية.

2.10 قرارات الترخيص

تحدد المواصفة SAML 2.0 استجواب قرار ترخيص AuthzDecisionQuery أولي (انظر التوصية ITU-T X.1141). والاستجواب SAML AuthzDecisionQuery غير قادر على نقل جميع المعلومات التي تتمكن النقطة XACML PDP من قبولها كجزء من سياق طلبها. كما أن البيان SAML AuthzDecisionStatement غير قادر على نقل جميع المعلومات التي يضمها سياق الاستجابة XACML.

ولكي يتاح لنقطة PEP أن تستعمل قواعد تركيب الطلب والاستجابة SAML مع الدعم الكامل لقواعد سياق الطلب وسياق الاستجابة XACML تحدد هذه التوصية إمكانيتين للتوسع SAML هما:

- الاستجواب <xacml-samlp:XACMLAuthzDecisionQuery> وهو استجواب SAML يوسع مخطط البروتوكول SAML (انظر التوصية ITU-T X.1141). ويتيح هذا الاستجواب للنقطة PEP تقديم سياق طلب XACML في طلب SAML مع معلومات أخرى.
- البيان <xacml-saml:XACMLAuthzDecisionStatement> وهو بيان SAML يوسع مخطط المزاعم SAML (انظر التوصية ITU-T X.1141). وهو يتيح لنقطة XACML PDP أن تعيد سياق استجابة XACML في الإجابة على البيان <XACMLAuthzDecisionStatement> مع معلومات أخرى. وهو يتيح أيضاً تخزين سياق استجابة XACML أو إرساله على شكل مزعم SAML.

1.2.10 العنصر <XACMLAuthzDecisionQuery>

تستخدم نقطة PEP العنصر <XACMLAuthzDecisionQuery> في طلب قرار ترخيص من نقطة XACML PDP. ويتيح هذا العنصر لطلب SAML نقل حالة سياق طلب XACML.

```
<xs:element name="XACMLAuthzDecisionQuery" type="XACMLAuthzDecisionQueryType"/>
<xs:complexType name="XACMLAuthzDecisionQueryType">
  <xs:complexContent>
   <xs:extension base="samlp:RequestAbstractType">
    <xs:sequence>
        <xs:element ref="xacml-context:Request"/>
    </xs:sequence>
    <xs:attribute name="InputContextOnly" type="boolean" use="optional" default="false"/>
    <xs:attribute name="ReturnContext" type="boolean" use="optional" default="false"/>
   </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

والعنصر <XACMLAuthzDecisionQuery> هو نمط معقد **XACMLAuthzDecisionQueryType**. وهذا النمط هو بديل للاستجواب <samlp:AuthzDecisionQuery> الذي يسمح للنقطة PEP باستعمال المقدرات الكاملة لنقطة XACML PDP.

ويضم العنصر <XACMLAuthzDecisionQuery> النعوت والعناصر XML التالية:

– InputContextOnly [قيمة التغيب "false"]

يحكم هذا النعت XML موارد المعلومات التي يُسمح للنقطة PDP باستعمالها في إعداد قرار ترخيصها. وإذا كان هذا النعت "true" XML توجب أخذ قرار الترخيص على أساس المعلومات الموجودة في <XACMLAuthzDecisionQuery> لا غير؛ ولا يجوز استخدام أي نعوت خارجية. أما إذا كان هذا النعت XML "false" فإنه يجوز إصدار قرار الترخيص استناداً إلى نعوت خارجية غير متضمنة في <XACMLAuthzDecisionQuery>.

– ReturnContext [قيمة التغيب "false"]

يتيح هذا النعت XML للنقطة PEP أن تطلب إدراج عنصر <xacml-context:Request> في العنصر <XACMLAuthzDecisionStatement> الناتج عن الطلب. وهو يتحكم أيضاً بمحتويات ذلك العنصر <xacml-context:Request>.

وإذا كان هذا النعت XML "true"، توجب على النقطة PDP أن تدرج <xacml-context:Request> في العنصر <XACMLAuthzDecisionStatement> الموجود في <XACMLResponse>. ويدرج هذا العنصر

<xacml-context:Request> جميع النعوت التي توفرها النقطة PEP في الاستجواب <XACMLAuthzDecisionQuery> الذي استعملته لإعداد قرار الترخيص. وقد تدرج النقطة PDP نعوتاً إضافية في هذا العنصر <xacml-context:Request> مثل نعوت خارجية تحصل عليها النقطة PDP وتستخدم في إعداد قرار الترخيص أو نعوت أخرى تعرفها النقطة PDP وقد تستفيد منها النقطة PEP في إعداد طلبات <XACMLAuthzDecisionQuery> لاحقة.

وإذا كان هذا النعت XML "false"، فإن النقطة PDP عندئذٍ لا تضم العنصر <xacml-context:Request> في العنصر <XACMLAuthzDecisionStatement> الاستجابة <XACMLResponse>.

- <xacml-context:Request> [مطلوب]

وهو سياق طلب XACML.

2.2.10 العنصر <XACMLAuthzDecisionStatement>

يجوز للنقطة XACML PDP أن تستخدم العنصر <XACMLAuthzDecisionStatement> في إرسال إجابة SAML تضم سياق إجابة XACML إلى النقطة PEP رداً على استجواب <XACMLAuthzDecisionQuery>. ويجوز أيضاً استخدام هذا العنصر في مزعم SAML كنسق لتخزين قرار ترخيص في مستودع.

```
<xs:element name="XACMLAuthzDecisionStatement" type="xacml-
saml:XACMLAuthzDecisionStatementType"/>
<xs:complexType name="XACMLAuthzDecisionStatementType">
  <xs:complexContent>
    <xs:extension base="saml:StatementAbstractType">
      <xs:sequence>
        <xs:element ref="xacml-context:Response"/>
          <xs:element ref="xacml-context:Request" MinOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

والعنصر <XACMLAuthzDecisionStatement> هو من النمط المعقد **XACMLAuthzDecisionStatementType** وهذا العنصر هو بديل للعنصر <samlp:AuthzDecisionStatement> المحدد في اللغة SAML والذي يتيح للمزعم SAML أن يضم كامل محتوى الاستجابة الواردة من النقطة XACML PDP.

ويضم العنصر <XACMLAuthzDecisionStatement> العناصر التالية:

- <xacml-context:Response> [إلزامي]

وهو سياق الإجابة XACML الذي استحدثته النقطة XACML PDP رداً على الاستجواب <XACMLAuthzDecisionQuery>.

- <xacml-context:Request> [خياري]

وهو طلب <xacml-context:Request> يضم نعوت XACML أرسلتها XACML PDP رداً على الاستجواب <XACMLAuthzDecisionQuery>. ويدرج هذا العنصر إذا كان النعت XML ReturnResponse في <XACMLAuthzDecisionQuery> "true". أما إذا كان هذا النعت "false" فلا يدرج العنصر المذكور.

3.10 السياسات

تحدد السياسة XACML عنصرين لمخطط السياسة هما: <Policy> و<PolicySet>. ولا تحدد اللغة SAML أي بروتوكول أو مخططات مزاعم خاصة بالسياسات. وتحدد هذه الفقرة توسيعات SAML جديدة للعنصرين <XACMLPolicyQuery> و<XACMLPolicyStatement>. ويمكن استعمال حالات هذين العنصرين الجديدين لطلب وإرسال وتخزين حالات <Policy> و <PolicySet> للغة XACML.

1.3.10 العنصر <XACMLPolicyQuery>

تستخدم النقطة PDP العنصر <XACMLPolicyQuery> في طلب حالة واحدة أو أكثر للعنصر policy أو PolicySet للغة XACML من نقطة إدارة سياسة على الخط كجزء من طلب SAML.

```
<xs:element name="XACMLPolicyQuery" type="XACMLPolicyQueryType"/>
<xs:complexType name="XACMLPolicyQueryType">
   <complexContent>
```

```
          <xs:extension base="samlp:RequestAbstractType">
                <xs:choice minOccurs="0" maxOccurs="unbounded">
                      <xs:element ref="xacml-context:Request"/>
                      <xs:element ref="xacml:Target"/>
                      <xs:element ref="xacml:PolicySetIdReference"/>
                      <xs:element ref="xacml:PolicyIdReference"/>
                </xs:choice>
          </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

والعنصر <XACMLPolicyQuery> هو من النمط المعقد **XACMLPolicyQueryType**.

ويضم العنصر <XACMLPolicyQuery> عنصراً واحداً أو أكثر من العناصر التالية:

- <xacml-context:Request> [أي عدد]

وهو يوفر سياق طلب XACML. ويجب إعادة جميع حالات السياسة ومجموعات PolicySet للغة XACML التي تطبق في هذا الطلب.

- <xacml:Target> [أي عدد]

وهو يوفر <Target> XACML. ويجب إعادة جميع حالات السياسة والمجموعات وPolicySet في اللغة XACML التي تطبق على هذا العنصر <Target>.

- <xacml:PolicySetIdReference> [أي عدد]

وهو يحدد العنصر <PolicySet> XACML الذي ينبغي إعادته.

- <xacml:PolicyIdReference> [أي عدد]

وهو يحدد العنصر <Policy> XACML الذي ينبغي إعادته.

2.3.10 العنصر <XACMLPolicyStatement>

تستخدم نقطة إدارة السياسة البيان <XACMLPolicyStatement> من أجل أن تعيد حالة واحدة أو أكثر لعنصر <Policy> أو <PolicySet> للغة SAML في إجابة SAML رداً على طلب <XACMLPolicyQuery>. ويجوز أيضاً استخدام البيان <XACMLPolicyStatement> في مزعم SAML كنسق لتخزين العنصر <XACMLPolicyStatement>.

```
<xs:element name="XACMLPolicyStatement" type="xacml-
saml:XACMLPolicyStatementType"/>
<xs:complexType name="XACMLPolicyStatementType">
    <xs:complexContent>
          <xs:extension base="saml:StatementAbstractType">
                <xs:choice minOccurs="0" maxOccurs=unbounded">
                      <xs:element ref="xacml:Policy"/>
                      <xs:element ref="xacmlPolicySet"/>
                </xs:choice>
                </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

والعنصر <XACMLPolicyStatement> هو من النمط المعقد **XACMLPolicyStatementType**.

ويضم العنصر <XACMLPolicyStatement> العناصر التالية. وإذا صدر العنصر <XACMLPolicyStatement> رداً على استجواب <XACMLPolicyQuery>، ولم يستوف أي حالة عنصر <xacml:Policy> أو <xacml:PolicySet> المواصفات المصاحبة للاستجواب <XACMLPolicyQuery> فلن يوجد أي عنصر في <XACMLPolicyStatement>.

- <xacml:Policy> [أي عدد]

وهي حالة <xacml:Policy> تستوفي المواصفات المصاحبة للاستجواب <XACMLPolicyQuery>، إن وجدت.

- <xacml:PolicySet> [أي عدد]

وهي حالة <xacml:PolicySet> تستوفي المواصفات المصاحبة للاستجواب <XACMLPolicyQuery>، إن وجدت.

4.10 العنصر <saml:Assertion>

يغلف عنصر <XACMLAuthzDecisionStatement> أو <XACMLPolicyStatement> أو <saml:AttributeStatement> معياري SAML في عنصر <saml:Assertion> قد يكون موقَّع.

ومعظم مكونات <saml:Assertion> محددة كاملة في التوصية ITU-T X.1141. وتتحدد العناصر والنعوت XML التالية هنا للاستخدام مع أنماط البيانات SAML المحددة والمستخدمة في هذه المواصفة.

ولا تفرض هذه المواصفة أي متطلبات أو تقييدات على المعلومات في العنصر <saml:Assertion> باستثناء تلك التي ترد هنا.

1.4.10 العنصر <saml:Issuer>

العنصر <saml:Issuer> هو عنصر مطلوب لالتقاط المعلومات بشأن "السلطة SAML التي تعد الطلب (الطلبات) في المزاعم".

ولا تتطلب هذه المواصفة أن تكون الهوية المتاحة <saml:Issuer> متسقة مع هوية الموقِّع من أجل توفير تواقيع رقمية لطرف ثالث. وتقع على الجهة المستعملة مسؤولية إقامة علاقة ثقة مناسبة مع السلطة التي توقِّع المزاعم <saml:Assertion>.

وعند استخدام <saml:AttributeAssertion> في إنشاء نعت XACML، تستعمل قيمة السلسلة للعنصر <saml:Issuer> كقيمة نعت XACML Issuer XML بحيث تتحدد القيمة SAML مع مراعاة هذه النقطة.

2.4.10 العنصر <ds:Signature>

العنصر <ds:Signature> عنصر خياري لالتقاط "توقيع XML يستيقن المزعم".

ويستخدم عنصر <ds:Signature> في مزعم مستعمل مع بيان XACML. ولا تشترط هذه المواصفة أن تكون الهوية المتاحة في العنصر <saml:Issuer> متسقةً مع هوية الموقِّع من أجل توفير تواقيع رقمية لطرف ثالث. وتقع على الجهة المستعملة مسؤولية إقامة علاقة ثقة مناسبة مع السلطة التي توقِّع <saml:Assertion>.

وينبغي أن يتحقق الطرف المستعمل من أي توقيع مدرج في مزعم وينبغي ألاّ يستعمل معلومات مشتقة من المزاعم إلاّ إذا تم التحقق من التوقيع بنجاح.

3.4.10 العنصر <saml:Subject>

العنصر <saml:Subject> هو عنصر خياري يستعمل لالتقاط "الجهة المستعملة للبيان (للبيانات) في المزعم".

ولا يدرج العنصر <saml:Subject> في مزعم يتضمن <XACMLAuthzDecision> أو <XACMLPolicy>.

ويضم العنصر <saml:Subject> في عنصر <saml:AttributeAssertion> يتعين تقابله مع نعت XACML هوية الكيان الذي يربط به النعت وقيمته. وينبغي أن تكون هذه الهوية فيما يتعلق بنعت <Subject> XACML، متسقة مع قيمة أي نعت XACML &subject-id يظهر في نفس العنصر <Subject>.

وفيما يتعلق بنعت <Resource> XACML ينبغي أن تكون هذه الهوية متسقة مع قيمة أي نعت XACML &resource-id يظهر في نفس العنصر <Resource>. وفيما يخص النعت <Action> XACML، ينبغي أن تكون هذه الهوية متسقة مع قيمة أي نعت XACML &action-id تظهر في نفس العنصر <Action>. وفيما يتعلق بالنعت <Environment> XACML، ينبغي أن تكون هذه الهوية متسقة مع قيمة أي نعت XACML يظهر في نفس العنصر <Environment> ويعطي هوية بيئة ما.

4.4.10 العنصر <saml:Conditions>

العنصر <saml:Conditions> هو عنصر خياري يستخدم لأغراض "الظروف التي يجب مراعاتها عند تقدير صلاحية المزعم و/أو استعماله".

وينبغي أن يضم العنصر <saml:Conditions> النعتين NotBefore وNotOnOrAfter للغة XML من أجل تحديد حدود صلاحية مزعم ما. وينبغي أن يتأكد الطرف المستخدم في حالة وجود هذين النعتين XML، من أجل النقطة PDP تستعمل المعلومات المأخوذة من المزعم من أجل تقييم السياسات عندما تكون قيمة نعت المورد &current-dateTime لسياق الطلب ضمن فترة الصلاحية التي يحددها المزعم.

5.10 العنصر <samlp:RequestAbstractType>

يجب تغليف عنصر <XACMLAuthzDecisionQuery> أو <XACMLPolicyQuery> في عنصر <samlp:RequestAbstractType> يمكن توقيعه.

ومعظم مكونات العنصر <samlp:RequestAbstractType> محددة بالكامل في التوصية ITU-T X.1141. ويجب استعمال العنصر<saml:Issuer> والعنصر <ds:Signature> مع أنماط الاستجواب SAML المحددة والمستخدمة في هذه المواصفة بنفس الطريقة

المحددة في الفقرة السابقة. ولا تفرض هذه المواصفة أي متطلبات أو تغييرات على المعلومات في العنصر <samlp:RequestAbstractType>.

1.5.10 العنصر <saml:Issuer>

انظر العنصر <saml:Issuer> في الفقرة 1.4.10.

2.5.10 العنصر <ds:Signature>

انظر العنصر <ds:Signature> في الفقرة 2.4.10.

6.10 العنصر <samlp:Response>

يجب إدراج عنصر <XACMLAuthzDecisionStatement> أو <XACMLPolicyStatement> في عنصر <samlp:Response> يمكن توقيعه.

ومعظم مكونات العنصر <samlp:Response> محددة بالكامل في التوصية ITU-T X.1141. والعناصر والنعوت XML التالية محددة أيضاً هنا لاستخدامها مع أنماط بيانات SAML محددة ومستعملة في هذه المواصفة. ولا تفرض هذه المواصفة أي متطلبات أو تقييدات على المعلومات الواردة في العنصر <samlp:Response>.

1.6.10 العنصر <samlp:Issuer>

انظر العنصر <saml:Issuer> في الفقرة 1.4.10.

2.6.10 العنصر Element <ds:Signature>

انظر العنصر <ds:Signature> في الفقرة 2.4.10.

3.6.10 العنصر <samlp:StatusCode>

العنصر <samlp:StatusCode> هو مكونة من العنصر <samlp:Status> في العنصر <samlp:Response>.

1.3.6.10 الإجابة على <XACMLAuthzDecisionQuery>

في الإجابة على الطلب <XACMLAuthzDecisionQuery>، يجب أن يرتبط النعت <samlp:StatusCode> بالعنصر <xacml:StatusCode> من العنصر <xacml:Status> لقرار الترخيص على النحو التالي:

(1 urn:oasis:names:tc:SAML:2.0:status:Success

تستعمل هذه القيمة لنعت XML القيمة <samlp:StatusCode> إذا كانت القيمة <xacml:StatusCode> هي urn:oasis:names:tc:xacml:1.0:status:ok.

(2 urn:oasis:names:tc:SAML:2.0:status:Requester

تستعمل هذه القيمة لنعت XML القيمة <samlp:StatusCode> عندما تكون القيمة <xacml:StatusCode> urn:oasis:names:tc:xacml:1.0:status:missing-attribute أو عندما تكون القيمة <xacml:StatusCode> urn:oasis:names:tc:xacml:1.0:status:syntax-error ناجمة عن خطأ تركيب في الطلب <xacml:Request>.

(3 urn:oasis:names:tc:SAML:2.0:status:Responder

تستعمل هذه القيمة للنعت XML للقيمة <samlp:StatusCode> عندما تكون القيمة <xacml:StatusCode> هي: urn:oasis:names:tc:xacml:1.0:status:syntax-error ناجمة عن خطأ تركيب في <xacml:Policy> أو <xacml:PolicySet>. ويلاحظ أن جميع أخطاء التركيب في السياسات لن تكشف بالارتباط مع معالجة طلب ما، وبالتالي فلن تنقل جميع أخطاء تركيب السياسة بهذه الطريقة.

(4 urn:oasis:names:tc:SAML:2.0:status:VersionMismatch

لا تستعمل هذه القيمة لنعت XML للقيمة <samlp:StatusCode> إلا عندما لا يوفر السطح البيني SAML في النقطة PDP نسخة رسالة الطلب SAML.

2.3.6.10 الإجابة على الطلب < XACMLPolicyQuery >

في الإجابة على الطلب <XACMLPolicyQuery>، يكون نعت XML للقيمة <samlp:StatusCode> على النحو الذي تحدده التوصية ITU-T X.1141.

11 مواصفة التوقيع الرقمي XML

تعرض هذه الفقرة مواصفةً تستخدم مع التوقيع W3C Signature:2002 من أجل توفير الاستيقان وحماية التكاملية في حالات نظام اللغة XACML.

لا يستعمل التوقيع الرقمي لتوفير الاستيقان وحماية التكاملية إلاّ إذا ضمت المعلومات الموقعة مواصفة هوية الموقع ومواصفة فترة صلاحية غرض المعطيات الموقعة. ولا تحدد اللغة XACML ذاتها نسق معلومات من هذا القبيل نظراً إلى أنه يفترض باللغة XACML أن تستخدم معايير أخرى للوظائف غير المواصفة الراهنة وتقييم سياسات التحكم في النفاذ وطلباته واستجاباته.

وقد تحدد نسق واحد مناسب في اللغة SAML. وتضم الفقرة 10 تعريف مواصفة لاستعمال اللغة SAML مع حالات المخطط XACML. وتوصي هذه المواصفة باستعمال حالات المخطط XACML في مزاعم اللغة SAML وطلباتها وإجاباتها مما يمكن توقيعه رقمياً على النحو المحدد في التوصية ITU-T X.1141.

1.11 استعمال اللغة SAML

توصي المواصفة باستخدام حالات المخطط XACML المدرجة في مزاعم وطلبات وإجابات اللغة SAML كما يرد وصفها في الفقرة 10. ويتم توقيع هذه الأغراض SAML رقمياً كما يرد في الفقرة 4.8 من التوصية X.1141 "التوقيع والتركيب والمعالجة في اللغتين *SAML* و*XML*".

2.11 التقنين

يجب أن يكون تدفق الأثمونات الموقع مماثلاً للتدفق الذي يتم التحقق منه من أجل أن يتحقق الطرف ذا الصلة من توقيع رقمي. وضماناً لذلك يجب أن يتم تقنين الوثيقة XML الموقعة (انظر التقنين W3C :2002). وتحدد التوصية ITU-T X.1141 استعمال التقنين الحصري (انظر التقنين W3C :2002).

1.2.11 عناصر مكان الاسم في أغراض المعطيات XACML

يجب أن يحدد أي غرض معطيات XACML ينبغي توقيعه جميع عناصر مكان الاسم المستعملة في هذا الغرض. وإلاّ فإن هذا الغرض سيجتذب معاريف اسم المكان من أسلاف غرض المعطيات التي قد تختلف من غلاف إلى آخر.

وعند استعمال التقنين الحصري كتقنين أو كطريقة تحويل، يجب ضم اسم المكان في المخططات XACML الذي تستخدمه عناصر غرض معطيات XACML إلى السوابق وإدراجه في معلمة `InclusiveNamespacesPrefixList` في الموقع http://www.w3.org/2001/10/xml-exc-c14n# (انظر التقنين W3C :2002).

2.2.11 اعتبارات إضافية خاصة بالتقنين

يجب عادة إجراء تحويلات إضافية بشأن غرض المعطيات XACML من أجل ضمان مواءمة غرض المعطيات الموقع مع غرض المعطيات الذي يتم التحقق منه. وتعدد هذه المواصفة بعض هذه التحويلات لكنها لا تعمل على تحديد خوارزميات لإجرائها.

وإذا ضم غرض معطيات XACML عناصر معطيات قد تظهر في أكثر من شكل واحد (مثل TRUE وFALSE)، و(1، 0)، و(true وfalse))، فإنه يجب تعريف وتحديد طريقة تحويل تقييس تلك العناصر.

وتوصي هذه المواصفة بتطبيق القوانين التالية على قيم أنماط المعطيات المقابلة لها سواء ظهرت في قيم نعوت XML أو في نعوت XACML.

1) عندما يعرف تمثيل قانوني لنمط معطيات XACML في المخطط http://www.w3.org/2001/XMLSchema، يجب أن توضع قيمة نمط المعطيات في الشكل القانوني المحدد في http://www.w3.org/2001/XMLSchema. ويتضمن ذلك التنسيق البولاني {"true"، "false"}، والمعلمات double وdateTime وtime وdate وhexBinary (الحروف الكبيرة).
2) http://www.w3.org/2001/XMLSchema#anyURI – استخدام الشكل النظامي المحدد في المعيار IETF RFC 2396.
3) http://www.w3.org/2001/XMLSchema#base64Binary – إلغاء جميع الانقطاعات بين السطور والفراغات. وإلغاء جميع السمات التالية للتابع الأول من السمات "=". يجوز استعمال التحويل Base64 (المعرف: http://www.w3.org/TR/xmldsig-core/#sec-Base-64).
4) `urn:oasis:names:tc:xacml:1.0:data-type:x500Name` – التقييس أولاً وفقاً للمعيار IETF RFC 2253. وإذا تضمن أي اسم RDN عدة أزواج معلمات `attributeTypeAndValue` يعاد ترتيب المعلمة `AttributeValuePairs` في ذلك الاسم RDN في ترتيب تصاعدي عند مقارنتها كسلسلات أثمونات (انظر الفقرة 6.11 من التوصية X.690).
5) urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name – تقييس جزء المجال للاسم بالحروف الصغيرة.

6) التعبير XPath – تطبيق المعرف http://www.w3.org/2002/06/xmldsig-filter2 من أجل وضع التعبير XPath في شكل نظامي.

3.11 مخططات التوقيع

يتوقف تحليل كل غرض معطيات XACML على الحصول على نسخة دقيقة من جميع المخططات التي تتبع لها أغراض المعطيات XACML. ويلاحظ أن إدراج معرف URI في نعوت حالة مخطط XACML لا يضمن أن نسخة دقيقة من المخطط ستستعمل: فقد يضع مهاجم ما مخططاً مزيفاً يضم معرفاً صحيحاً. وتساعد التواقيع على الحماية من تبديل أو تغيير المخططات التي يتبع لها غرض المعطيات XACML. ويرد وصف استعمال التواقيع لهذا الغرض في هذه الفقرة.

وينبغي في معظم الحالات أن يضم موقع غرض المعطيات عنصر <Reference> لكل مخطط يتبع له غرض المعطيات XACML في العنصر <SignedInfo> الذي يضم العنصر المحيل <Reference> إلى غرض المعطيات XACML ذاته أو يتضمنه.

وفي بعض الحالات يعرف موقع غرض المعطيات أن جميع النقاط PDP التي ستقيم غرض معطيات XACML معين ستحصل على نسخ دقيقة من بعض المخططات اللازمة لتحليل غرض المعطيات، ولا يريد أن يلزم النقطة PDP بالتحقق من موجز الرسالة لهذه المخططات. وفي هذه الحالات يجوز لموقع غرض المعطيات أن يحذف العناصر <Reference> لأي مخطط لا حاجة للتحقق منه.

12 مواصفة مورد تراتبي في اللغة XACML

هذه الحالة هي غالباً الحالة التي ينتظم فيها المورد على نحو تراتبي. وتتضمن الأمثلة أنظمة الملفات والوثائق XML والتنظيمات. وتحدد هذه الفقرة كيفية توفير اللغة XACML تحكماً في النفاذ إلى مورد منظم على نحو تراتبي.

في أي شيء تختلف الموارد المنظمة على نحو تراتبي؟ أولاً، غالباً ما تطبق السياسات على التراتب نفس عمليات التحكم في النفاذ إلى كامل فروع التراتب. والقدرة على وضع تقييد واحد للسياسة يطبق على كامل فروع العقد في التراتب بدلاً من ضرورة تحديد تقييد مختلف لكل عقدة تزيد من سهولة الاستعمال ومن احتمال أن السياسة ستعكس بدقة عمليات التحكم في النفاذ المطلوبة. وتكمن إحدى الخصائص الأخرى للموارد التراتبية في أن النفاذ إلى عقدة ما قد يرتبط بقيمة عقدة أخرى. على سبيل المثال قد يكون للمريض نفاذ مضمون إلى عقدة "التشخيص" في السجل الطبي للوثيقة XML إذا تواءم اسم المريض مع القيمة في عقدة "اسم المريض". وفي هذه الحالة لا تستطيع العقدة المطلوبة أن تعمل بمعزل عن باقي العقد في التراتب، ويجب أن يتوفر للنقطة PDP نفاذ إلى قيم العقد الأخرى وأخيراً، كثيراً ما ترتبط هوية العقد في تراتب ما بموقع العقدة في هذا التراتب؛ وهناك أيضاً عدة طرق لوصف هوية عقدة ما، ومن أجل تطبيق السياسات على العقد كما هو مطلوب، يجب إيلاء الاهتمام بالتمثيل المتسق لهوية العقد. وإلاّ فقد يتحايل طالب ما على التحكم في النفاذ بأن يطلب عقدة تستعمل هوية مختلفة عن تلك المستعملة في السياسة.

وقد يكون المورد التراتبي "شجرة" (تراتب ذو جذر واحد) أو "غابة" (تراتب ذو جذور متعددة)، لكن التراتب قد لا يكون له دورات. والمصطلح الآخر لهذين النمطين من التراتب هو "خط لا دوري موجه" أو "DAG". وتسمى جميع الموارد من هذا القبيل في هذه المواصفة موارد تراتبية. وتنتظم الوثيقة XML دائماً على شكل "شجرة". وقد تنتظم أنماط أخرى للموارد التراتبية مثل الملفات في نظام ملفات يوفر وصلات، على شكل "غابات".

وتعالج العقد في مورد تراتبي كموارد متفرقة. ولا يفترض قرار ترخيص يسمح بالنفاذ إلى عقدة داخلية أن النفاذ إلى عقدها الأخلاف مسموح. ولا يفترض قرار ترخيص يرفض النفاذ إلى عقدة داخلية ما أن النفاذ إلى عقدها الأخلاف مرفوض.

وثمة ثلاثة أنواع من التسهيلات المحددة في هذه المواصفة للتعامل مع الموارد التراتبية، وهي:

- تمثيل هوية عقدة.
- طلب نفاذ إلى عقدة.
- وضع سياسات تطبق على عقدة واحدة أو أكثر.

وتوفر كل من هذه التسهيلات أمر خياري.

وتعرض هذه الفقرة طريقتين لتمثيل مورد تراتبي. في الطريقة الأولى يتمثل التراتب الذي تشكل العقدة فيه جزءاً كوثيقة XML مدرجةٍ في الطلب، ويتمثل المورد المطلوب كعقدة في تلك الوثيقة. وفي الطريقة الثانية، لا يتمثل المورد المطلوب على شكل عقدة في وثيقة XML ولا يوجد في الطلب تمثيل للتراتب الذي يشكل ذلك المورد جزءاً منه. ويلاحظ أن المورد الفعلي المستهدف في الحالة الأولى لا يحتاج إلى أن يكون جزءاً من وثيقة XML – وهو ممثل بهذه الطريقة في الطلب فحسب. وبشكل مماثل قد يكون المورد المستهدف في الحالة الثانية بالفعل جزءاً من وثيقة XML – لكنه ممثل بطريقة أخرى في الطلب. ولذلك لا وجود لترابط مفترض بين بنية المورد وفق تمثيله في الطلب والبنية الفعلية للمورد المادي الذي يتم النفاذ إليه.

ويمكن للتسهيلات المتوفرة للتعامل مع الموارد الممثلة كعقد في الوثائق XML أن تفيد من أن الوثيقة XML ذاتها مدرجة في طلب القرار. ويمكن استعمال التعابير XPath في الإحالة إلى عقد في هذه الوثيقة بطريقة معيارية وفي توفير أشكال تمثيل فريدة لعقدة معينة في الوثيقة. ولا تتاح هذه التسهيلات للموارد التراتبية غير الممثلة في وثائق XML. ويجب توفير وسائل أخرى في حالة الوثائق غير XML من هذا القبيل من أجل تحديد موقع العقدة المطلوبة في التراتب. ويمكن إجراء ذلك في بعض الحالات من خلال إدراج وضعية العقدة في التراتب كجزء من هوية العقدة. وقد يكون أحياناً لعقدة ما أكثر من هوية معيارية كما هو الحال عندما يستطيع اسم مسير ملف ما في نظام ملفات معين إدراج وصلات مادية. وقد تحتاج إدارة سياق النقطة XACML PDP في مثل هذه الحالة إلى تقديم هويات جميع أسلاف العقدة. ولهذه الأسباب كافة تختلف تسهيلات التعامل مع العقد في الوثائق XML عن تسهيلات التعامل مع العقد في الموارد التراتبية الأخرى.

وقد يكون من المفيد لدى التعامل مع مورد تراتبي، طلب قرارات ترخيص لعدة عقد في المورد ضمن طلب قرار واحد. ويمكن اعتبار هذه الفقرة موضوعة في أعلى مواصفة الموارد المتعددة (انظر الفقرة 9)، الموضوعة بدورها في الطبقة العليا للسلوك المحدد في الفقرة 7. غير أن الوظائف الواردة في هذه الفقرة يمكن أن تستند مباشرة إلى الوظائف الواردة في الفقرة 7.

وتفترض هذه الفقرة الخاصة بالموارد التراتبية أن جميع طلبات النفاذ إلى عقد متعددة في مورد تراتبي تحولت إلى طلبات فردية للنفاذ إلى عقدة وحيدة.

1.12 تمثيل هوية العقدة

لكي تطبق السياسات XACML باتساق على العقد في مورد تراتبي ما لا بد للعقد في ذلك المورد من أن تتمثل بطريقة متسقة. فإذا كانت سياسة ما تحيل إلى عقدة تستعمل تمثيلاً واحداً، وكان الطلب يحيل إلى العقدة باستعمال تمثيل مختلف، تعذر تطبيق السياسة وتعرض الأمن إلى الخطر.

وتصف الفقرات التالية أشكال تمثيل يوصى بها للعقد في الموارد التراتبية. ويسمح بأشكال أخرى للعقد في مورد معين، طالما تم التعاقد على أن تستعمل جميع نقاط إدارة السياسة وجميع نقاط تعزيز السياسة التي تتعامل مع ذلك المورد أشكال تمثيل بديلة.

1.1.12 العقد في الوثائق XML

هذه الفقرة معيارية ولكنها خيارية.

يستعمل المعرف URI التالي معرفاً للوظائف المحددة في هذا الجزء من المواصفة:

```
urn:oasis:names:tc:xacml:2.0:profile:hierarchical:xml-node-id
```

وتكون عقدة في مورد ما يتمثل في حالة وثيقة XML تعبيراً XPath التي تقدر تماماً بتلك العقدة في نسخة المورد التي يتضمنها العنصر <ResourceContent> للعنصر <Resource> في الطلب <Request>.

2.1.12 العقد في الموارد التي ليست وثائق XML

هذه الفقرة معيارية ولكنها خيارية.

يستعمل المعرف URI التالي كمعرف للوظائف المحددة في هذا الجزء من المواصفة:

```
urn:oasis:names:tc:xacml:2.0:profile:hierarchical:non-xml-node-id
```

ينبغي تمثيل هوية عقدة في مورد تراتبي لا يتخذ شكل حالة وثيقة XML كمعرف URI مطابق للمعيار IETF RFC 2396. وتتخذ هذه المعرفات URI الشكل التالي:

```
<scheme> ":" <authority> "/" <pathname>
```

وتستعمل موارد نظام الملفات النظام ":file". وإذا لم يتحدد <scheme> معياري لنمط المورد في المعيار IETF RFC 2396 في معيار ذي صلة لنظام URI مسجل، فإن المعرف URI يستعمل النظام ":file".

ويتخذ الجزء <pathname> من المعرف URI الشكل التالي:

```
<root name> [ "/" <node name> ]*
```

ويجب أن تقابل تتابع القيمتين <root name> و<node name> اسمي المكونات التراتبية لأسلاف العقدة الممثلة على طول المسير من عقدة <root> حتى العقدة الممثلة.

وينبغي استعمال التقنين التالي:

- يشفر المعرف URI بالشفرة UTF8.
- تظهر الأجزاء المقاومة للكسر في المعرف URI في حروف صغيرة.
- يطبق تشفير السمات المئوي المعيار IETF RFC 2396.

- يتحدد الجزء <authority> من المعرف URI ويكون تمثيل السلطة المعيارية لنمط المورد المعني. وإذا ما أمكن تحديد العنصر <authority> باستعمال نظام اسم المجال (DNS) أو عنوان رقمي IPv4 أو IPv6، اختير استعمال الاسم DNS.
- تتحدد مكون الجزء <pathname> من المعرف URI باستخدام الشكل النظامي لمكونات مسير العنصر <authority>.
- وفقاً للمعيار IETF RFC 2396، تكون السمة الفاصلة بين المكونات التراتبية للجزء <pathname> للمعرف URI هي السمة "/". وتتحول تتابعات السمة "/" إلى سمة واحدة "/". ولا تنتهي هويات العقدة بالسمة "/".
- لا يضم العنصر <pathname> وصلات رمزية (soft).
- جميع القيم <pathname> مطلقة.
- وإذا وجد أكثر من مسير واحد مطلق وكامل التحول صادر عن <root> في العنصر <authority> إلى العقدة الممثلة يكون عندئذٍ نعت مورد منفصل مع AttributeId "urn:oasis:names:tc:xacml:1.0:resource:resource-id" وDataType http://urn:oasis:names:tc:xacml:1.0:data-type:anyURI موجوداً في سياق طلب كل مسير من هذا القبيل.

2.12 طلب نفاذ إلى عقدة

لكي يمكن تطبيق السياسات XACML باتساق على العقد في مورد تراتبي ما لا بد لكل سياق طلب يمثل طلب نفاذ إلى عقدة ما في ذلك المورد من أن يستخدم وصفاً متسقاً للنفاذ إلى تلك العقدة. وإذا أحالت سياسة ما إلى بعض النعوت المتوقعة لعقدة ما دون أن يحتوي سياق الطلب على هذه النعوت أو دون التعبير عن هذه النعوت بالطريقة المتوقعة فقد يتعذر عندئذ تطبيق السياسة ويتعرض الأمن بالتالي للخطر.

وتصف الفقرات التالية أوصاف سياق الطلب الموصى بها للنفاذ إلى العقد في الموارد التراتبية. وأشكال التمثيل الأخرى لمثل هذه الطلبات مسموحة طالما تعاقدت جميع نقاط إدارة السياسة وجميع نقاط تعزيز السياسة التي تتعامل مع ذلك المورد على استعمال أشكال تمثيل بديلة.

1.2.12 عقد في الوثيقة XML

هذه الفقرة معيارية ولكنها خيارية.

يستعمل المعرف التالي كمعرف للوظائف المحددة في هذا الجزء من المواصفة:

```
urn:oasis:names:tc:xacml:2.0:profile:hierarchical:xml-node-req
```

وتكون النعوت مع المعرفات AttributeIds كما يلي:

```
"urn:oasis::names:tc:xacml:2.0:resource:resource-parent"
"urn:oasis::names:tc:xacml:2.0:resource:resource-ancestor"
```

و:

```
"urn:oasis::names:tc:xacml:2.0:resource:resource-ancestor-or-self"
```

خيارية. وإذا توفرت للاستعمال في موارد تتخذ شكل وثائق XML فإن المعرفات URI التالية تستخدم كمعرفات للوظائف التي تمثلها:

```
"urn:oasis:names:tc:xacml:2.0:profile:hierarchical:xml-node-req:resource-parent"
"urn:oasis:names:tc:xacml:2.0:profile:hierarchical:xml-node-req:resource-ancestor"
```

و:

```
"urn:oasis:names:tc:xacml:2.0:profile:hierarchical:xml-node-req:resource-ancestor-
or-self"
```

ومن أجل طلب نفاذ إلى مورد يمثله كعقدة في وثيقة XML يجب أن يحتوي العنصر <Resource> لسياق الطلب على العناصر والنعوت XML التالية:

- عنصر <ResourceContent> يضم كامل حالة الوثيقة XML التي تشكل العقدة المطلوبة جزءاً منها.
- عنصر <Attribute> مع AttributeId للاسم "urn:oasis::names:tc:xacml:1.0:resource:resource-id" والنمط DataType للتعبير "urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression". ويكون العنصر <AttributeValue> لهذا العنصر <Attribute> تعبيراً XPath تكون عقدة سياقه فرعاً وحيداً للعنصر <ResourceContent>. ويجب أن يساوي هذا التعبير XPath مجموعة عقد تضم العقدة الوحيدة في العنصر <ResourceContent> الذي يشكل العقدة التي يطلب النفاذ إليها. ويجوز لهذا العنصر <Attribute> أن يحدد الجهة المنتجة.
- عنصر <Attribute> مع AttributeId للاسم "urn:oasis::names:tc:xacml:2.0:resource:resource-parent" وDataType للاسم "urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression". ويكون <AttributeValue> لهذا العنصر <Attribute> تعبيراً XPath؛ وتكون عقدة سياق هذا التعبير XPath العقدة الفرع الوحيد للعنصر

<ResourceContent>. ويجب أن يساوي التعبير XPath مجموعة عقد تضم العقدة الوحيدة في العنصر <ResourceContent> الذي يشكل الأصل المباشر للعقدة الممثلة في النعت "resource-id". ويجوز لهذا العنصر <Attribute> أن يحدد الجهة المنتجة.

- عنصر <Attribute> مع AttributeId للاسم "urn:oasis:names:tc:xacml:2.0:resource:resource-ancestor" وDataType للاسم "urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression". لكل عقدة في حالة الوثيقة XML التي تشكل سلفاً للنقطة الممثلة في النعت "resource-id". ويجب أن تكون القيمة <AttributeValue> لهذا النعت <Attribute> تعبيراً XPath؛ وتكون عقدة سياق هذا التعبير XPath العقدة الفرع الوحيد للعنصر <ResourceContent>. ويساوي هذا التعبير XPath مجموعة عقد تضم العقدة الوحيدة في العنصر <ResourceContent> الذي يشكل السلف المقابل للعقدة الممثلة في النعت "resource-id". ويكون لكل نعت "resource-parent" نعتاً مقابلاً "resource-ancestor". ويجوز لهذا النعت <Attribute> أن يحدد الجهة المنتجة.

- عنصر <Attribute> مع AttributeId للاسم "urn:oasis::names:tc:xacml:2.0:resource:resource-ancestor-or-self" وDataType للاسم "urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression"، لكل عقدة في حالة الوثيقة XML تشكل سلفاً للعقدة الممثلة في النعت "resource-id" للعقدة "resource-id" ذاتها. وتكون القيمة <AttributeValue> لهذا النعت <Attribute> تعبيراً XPath؛ وتكون عقدة السياق لهذا التعبير XPath العقدة الفرع الوحيد للعنصر <ResourceContent>. ويساوي هذا التعبير مجموعة عقد تضم العقدة الوحيدة في العنصر <ResourceContent> الذي يشكل السلف المقابل للعقدة المتمثلة في النعت "resource-id" أو يشكل العقدة "resource-id" ذاتها. ويكون لكل نعت "resource-parent" و"resource-id" نعت "resource-ancestor-or-self" مقابل. ويجوز لهذا النعت <Attribute> أن يحدد الجهة المنتجة.

ويمكن إدراج نعوت إضافية في العنصر <Resource> وعلى وجه الخصوص النعت التالي:

- عنصر <Attribute> مع المعرف AttributeId للاسم "urn:oasis:names:tc:xacml:2.0:resource:document-id" ونمط DataType للاسم "urn:oasis:names:tc:xacml:1.0:data-type:anyURI". وتكون القيمة <AttributeValue> لهذا النعت <Attribute> معرفاً URI يحدد هوية الوثيقة XML التي يشكل المورد المطلوب جزءاً منها والتي تضم العنصر <ResourceContent> نسخةً منها. ويجوز لهذا النعت <Attribute> أن يحدد الجهة المنتجة.

2.2.12 عقد في مورد ليس وثيقة XML

هذه الفقرة معيارية لكنها خيارية.

يستعمل المعرف URI التالي كمعرف للوظائف المحددة في هذا الجزء من الفقرة:

```
urn:oasis:names:tc:xacml:2.0:profile:hierarchical:non-xml-node-req
```

والنعوت مع المعرفات AttributeIds للوسمين:

```
"urn:oasis::names:tc:xacml:2.0:resource:resource-parent"
"urn:oasis::names:tc:xacml:2.0:resource:resource-ancestor"
```

و:

```
"urn:oasis::names:tc:xacml:2.0:resource:resource-ancestor-or-self"
```

خيارية في التنفيذ. وإذا توفرت للاستخدام في موارد ليست متمثلة في وثائق XML، يتعين استخدام المعرفات URI التالية كمعرفات للوظائف التي تمثلها:

```
"urn:oasis:names:tc:xacml:2.0:profile:hierarchical:non-xml-node-req:resource-
parent"
"urn:oasis:names:tc:xacml:2.0:profile:hierarchical:non-xml-node-req:resource-
ancestor"
```

و:

```
"urn:oasis:names:tc:xacml:2.0:profile:hierarchical:non-xml-node-req:resource-
ancestor-or-self"
```

ومن أجل طلب النفاذ إلى عقدة في مورد تراتبي ليس ممثلاً في وثيقة XML يتعين على عنصر <Resource> لسياق الطلب ألا يحتوي على عنصر <ResourceContent>، بل على العناصر والنعوت XML التالية. ويلاحظ أن عقدة المورد التراتبي التي لا تتمثل في شكل وثيقة XML قد تتخذ عدة أصول. مثال: في نظام ملفات يوفر وصلات مادية قد توجد عدة مسارات معيارية لملف واحد. وقد يضم كل من هذه المسارات مجموعات مختلفة من الأصول والأسلاف.

- عنصر <Attribute> مع AttributeId للاسم "urn:oasis::names:tc:xacml:1.0:resource:resource-id" لكل تمثيل معياري للعقدة المطلوبة. وتكون القيمة <AttributeValue> لهذا النعت هوية فريدة معيارية للعقدة التي يُطلب النفاذ إليها. ويتوقف نمط معطيات هذا النعت على التمثيل المختار لهوية العقد في المورد المعني. ويجوز للعنصر <Attribute> أن يحدد الجهة المنتجة.
- عنصر <Attribute> مع AttributeId للاسم "urn:oasis::names:tc:xacml:2.0:resource:resource-parent" لكل أصل مباشر من العقدة المحددة في النعت أو النعوت "resource-id" ولكل تمثيل معياري لتلك العقدة الأصل. وتكون القيمة <AttributeValue> لهذا النعت الهوية المعيارية للعقدة الأصل. ويرتبط نمط معطيات هذا النعت بالتمثيل المختار لهوية العقد في هذا المورد بعينة. ويجوز للعنصر <Attribute> أن يحدد جهة منتجة. وإذا شكلت العقدة المطلوبة جزءاً من مجموعة تفرعات وليس من تفرع واحد أو إذا كانت العقدة الأصل أكثر من تمثيل معياري واحد يتعين وجود استطباق واحد على الأقل لهذا النعت لكل أصل على طول كل مسار إلى الجذور المتعددة التي تنحدر منها العقدة المطلوبة ولكل تمثيل معياري لكل أصل من هذا القبيل.
- عنصر <Attribute> مع AttributeId للاسم "urn:oasis::names:tc:xacml:2.0:resource:resource-ancestor" لكل سلف عقدة محددة في النعت أو النعوت "resource-id" ولكل تمثيل معياري لتلك العقدة السلف. وتكون القيمة <AttributeValue> لهذا النعت الهوية المعيارية للعقدة السلف. ويرتبط نمط معطيات هذا العنصر بالتمثيل المختار لهوية العقد في ذلك المورد المعين. ويجوز لهذا النعت أن يحدد جهة منتجة. ويتعين أن يكون لكل "resource-parent" مقابل. وإذا شكلت العقدة المطلوبة جزءاً من مجموعة تفرعات بدلاً من تفرع واحد أو إذا كانت للعقدة السلف أكثر من تمثيل معياري واحد يتعين وجود استطباق واحد على الأقل لهذا النعت لكل سلف على طول المسار إلى الجذور المتعددة التي تنحدر منها العقدة المطلوبة، ولكل تمثيل معياري لكل سلف من هذا القبيل. ولا يعكس ترتيب قيم هذا النعت بالضرورة موقع كل عقدة سلف في هذا التراتب.
- عنصر <Attribute> مع AttributeId للاسم "urn:oasis::names:tc:xacml:2.0:resource:resource-ancestor-or-self". لكل سلف عقدة محددة في نعت "resource-id" واحد أو أكثر ولكل تمثيل معياري لتلك العقدة السلف ولكل تمثيل معياري للعقدة "resource-id" ذاتها. وتكون القيمة <AttributeValue> لهذا النعت الهوية المعيارية للعقدة السلف أو بالعقدة "resource-id". ويرتبط نمط معطيات هذا النعت <Attribute> بالتمثيل المختار لهوية العقد في ذلك المورد المعين. ويجوز لهذا النعت أن يحدد جهة منتجة. ويكون لكل نعت "resource-ancestor" و"resource-id" نعت "resource-ancestor-or-self" مقابل. وإذا شكلت العقدة المطلوبة جزءاً من مجموعة تفرعات وليس من تفرع واحد أو إذا كان للعقدة السلف أكثر من تمثيل معياري واحد يتعين وجود استطباق واحد على الأقل لهذا النعت لكل سلف على طول المسار المؤدي إلى الجذور المتعددة التي تنحدر منها العقدة المطلوبة، ولكل تمثيل معياري لكل سلف من هذا القبيل. ولا يعكس ترتيب قيم هذا النعت بالضرورة موقع كل عقدة سلف في هذا التراتب.

ويجوز إدراج نعوت إضافية في العنصر <Resource>.

3.12 وضع سياسات تطبق على العقد

ترد هذه الفقرة على سبيل الإعلام.

تصف هذه الفقرة طرقاً مختلفة لتحديد عبارات منطقية سياسية يمكن تطبيقها على عدة عقد في مورد تراتبي. وليست هذه القائمة شاملة.

1.3.12 سياسات تطبق على العقد في جميع الموارد التراتبية

ترد هذه الفقرة على سبيل الإعلام.

يمكن استخدام نعوت المورد مع القيم AttributeId التالية الواردة في الفقرة 5.12 من أجل وضع سياسات تطبق على عقدة واحدة أو أكثر من أي مورد تراتبي.

```
urn:oasis:names:tc:xacml:2.0:resource:resource-parent
urn:oasis:names:tc:xacml:2.0:resource:resource-ancestor
urn:oasis:names:tc:xacml:2.0:resource:resource-ancestor-or-self
```

ويلاحظ أن عنصر <ResourceAttributeDesignator> يحيل إلى النعوت "resource-parent" أو "resource-ancestor" أو "resource-ancestor-or-self" يعيد سلة قيم تمثل جميع الهويات المعيارية لجميع الأصول أو الأسلاف أو الأسلاف زائد المورد ذاته على التوالي للمورد الذي طلب النفاذ إليه. ولا تدل أشكال تمثيل هوية هذه الأصول أو الأسلاف أو المورد ذاته بالضرورة على المسار من جذر التراتب إلى الأصل أو السلف أو المورد ذاته على التوالي إلا إذا استعمل التمثيل الموصى به في الفقرة 2.2.12 عقد في مورد ليس وثيقة XML.

ويجوز استخدام وظائف السلة المعيارية XACML وسلة المرتبة الأعلى في وضع سياسات تطبق على عقدة واحدة أو أكثر في أي مورد تراتبي. وتتحدد العقد المستخدمة كمتغيرات في هذه الوظائف باستعمال العنصر <ResourceAttributeDesignator> مع قيمة معرف نعت "resource-parent" أو "resource-ancestor" أو "resource-ancestor-or-self".

2.3.12 سياسات تطبق عمل عقد الوثائق XML حصراً

ترد هذه الفقرة على سبيل الإعلام.

يمكن استخدام الوظائف التالية في وضع عبارات منسقة لسياسة تطبق على عقدة واحدة أو أكثر في الموارد التراتبية المتمثلة في حالات وثائق XML.

```
urn:oasis:names:tc:xacml:2.0:function:xpath-node-match
```

ويمكن استخدام العنصر <AttributeSelector> المعياري XACML في السياسات من أجل الإحالة إلى كامل المورد الممثل في وثيقة XML أو إلى أجزاء منه والذي يضم سياق الطلب في العنصر <ResourceContent>.

ويمكن استخدام وظائف السلة المعيارية XACML وسلة المرتبة الأعلى في وضع سياسات تطبق على عقدة واحدة أو أكثر في موردٍ ممثل في وثيقة XML. وتتحدد العقد المستخدمة كمتغيرات لهذه الوظائف باستعمال عنصر <AttributeSelector> ينتقي جزءاً من العنصر <ResourceContent> للعنصر <Resource>.

3.3.12 سياسات تطبق على عقد الموارد غير XML حصراً

ترد هذه الفقرة على سبيل الإعلام.

فيما يتعلق بالموارد التراتبية غير الممثلة في حالات وثائق XML وحيث يستعمل التمثيل المعرف URI للعقد كما تحددها هذه المواصفة، تستخدم الوظائف التالية من أجل وضع سياسات تطبق على عقدة واحدة أو أكثر في تلك الموارد.

```
urn:oasis:names:tc:xacml:1.0:function:anyURI-equal
urn:oasis:names:tc:xacml:1.0:function:regexp-uri-match
```

4.12 نمط معطيات جديدة: تعبير–xpath

ترد هذه الفقرة معيارية لكنها خيارية.

يمكن توفير القيمة التالية لقيمة النعت XML DataType لاستعمالها مع موارد تراتبية ممثلة على شكل وثائق XML. وتوفير هذا النعت DataType إلزامي من أجل دعم أحكام الفقرة 1.1.12.

والنعت DataType الذي يمثله المعرف URI التالي تعبير XPath. وتكون قيم النعت المزودة بالنعت DataType سلاسلٍ ينبغي تفسيرها بتعابير XPath. وينتج عن تقدير مثل هذا النعت مجموعة العقد الناجمة عن تقييم التعبير XPath. وإذا لم تكن السلسلة تعبيراً XPath صالحاً تكون نتيجة تقييم النعت "غير محدد".

```
urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression
```

5.12 معرفات جديدة للنعوت

ترد هذه الفقرة معيارية لكنها خيارية.

1.5.12 المعرف document-id

يدل المعرف التالي على هوية الوثيقة XML التي تمثل التراتب الذي يشكل المورد المطلوب جزءاً منه والذي يضم العنصر <ResourceContent> نسخة منه. وفي كل مرة يطلب فيها النفاذ إلى عقدة في مورد يتمثل في وثيقة XML، يمكن توفير حالة أو أكثر لنعت هذا المعرف AttributeId في العنصر <Resource> في سياق الطلب. ويكون نمط معطيات هذه النعوت كالتالي: "urn:oasis:names:tc:xacml:1.0:data-type:anyURI".

```
urn:oasis:names:tc:xacml:2.0:resource:document-id
```

2.5.12 المعرف resource-parent

يدل المعرف التالي على هوية معيارية واحدة لعقدة أصل واحدة في تفرع أو مجموعة تفرعات تشكل العقدة المطلوبة جزءاً منها. وفي كل مرة يطلب فيها النفاذ إلى عقدة في مورد تراتبي يتعين توفيرٍ حالة نعت مجمل هذا المعرف AttributeId في العنصر <Resource> في سياق الطلب وذلك لكل تمثيل معياري لكل عقدة تشكل سلفاً للعقدة المطلوبة.

```
urn:oasis:names:tc:xacml:2.0:resource:resource-parent
```

3.5.12 المعرف resource-ancestor

يدل المعرف التالي على هوية معيارية واحدة لعقدة سلف واحدة في تفرع أو مجموعة تفرعات تشكل العقدة المطلوبة جزءاً منها. وفي كل مرة يطلب فيها النفاذ إلى عقدة في مورد تراتبي، يتعين توفير حالة لنعت يحمل هذا المعرف AttributeId في العنصر <Resource> في سياق الطلب وذلك لكل تمثيل معياري لكل عقدة تشكل سلفاً للعقدة المطلوبة.

```
urn:oasis:names:tc:xacml:2.0:resource:resource-ancestor
```

4.5.12 المعرف resource-ancestor-or-self

يدل المعرف التالي على هوية معيارية واحدة لعقدة سلف واحدة في تفرع أو مجموعة تفرعات تشكل العقدة المطلوبة جزءاً منها أو هوية معيارية واحدة للعقدة المطلوبة ذاتها. وفي كل مرة يطلب فيها النفاذ إلى عقدة في مورد تراتبي يتعين توفير حالة لنعت يحمل هذا المعرف AttributeId في عنصر <Resource> من سياق الطلب وذلك لكل تمثيل معياري لكل عقدة تشكل سلفاً للعقدة المطلوبة ولكل تمثيل معياري للعقدة المطلوبة ذاتها.

```
urn:oasis:names:tc:xacml:2.0:resource:resource-ancestor-or-self
```

6.12 معرفات مواصفة جديدة

تستعمل قيم المعرفات URI التالية كمعرفات للوظائف المحددة في فقرات مختلفة من هذه المواصفة:

الفقرة 1.1.12: عقد في وثائق XML

```
urn:oasis:names:tc:xacml:2.0:profile:hierarchical:xml-node-id
```

الفقرة 2.1.12: عقد في موارد ليست وثائق XML

```
urn:oasis:names:tc:xacml:2.0:profile:hierarchical:non-xml-node-id
```

الفقرة 1.2.12: عقد في وثيقة XML

```
urn:oasis:names:tc:xacml:2.0:profile:hierarchical:xml-node-req
```

وتوفير أغراض النعوت "resource-parent" و"resource-ancestor" و"resource-ancestor-or-self" أمر خياري في هذه الفقرة وبالتالي فلها معرفات هي:

```
urn:oasis:names:tc:xacml:2.0:profile:hierarchical:xml-node-req:resource-parent
urn:oasis:names:tc:xacml:2.0:profile:hierarchical:xml-node-req:resource-ancestor
urn:oasis:names:tc:xacml:2.0:profile:hierarchical:xml-node-req:resource-ancestor-
or-self
```

الفقرة 2.2.12: عقد في مورد ليس وثيقة XML

```
urn:oasis:names:tc:xacml:2.0:profile:hierarchical:non-xml-node-req
```

وتوفير أغراض النعوت "resource-parent" و"resource-ancestor" و"resource-ancestor-or-self" أمر خياري في هذه الفقرة وبالتالي فلها معرفات هي:

```
urn:oasis:names:tc:xacml:2.0:profile:hierarchical:non-xml-node-req:resource-parent
urn:oasis:names:tc:xacml:2.0:profile:hierarchical:non-xml-node-req:resource-
ancestor
urn:oasis:names:tc:xacml:2.0:profile:hierarchical:non-xml-node-req:resource-
ancestor-or-self
```

13 مواصفة سياسة السرية

التزامان يقعان على عاتق حارس المعطيات هما: ضمان أن استعمال المعطيات الشخصية يقتصر على تلبية الأغراض التي تجمع من أجلها أو أغراض أخرى لا تتعارض معها، ومنع إفشاء المعطيات الشخصية إلاّ بموافقة الجهة المعنية أو بسلطة القانون. وتقدم هذه الفقرة مواصفة لنعوت معيارية وعنصر <Rule> معياري بهدف تعزيز هذين الالتزامين المتعلقين بالفرض الذي تجمع من أجله معلومات شخصية محددة وتستخدم.

1.13 النعوت المعيارية

تحدد هذه المواصفة نعتين اثنين.

```
urn:oasis:names:tc:xacml:2.0:resource:purpose
```

يدل هذا النعت وهو من النمط "http://www.w3.org/2001/XMLSchema#string" على الغرض من جمع موارد المعطيات. وينبغي إعلام صاحب الموارد والحصول على موافقته على استعمال الموارد لهذا الغرض. وقد تكون قيمة النعت تعبير نظامي. وينبغي أن تحدد سياسة سرية الحراسة دلالات جميع القيم المتاحة.

```
urn:oasis:names:tc:xacml:2.0:action:purpose
```

ويدل هذا النعت وهو من النمط "http://www.w3.org/2001/XMLSchema#string" على الغرض من طلب النفاذ إلى المورد. وقد تنظم الأغراض تراتبياً؛ وفي هذه الحالة يجب أن تمثل القيمة عقدة في التراتب.

2.13 قواعد معيارية: توافق الأغراض

يجب استعمال هذه القاعدة مع خوارزمية جمع القواعد "urn:oasis:names:tc:xacml:2.0:rule-combining-algorithm:deny-overrides" التي تقضي بوجوب رفض النفاذ إلاّ إذا كان الغرض من طلب النفاذ يتطابق مع الغرض من جمع موارد المعطيات.

```
<?xml version="1.0" encoding="UTF-8"?>
<Rule xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os" RuleId="
urn:oasis:names:tc:xacml:2.0:matching-purpose"
Effect="Permit">
      <Condition FunctionId="urn:oasis:names:tc:xacml:2.0:function:regexp-
string-match">
            <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:2.0:resource:purpose"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
            <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:2.0:action:purpose"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </Condition>
</Rule>
```

الملحق A

أنماط المعطيات والدالات

1.A مقدمة

يحدد هذا الملحق أنماط المعطيات والدالات المستعملة في لغة XACML لتكوين العبارات المنطقية اللازمة لمطابقات الحالات والأهداف.

وتصف هذه التوصية الأنماط الأولية للمعطيات والمجموعات غير المرتبة. وتُسمى هاهنا الدالات المعيارية وتُوصف دلالات معانيها التشغيلية.

ملاحظة – انظر الوثيقتين [IEEE 754] و[RBAC] للاطلاع على تمثيل سلاسل معلومات القيم الرقمية.

2.A أنماط المعطيات

بالرغم من أن حالات لغة XML تمثل جميع أنماط المعطيات كسلاسل، يجب أن يقدم بروتوكول XACML PDP تبريرات بشأن أنماط المعطيات التي مع أنها ممثلة كسلاسل، فإنها ليست مجرد سلاسل. ويجب تحويل الأنماط، مثل السلسلة والنمط البولاني والنمط الصحيح والنمط المضاعف، من حالات تمثيلها كسلاسل XML إلى قيم يمكن مقارنتها مع قيم تندرج ضمن نطاق ميدان محادثتها، كالأرقام. وفيما يلي الأنماط الأولية من المُعطيات المُحددة من أجل استعمالها مع لغة XACML ولديها حالات تمثيل واضحة للمعطيات:

- http://www.w3.org/2001/XMLSchema#string
- http://www.w3.org/2001/XMLSchema#boolean
- http://www.w3.org/2001/XMLSchema#integer
- http://www.w3.org/2001/XMLSchema#double
- http://www.w3.org/2001/XMLSchema#time
- http://www.w3.org/2001/XMLSchema#date
- http://www.w3.org/2001/XMLSchema#dateTime
- http://www.w3.org/2001/XMLSchema#anyURI
- http://www.w3.org/2001/XMLSchema#hexBinary
- http://www.w3.org/2001/XMLSchema#base64Binary
- urn:oasis:names:tc:xacml:2.0:data-type:dayTimeDuration
- urn:oasis:names:tc:xacml:2.0:data-type:yearMonthDuration
- urn:oasis:names:tc:xacml:1.0:data-type:x500Name
- urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name
- urn:oasis:names:tc:xacml:2.0:data-type:ipAddress
- urn:oasis:names:tc:xacml:2.0:data-type:dnsName

ولغرض تحسين قابلية التشغيل البيني، يُوصى بأن تكون جميع الإشارات الزمنية بالتوقيت العالمي المنسق (UTC).

ويتعين أن يكون بروتوكول XACML PDP قادراً على تحويل حالات تمثيل السلاسل إلى عدة أنماط معطيات أولية.

ملاحظة – يتعين أن تستعمل لغة XACML حالات التحويل التي تصفها الوثيقة [IEEE 754] فيما يخص الأنماط الصحيحة والمضاعفة.

وتعرف XACML ستة أنماط من المعطيات، هي كالتالي:

```
"urn:oasis:names:tc:xacml:2.0:data-type:dayTimeDuration"
"urn:oasis:names:tc:xacml:2.0:data-type:yearMonthDuration"
"urn:oasis:names:tc:xacml:1.0:data-type:x500Name"
"urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name"
"urn:oasis:names:tc:xacml:2.0:data-type:ipAddress"
"urn:oasis:names:tc:xacml:2.0:data-type:dnsName"
```

وتمثل هذه الأنماط معرفات مواضيع أو موارد، وتظهر في عدة تطبيقات معيارية، كتطبيق SSL/TLS والبريد الإلكتروني.

1.2.A المدة بالأيام والساعات

يُعرف النمط الأولي "urn:oasis:names:tc:xacml:2.0:data-type:dayTimeDuration" على أنه أحد قيود النمط **xs:duration**، ولا يحتفظ سوى بمكونات كل من الإشارة والسنة والشهر.

```
<xs:simpleType name='urn:oasis:names:tc:xacml:2.0:data-
type:yearMonthDuration'>
    <xs:restriction base='xs:duration'>
        <xsd:pattern value="[-]?P\p{Nd}+(Y(\p{Nd}+M)?|M)"/>
    </xs:restriction>
</xs:simpleType>
```

وقيمة yearMonthDuration هي بوحدات الشهور، وهي كالآتي:

```
('value of the year component' * 12) + ('value of the month component')
```

وإذا كان مكون الإشارة "-"، يُحصل على قيمة سالبة، وبخلافه، يُحصل على قيمة موجبة.

2.2.A المدة بالسنوات والأشهر

يُعرف النمط الأولي "urn:oasis:names:tc:xacml:2.0:data-type:yearMonthDuration" على أنه أحد قيود النمط **xs:duration**، ولا يحتفظ سوى بمكونات كل من الإشارة واليوم والساعة والدقيقة والثانية.

```
<xs:simpleType name='urn:oasis:names:tc:xacml:2.0:data-
type:dayTimeDuration'>
    <xs:restriction base='xs:duration'>
         <xsd:pattern value="[-
]?P(\p{Nd}D(T(\p{Nd}+(H(\p{Nd}+(M(\p{Nd}+(\.\p{Nd}*)?S
            |\.\p{Nd}+S)?|(\.\p{Nd}*)?S)|(\.\p{Nd}*)?S)?|M(\p{Nd}+
            (\.\p{Nd}*)?S|\.\p{Nd}+S)?|(\.\p{Nd}*)?S)|\.\p{Nd}+S))?
            |T(\p{Nd}+(H(\p{Nd}+(M(\p{Nd}+(\.\p{Nd}*)?S|\.\p{Nd}+S)?

|(\.\p{Nd}*)?S)|(\.\p{Nd}*)?S)?|M(\p{Nd}+(\.\p{Nd}*)?S|\.\p{Nd}+S)?
            |(\.\p{Nd}*)?S)|\.\p{Nd}+S))"/>
    </xs:restriction>
</xs:simpleType>
```

وقيمة dayTimeDuration هي بوحدات الثواني، وهي كالآتي:

```
('value of the day component' * 24) +
('value of the hour component' * 60) +
('value of the minute component' * 60) +
('value of the second component')
```

وإذا كان مكون الإشارة "-"، يُحصل على قيمة سالبة، وبخلافه، يُحصل على قيمة موجبة.

3.2.A اسم الدليل X.500

يمثل النمط الأولي "urn:oasis:names:tc:xacml:1.0:data-type:x500Name" اسم X.520 مميز، وتصف الوثيقة IETF RFC 2253 قواعد التركيب الصحيحة لهذا الاسم.

4.2.A اسم IETF RFC 822

يمثل النمط الأولي "urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name" عنوان بريد إلكتروني، وتصف الفقرة 2.1.4 من الوثيقة IETF RFC 2821 قواعد التركيب الصحيحة لهذا الاسم.

5.2.A عنوان بروتوكول الإنترنت (IP)

يمثل النمط الأولي "urn:oasis:names:tc:xacml:2.0:data-type:ipAddress" عنوان شبكة IPv4 أو IPv6، بقناع ومنفذ اختيارين أو مدى منفذ اختياري. وفيما يلي قواعد تركيب العنوان:

```
ipAddress = address [ "/" mask ] [ ":" [ portrange ] ]
```

وفيما يخص عنوان IPv4، يتم إنساق العنوان والقناع وفقاً لقواعد التركيب الخاصة "بمضيف" يرد في الفقرة 2.3 من الوثيقة IETF RFC 2396.

أما بالنسبة لعنوان IPv6، فيتم إنساق العنوان والقناع وفقاً لقواعد التركيب الخاصة بمرجع "ipv6reference" الوارد في الوثيقة IETF RFC 2396. (يُلاحظ أن عنوان IPv6 أو القناع المبين في قواعد التركيب هذه، محصور بين أقواس "[" "]" حرفية.)

6.2.A اسم DNS

يمثل النمط الأولي "urn:oasis:names:tc:xacml:2.0:data-type:dnsName" اسم مضيف نظام اسم ميدان (DNS)، بمنفذ اختياري أو مدى منفذ اختياري. وفيما يلي قواعد تركيب الاسم:

```
dnsName = hostname [ ":" portrange ]
```

ويتم إنساق الاسم hostname وفقاً للفقرة 2.3 من الوثيقة IETF RFC 2396، باستثناء توفر إمكانية استعمال بطاقة رموز تنوعية "*" في أقصى يسار مكون الاسم hostname لبيان "جميع الميادين الفرعية" الموجودة تحت الميدان المُحدد إلى يمين المكون.

وفيما يتعلق بكل من نمطي المعطيات "urn:oasis:names:tc:xacml:2.0:data-type:ipAddress" و"urn:oasis:names:tc:xacml:2.0:data-type:dnsName"، فإن قواعد تركيب المنفذ أو مدى المنفذ فيهما هي كالآتي:

```
portrange = portnumber | "-"portnumber | portnumber"-"[portnumber]
```

حيث رقم المنفذ "portnumber" هو رقم منفذ عشري. وإذا كان رقم المنفذ في شكل "x-"، حيث "x" أحد أرقام المنفذ، يشمل المدى عندئذ جميع المنافذ المرقمة "x" وما دونها. أما إذا كان رقم المنفذ في شكل "-x"، يشمل المدى حينئذ جميع المنافذ المرقمة "x" وما فوقها.

3.A الدالات

تحدد XACML الدالات الواردة أدناه. وفي حال تقييم متغير من إحدى هذه الدالات على أنه "Indeterminate"، يتعين عندئذ ضبط الدالة على "Indeterminate".

1.3.A العبارات المنطقية للمساواة

الدالات الواردة أدناه هي دالات مساواة لمختلف الأنماط الأولية. وتتبع كل دالة لنمط معطيات معين اصطلاحاً معيارياً محدداً لنمط المعطيات المذكور.

```
urn:oasis:names:tc:xacml:1.0:function:string-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#string" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا تساوى طول قيمة متغيريها على حد سواء، وحُددت كل سلسلة على أنها متساوية بايتة ببايتة وفقاً لدالة "integer-equal". وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False".

```
urn:oasis:names:tc:xacml:1.0:function:boolean-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#boolean" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا تساوى المتغيران. وبخلافه، يتعين أن تعيد قيمة "False".

```
urn:oasis:names:tc:xacml:1.0:function:integer-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#integer" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean".

الملاحظة 1 – انظر المرجع [IEEE 754] للحصول على معلومات عن تقييم الأنماط الصحيحة على الأعداد الصحيحة.

```
urn:oasis:names:tc:xacml:1.0:function:double-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#double" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean".

الملاحظة 2 – انظر المرجع [IEEE 754] للاطلاع على كيفية تقييم الأنماط المضاعفة.

```
urn:oasis:names:tc:xacml:1.0:function:date-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#date" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا تساوت قيمتا المتغيرين. وفي حال افتقار أحد المتغيرين إلى نطاق زمني واضح، ينبغي أن يوفر التنفيذ قيمة نطاق زمني معينة.

```
urn:oasis:names:tc:xacml:1.0:function:time-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#time" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا تساوت قيمتا المتغيرين. وفي حال افتقار أحد المتغيرين إلى نطاق زمني واضح، ينبغي أن يوفر التنفيذ قيمة نطاق زمني معينة.

```
urn:oasis:names:tc:xacml:1.0:function:dateTime-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#dateTime" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا تساوت قيمتا المتغيرين. وفي حال افتقار أحد المتغيرين إلى نطاق زمني واضح، ينبغي أن يوفر التنفيذ قيمة نطاق زمني معينة.

```
urn:oasis:names:tc:xacml:1.0:function:dayTimeDuration-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "urn:oasis:names:tc:xacml:2.0:data-types:dayTimeDuration" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا تساوت قيمتا المتغيرين. ويُلاحظ أنه يجب تحويل تمثيل مفردات كل متغير إلى قيمة يُعبر عنها بأجزاء الثانية.

```
urn:oasis:names:tc:xacml:1.0:function:yearMonthDuration-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "urn:oasis:names:tc:xacml:2.0:data-types:yearMonthDuration" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا تساوت قيمتا المتغيرين. ويُلاحظ أنه يجب تحويل تمثيل مفردات كل متغير إلى قيمة يُعبر عنها بأشهر صحيحة.

```
urn:oasis:names:tc:xacml:1.0:function:anyURI-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#anyURI" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا تساوت قيمتا المتغيرين على أساس كل تتابع تشفير على حدة.

```
urn:oasis:names:tc:xacml:1.0:function:x500Name-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات"urn:oasis:names:tc:xacml:1.0:data-type:x500Name" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا تطابق كل اسم من الأسماء المميزة النسبية (RDN) في المتغيرين. وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False". وينبغي القول إن اسمي RDN متطابقان، إذا، وفقط إذا كانت نتيجة العمليات الواردة أدناه "True".

1) تقييس المتغيرين وفقاً لأحكام الوثيقة IETF RFC 2253.
2) إذا احتوى اسم RDN على عدة أزواج من attributeTypeAndValue، يُعاد ترتيب AttributeValuePairs في اسم RDN هذا ترتيباً تنازلياً عند مقارنتها كسلاسل أثمونات (تصفها الفقرة 6.11 في التوصية X.690).
3) مقارنة أسماء RDN باستعمال القواعد الواردة في الفقرة 4.2.1.4 من الوثيقة IETF RFC 3280.

```
urn:oasis:names:tc:xacml:1.0:function:rfc822Name-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا تساوت قيمتا المتغيرين. وبخلاف ذلك، يتعين أن تعيد قيمة "False". ويتكون اسم IETF REC 822 من جزء محلي تتبعه علامة "@" يليها جزء ميدان. والجزء المحلي حساس من حيث وضعية الحرف، بينما جزء الميدان ليس كذلك (عادة ما يكون اسم مضيف DNS). وتُطبق العمليات التالية:

1) يتم تقييس جزء ميدان كل متغير إلى حرف صغير.
2) تُقارن التعابير بتطبيق الدالة "urn:oasis:names:tc:xacml:1.0:function:string-equal" على المتغيرات المقيسة.

```
urn:oasis:names:tc:xacml:1.0:function:hexBinary-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#hexBinary" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا كانت تتابعات الأثمونات المُمثلة بقيمة كلا المتغيرين متساوية الطول ومتساوية في مقارنة رابطة نقطة بنقطة باستعمال دالة "urn:oasis:names:tc:xacml:1.0:function:integer-equal". وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False". وينبغي أن يكون تحويل تمثيل السلاسل إلى تتابع أثمونات على غرار ما هو مُحدد في الفقرة 15.2.3 من W3C Datatypes:2001.

```
urn:oasis:names:tc:xacml:1.0:function:base64Binary-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#base64Binary" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا كانت تتابعات الأثمونات المُمثلة بقيمة كلا المتغيرين متساوية الطول ومتساوية في مقارنة رابطة نقطة بنقطة باستعمال دالة "urn:oasis:names:tc:xacml:1.0:function:integer-equal". وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False". وينبغي أن يكون تحويل تمثيل السلاسل إلى تتابع أثمونات على غرار ما هو مُحدد في الفقرة 16.2.3 من W3C Datatypes:2001.

2.3.A الدالات الحسابية

يتعين أن تأخذ جميع الدالات الواردة أدناه متغيرين من نمط المعطيات المحدد أو النمط الصحيح أو النمط المضاعف، وأن تعيد عنصر نمط معطيات عدد صحيح أو مضاعف على التوالي. ومع ذلك، يمكن أن تأخذ دالات "add" (الإضافة) أكثر من متغيرين اثنين. وفي حال كان أحد المتغيرات "Indeterminate" في تعبير يحتوي على أي دالة من هذه الدالات، يتعين عندئذ تقييم التعبير على أنه "Indeterminate". وإذا كان القاسم صفراً في حالة دالات التقسيم، ينبغي عندئذ تقييم الدالة على أنها "Indeterminate".

ملاحظة – ينبغي استكمال كل تقييم من تقييمات الدالات على غرار ما تحدده مقابلاتها المنطقية في المرجع [IEEE 745].

```
urn:oasis:names:tc:xacml:1.0:function:integer-add
```

وقد يكون لهذه الدالة متغيرين أو أكثر.

```
urn:oasis:names:tc:xacml:1.0:function:double-add
```

وقد يكون لهذه الدالة متغيرين أو أكثر.

```
urn:oasis:names:tc:xacml:1.0:function:integer-subtract
urn:oasis:names:tc:xacml:1.0:function:double-subtract
urn:oasis:names:tc:xacml:1.0:function:integer-multiply
urn:oasis:names:tc:xacml:1.0:function:double-multiply
urn:oasis:names:tc:xacml:1.0:function:integer-divide
urn:oasis:names:tc:xacml:1.0:function:double-divide
urn:oasis:names:tc:xacml:1.0:function:integer-mod
```

ويتعين أن تأخذ الدالة المبينة أدناه متغيراً وحيداً من نمط المعطيات المُحدد. ويتعين أن تأخذ وظيفتا النطاق والقاع متغيراً وحيداً من نمط المعطيات "http://www.w3.org/2001/XMLSchema#double" وأن تعيد قيمة من نمط المعطيات "http://www.w3.org/2001/XMLSchema#double".

```
urn:oasis:names:tc:xacml:1.0:function:integer-abs
urn:oasis:names:tc:xacml:1.0:function:double-abs
urn:oasis:names:tc:xacml:1.0:function:round
urn:oasis:names:tc:xacml:1.0:function:floor
```

3.3.A دالات تحويل السلسلة

تحول الدالات الواردة أدناه قيم الأنماط الأولية من نمط المعطيات "http://www.w3.org/2001/XMLSchema#string".

```
urn:oasis:names:tc:xacml:1.0:function:string-normalize-space
```

ويتعين أن تأخذ هذه الدالة متغيراً واحداً من نمط المعطيات "http://www.w3.org/2001/XMLSchema#string" وأن تقيّس القيمة بتجريدها من جميع رموز المجالات البيضاء الموجودة في المقدمة والمؤخرة.

```
urn:oasis:names:tc:xacml:1.0:function:string-normalize-to-lower-case
```

ويتعين أن تأخذ هذه الدالة متغيراً واحداً من نمط المعطيات "http://www.w3.org/2001/XMLSchema#string" وأن تقيّس القيمة بتحويل كل حرف كبير إلى حرف صغير يكافئه.

4.3.A دالات تحويل نمط المعطيات رقمياً

تحول الدالات المبينة أدناه نمط المعطيات "http://www.w3.org/2001/XMLSchema#integer" والأنماط الأولية "http://www.w3.org/2001/XMLSchema#double".

```
urn:oasis:names:tc:xacml:1.0:function:double-to-integer
```

ويتعين أن تأخذ هذه الدالة متغيراً واحداً من نمط المعطيات "http://www.w3.org/2001/XMLSchema#double" وأن تحول قيمته الرقمية إلى عدد صحيح وتعيد عنصراً من نمط المعطيات "http://www.w3.org/2001/XMLSchema#integer".

```
urn:oasis:names:tc:xacml:1.0:function:integer-to-double
```

ويتعين أن تأخذ هذه الدالة متغيراً واحداً من نمط المعطيات "http://www.w3.org/2001/XMLSchema#integer" وأن ترفع قيمته إلى عنصر من نمط المعطيات "http://www.w3.org/2001/XMLSchema#double" بالقيمة الرقمية نفسها.

5.3.A الدالات المنطقية

تتضمن هذه الفقرة مواصفة دالات منطقية تعمل على متغيرات من نمط المعطيات "http://www.w3.org/2001/XMLSchema#boolean".

```
urn:oasis:names:tc:xacml:1.0:function:or
```

ويتعين أن تعيد هذه الدالة قيمة "False" إن لم يكن لديها متغيرات، وأن تعيد قيمة "True" إذا تم تقييم متغير واحد من متغيراتها على الأقل على أنه "True". ويتعين أن يكون ترتيب التقييم من أول متغير إلى آخر متغير. وينبغي أن ينتهي التقييم بنتيجة "True" إذا تم تقييم أي من المتغيرات على أنه "True"، مع ترك ما تبقى من متغيرات دون تقييم.

```
urn:oasis:names:tc:xacml:1.0:function:and
```

ويتعين أن تعيد هذه الدالة قيمة "True" إن لم يكن لديها متغيرات، وأن تعيد قيمة "False" إذا تم تقييم أحد متغيراتها على أنه "False". ويتعين أن يكون ترتيب التقييم من أول متغير إلى آخر متغير. وينبغي أن ينتهي التقييم بنتيجة "False" إذا تم تقييم أي من المتغيرات على أنه "False"، مع ترك ما تبقى من متغيرات دون تقييم.

```
urn:oasis:names:tc:xacml:1.0:function:n-of
```

ويتعين أن يكون أول متغير من هذه الدالة من نمط المعطيات "http://www.w3.org/2001/XMLSchema#integer". ويتعين أن تكون المتغيرات المتبقية من نمط المعطيات "http://www.w3.org/2001/XMLSchema#boolean". ويحدد المتغير الأول الحد الأدنى لعدد المتغيرات المتبقية التي يجب أن تُقيّم على أنها "True" في التعبير المقرر النظر إليه على أنه "True". وإذا كان أول متغير 0، ينبغي أن تكون النتيجة "True". وإذا كان عدد المتغيرات التي تلي أول متغير أقل من قيمة المتغير الأول، يُحصل حينئذ من التعبير على نتيجة "indeterminate". ويتعين أن يكون ترتيب التقييم كالتالي: تُقدر أولاً قيمة المتغير الصحيح، ثم يتم تقييم كل متغير من المتغيرات التي تليه. ويتعين أن ينتهي التقييم ويعيد النتيجة "True" إذا تم تقييم العدد المحدد من المتغيرات على أنه "True". ويتعين إنهاء التقييم إذا رئي أن تقييم المتغيرات المتبقية لا يفي بالمتطلبات اللازمة.

```
urn:oasis:names:tc:xacml:1.0:function:not
```

ويتعين أن تأخذ هذه الدالة متغيراً واحداً من نمط المعطيات "http://www.w3.org/2001/XMLSchema#boolean". وإذا تم تقييم المتغير على أنه "True"، يتعين عندئذ أن تكون نتيجة التعبير "False"، أما إذا تم تقييمه على أنه "False"، يتعين عندئذ أن تكون النتيجة "True".

ملاحظة – عند تقييم and, or, or n-of فقد لا تقتضي الضرورة محاولة إجراء تقييم كامل لكل متغير من أجل البت فيما إذا كان تقييم المتغير سيفضي إلى الحصول على نتيجة "Indeterminate". وقد يؤدي تحليل المتغير من حيث مدى توفر نعوته، أو غيره من التحليلات من حيث الأخطاء، "كالقسمة على صفر"، إلى خلو المتغير من الأخطاء. ولا داعي لمعالجة هذه المتغيرات الواردة في التعبير في موقع يُقال فيه إن التقييم قد انتهى.

6.3.A دالات المقارنة الرقمية

تشكل هذه الدالات مجموعة بحد أدنى لمقارنة رقمين يُحصل منها على نتيجة بولانية.

ملاحظة – ينبغي أن تمتثل هذه الدالات للقواعد الناظمة الواردة في [IEEE 754].

```
urn:oasis:names:tc:xacml:1.0:function:integer-greater-than
urn:oasis:names:tc:xacml:1.0:function:integer-greater-than-or-equal
urn:oasis:names:tc:xacml:1.0:function:integer-less-than
urn:oasis:names:tc:xacml:1.0:function:integer-less-than-or-equal
urn:oasis:names:tc:xacml:1.0:function:double-greater-than
urn:oasis:names:tc:xacml:1.0:function:double-greater-than-or-equal
urn:oasis:names:tc:xacml:1.0:function:double-less-than
urn:oasis:names:tc:xacml:1.0:function:double-less-than-or-equal
```

7.3.A دالات التاريخ والوقت الحسابية

تجري هذه الدالات العمليات الحسابية المتعلقة بالتاريخ والوقت.

```
urn:oasis:names:tc:xacml:1.0:function:dateTime-add-dayTimeDuration
```

ويتعين أن تأخذ هذه الدالة متغيرين اثنين، ينبغي أن يكون أولهما من نمط المعطيات "http://www.w3.org/2001/XMLSchema#dateTime"، والثاني من نمط "urn:oasis:names:tc:xacml:2.0:data-types:dayTimeDuration". ويتعين أن تعيد نتيجة "http://www.w3.org/2001/XMLSchema#dateTime". وينبغي أن تعيد هذه الدالة القيمة بإضافة المتغير الثاني إلى الأول وفقاً لأحكام التذييل E من W3C Datatypes:2001.

```
urn:oasis:names:tc:xacml:1.0:function:dateTime-add-yearMonthDuration
```

ويتعين أن تأخذ هذه الدالة متغيرين اثنين، ينبغي أن يكون أولهما من نمط المعطيات "http://www.w3.org/2001/XMLSchema#dateTime"، والثاني من نمط "urn:oasis:names:tc:xacml:2.0:data-types:yearMonthDuration". ويتعين أن تعيد نتيجة "http://www.w3.org/2001/XMLSchema#dateTime". وينبغي أن تعيد هذه الدالة القيمة بإضافة المتغير الثاني إلى الأول وفقاً لأحكام التذييل E من W3C Datatypes:2001.

```
urn:oasis:names:tc:xacml:1.0:function:dateTime-subtract-dayTimeDuration
```

ويتعين أن تأخذ هذه الدالة متغيرين اثنين، ينبغي أن يكون أولهما من نمط المعطيات "http://www.w3.org/2001/XMLSchema#dateTime"، والثاني من نمط "urn:oasis:names:tc:xacml:2.0:data-types:dayTimeDuration". ويتعين أن تعيد نتيجة

"http://www.w3.org/2001/XMLSchema#dateTime". وإذا كان المتغير الثاني مدة إيجابية، يتعين حينئذ أن تعيد هذه الدالة القيمة بإضافة المدة السلبية المقابلة بحسب أحكام التذييل E من W3C Datatypes:2001. أما إذا كان المتغير الثاني مدة سلبية، ينبغي حينئذ أن تكون النتيجة وكأن الدالة "urn:oasis:names:tc:xacml:1.0:function:dateTime-add-dayTimeDuration" قد طُبِّقت على المدة الإيجابية المقابلة.

urn:oasis:names:tc:xacml:1.0:function:dateTime-subtract-yearMonthDuration

ويتعين أن تأخذ هذه الدالة متغيرين اثنين، ينبغي أن يكون أولهما من نمط المعطيات "http://www.w3.org/2001/XMLSchema#dateTime"، والثاني من نمط "urn:oasis:names:tc:xacml:2.0:data-types:dayTimeDuration". ويتعين أن تعيد نتيجة "http://www.w3.org/2001/XMLSchema#dateTime". وإذا كان المتغير الثاني مدة إيجابية، يتعين حينئذ أن تعيد هذه الدالة القيمة بإضافة المدة السلبية المقابلة، وذلك وفقاً لأحكام التذييل E من W3C Datatypes:2001. أما إذا كان المتغير الثاني مدة سلبية، ينبغي حينئذ أن تكون النتيجة وكأن الدالة "urn:oasis:names:tc:xacml:1.0:function:dateTime-add-yearMonthDuration" قد طُبِّقت على المدة الإيجابية المقابلة.

urn:oasis:names:tc:xacml:1.0:function:date-add-yearMonthDuration

ويتعين أن تأخذ هذه الدالة متغيرين اثنين، ينبغي أن يكون أولهما من نمط المعطيات "http://www.w3.org/2001/XMLSchema#date"، والثاني من نمط "urn:oasis:names:tc:xacml:2.0:data-types:yearMonthDuration". ويتعين أن تعيد نتيجة "http://www.w3.org/2001/XMLSchema#date". وينبغي أن تعيد هذه الدالة القيمة بإضافة المتغير الثاني إلى الأول وفقاً لأحكام التذييل E من W3C Datatypes:2001.

urn:oasis:names:tc:xacml:1.0:function:date-subtract-yearMonthDuration

ويتعين أن تأخذ هذه الدالة متغيرين اثنين، ينبغي أن يكون أولهما من نمط المعطيات "http://www.w3.org/2001/XMLSchema#date"، والثاني من نمط "urn:oasis:names:tc:xacml:2.0:data-types:yearMonthDuration". ويتعين أن تعيد نتيجة "http://www.w3.org/2001/XMLSchema#date". وإذا كان المتغير الثاني مدة إيجابية، يتعين حينئذ أن تعيد هذه الدالة القيمة بإضافة المدة السلبية المقابلة، وذلك وفقاً لأحكام (التذييل E من W3C Datatypes:2001). أما إذا كان المتغير الثاني مدة سلبية، ينبغي حينئذ أن تكون النتيجة وكأن الدالة "urn:oasis:names:tc:xacml:1.0:function:dateTime-add-yearMonthDuration" قد طُبِّقت على المدة الإيجابية المقابلة.

8.3.A دالات المقارنة غير الرقمية

تجري هذه الدالات عمليات مقارنة على متغيرين من نمطين غير رقميين.

urn:oasis:names:tc:xacml:1.0:function:string-greater-than

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#string" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا قُورِن المتغيران بايتة بايتة، وبعد بادئة أولية للبايتات المقابلة من متغيرين يعتبران كليهما متساويين بموجب "urn:oasis:names:tc:xacml:1.0:function:integer-equal"، تُجرى المقارنة اللاحقة لكل بايتة على حدة بطريقة تكون فيها بايتة المتغير الأول أكبر من بايتة المتغير الثاني باستعمال الدالة "urn:oasis:names:tc:xacml:2.0:function:integer-greater-then". وبخلاف ذلك، تعيد الدالة قيمة "False".

urn:oasis:names:tc:xacml:1.0:function:string-greater-than-or-equal

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#string" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة نتيجة كما لو كانت مقيّمة بالدالة المنطقية "urn:oasis:names:tc:xacml:1.0:function:or" بمتغيرين يحتويان على الدالتين "urn:oasis:names:tc:xacml:1.0:function:string-greater-than" و "urn:oasis:names:tc:xacml:1.0:function:string-equal" الطقمين على المتغيرين الأصليين.

urn:oasis:names:tc:xacml:1.0:function:string-less-than

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#string" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا قُورِن المتغيران بايتة بايتة، وبعد بادئة أولية للبايتات المقابلة من متغيرين يعتبران كليهما متساويين بموجب "urn:oasis:names:tc:xacml:1.0:function:integer-equal"، تُجرى المقارنة اللاحقة لكل بايتة على حدة بطريقة تكون فيها بايتة المتغير الأول أقل من بايتة المتغير الثاني باستعمال الدالة "urn:oasis:names:tc:xacml:2.0:function:integer-greater-then". وبخلاف ذلك، تعيد الدالة قيمة "False".

urn:oasis:names:tc:xacml:1.0:function:string-less-than-or-equal

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#string" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة نتيجة كما لو كانت مقيّمة بالدالة

"urn:oasis:names:tc:xacml:1.0:function:or" بمتغيرين يحتويان على الدالتين "urn:oasis:names:tc:xacml:1.0:function:string-less-than" و"urn:oasis:names:tc:xacml:1.0:function:string-equal" الطقمين على المتغيرين الأصليين.

```
urn:oasis:names:tc:xacml:1.0:function:time-greater-than
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#time" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول أكبر من الثاني وفقاً لعلاقة الترتيب المحددة في http://www.w3.org/2001/XMLSchema#time (الفقرة 8.2.3 من المرجع W3C Signature:2002) وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False".

الملاحظة 1 – ليس من الملائم مقارنة وقت يتضمن قيمة نطاق زمني مع وقت لا يتضمنها. وينبغي في هذه الحالات استعمال دالة time-in-range.

```
urn:oasis:names:tc:xacml:1.0:function:time-greater-than-or-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#time" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول أكبر من الثاني أو يساويه طبقاً لعلاقة الترتيب المحددة في "http://www.w3.org/2001/XMLSchema#time" (الفقرة 8.2.3 من المرجع W3C Datatypes:2002) وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False".

الملاحظة 2 – ليس من الملائم مقارنة وقت يتضمن قيمة نطاق زمني مع وقت لا يتضمنها. وينبغي في هذه الحالات استعمال دالة time-in-range.

```
urn:oasis:names:tc:xacml:1.0:function:time-less-than
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#time" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول أقل من الثاني وفقاً لعلاقة الترتيب المحددة في "http://www.w3.org/2001/XMLSchema#time" (الفقرة 8.2.3 من المرجع W3C Datatypes:2002) وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False".

الملاحظة 3 – ليس من الملائم مقارنة وقت يتضمن قيمة نطاق زمني مع وقت لا يتضمنها. وينبغي في هذه الحالات استعمال دالة time-in-range.

```
urn:oasis:names:tc:xacml:1.0:function:time-less-than-or-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#time" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول أقل من الثاني أو يساويه وفقاً لعلاقة الترتيب المحددة في "http://www.w3.org/2001/XMLSchema#time" وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False".

الملاحظة 4 – ليس من الملائم مقارنة وقت يتضمن قيمة نطاق زمني مع وقت لا يتضمنها. وينبغي في هذه الحالات استعمال دالة time-in-range.

```
urn:oasis:names:tc:xacml:1.0:function:time-in-range
```

ويتعين أن تأخذ هذه الدالة ثلاثة متغيرات من نمط المعطيات "http://www.w3.org/2001/XMLSchema#time" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول يندرج ضمن المدى الذي يحدده ضمناً المتغيران الثاني والثالث. وبخلاف ذلك، تعيد الدالة قيمة "False". وبصرف النظر عن قيمة المتغير الثالث، يتعين تفسير هذا المتغير على أنه وقت يساوي وقت المتغير الثاني بأربع وعشرين ساعة أو يتجاوزه أو يقل عنه. وفي حال عدم تقديم نطاق زمني للمتغير الأول، يتعين أن يستعمل المتغير النطاق الزمني المحدد بالتغيب في مدير السياق. وإن لم يُقدم نطاق زمني للمتغير الثاني أو الثالث، يتعين أن يستعملا النطاق الزمني للمتغير الأول.

```
urn:oasis:names:tc:xacml:1.0:function:dateTime-greater-than
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#dateTime" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول أكبر من الثاني وفقاً لعلاقة الترتيب المحددة في "http://www.w3.org/2001/XMLSchema#dateTime" بموجب الفقرة 7.2.3 من المرجع W3C Datatype:2001. وبخلافه، يتعين أن تعيد الدالة قيمة "False".

الملاحظة 5 – إذا كانت قيمة dateTime لا تحتوي على قيمة نطاق زمني، يتعين حينئذ تخصيص قيمة نطاق زمني ضمنية بحسب الوصف الوارد في W3C Datatype:2001.

```
urn:oasis:names:tc:xacml:1.0:function:dateTime-greater-than-or-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#dateTime" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول أكبر من الثاني أو يساويه وفقاً لعلاقة الترتيب المحددة في "http://www.w3.org/2001/XMLSchema#dateTime" بموجب الفقرة 7.2.3 من W3C Datatype:2001 وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False".

الملاحظة 6 – إذا كانت قيمة dateTime لا تحتوي على قيمة نطاق زمني، يتعين حينئذ تخصيص قيمة نطاق زمني ضمنية بحسب الوصف الوارد في W3C Datatype:2001.

```
urn:oasis:names:tc:xacml:1.0:function:dateTime-less-than
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#dateTime" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول أقل من الثاني وفقاً لعلاقة الترتيب المحددة في "http://www.w3.org/2001/XMLSchema#dateTime" بموجب الفقرة 7.2.3 من W3C Datatype:2001 وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False".

الملاحظة 7 – إذا كانت قيمة dateTime لا تحتوي على قيمة نطاق زمني، يتعين حينئذ تخصيص قيمة نطاق زمني ضمنية بحسب الوصف الوارد في W3C Datatype:2001.

```
urn:oasis:names:tc:xacml:1.0:function:dateTime-less-than-or-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#dateTime" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول أقل من الثاني أو يساويه وفقاً لعلاقة الترتيب المحددة في "http://www.w3.org/2001/XMLSchema#dateTime" بموجب الفقرة 7.2.3 من W3C Datatype:2001. وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False".

الملاحظة 8 – إذا كانت قيمة dateTime لا تحتوي على قيمة نطاق زمني، يتعين حينئذ تخصيص قيمة نطاق زمني ضمنية بحسب الوصف الوارد في W3C Datatype:2001.

```
urn:oasis:names:tc:xacml:1.0:function:date-greater-than
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#date" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول أكبر من الثاني وفقاً لعلاقة الترتيب المحددة في "http://www.w3.org/2001/XMLSchema#date". وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False".

الملاحظة 9 – إذا كانت قيمة التاريخ لا تحتوي على قيمة نطاق زمني، يتعين حينئذ تخصيص قيمة نطاق زمني ضمنية بحسب الوصف الوارد في W3C Datatype:2001.

```
urn:oasis:names:tc:xacml:1.0:function:date-greater-than-or-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#date" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول أكبر من الثاني أو يساويه وفقاً لعلاقة الترتيب المحددة في "http://www.w3.org/2001/XMLSchema#date". وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False".

الملاحظة 10 – إذا كانت قيمة التاريخ لا تحتوي على قيمة نطاق زمني، يتعين حينئذ تخصيص قيمة نطاق زمني ضمنية بحسب الوصف الوارد في W3C Datatype:2001.

```
urn:oasis:names:tc:xacml:1.0:function:date-less-than
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#date" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول أقل من الثاني وفقاً لعلاقة الترتيب المحددة في "http://www.w3.org/2001/XMLSchema#date". وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False".

الملاحظة 11 – إذا كانت قيمة التاريخ لا تحتوي على قيمة نطاق زمني، يتعين حينئذ تخصيص قيمة نطاق زمني ضمنية بحسب الوصف الوارد في W3C Datatype:2001.

```
urn:oasis:names:tc:xacml:1.0:function:date-less-than-or-equal
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط المعطيات "http://www.w3.org/2001/XMLSchema#date" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول أقل من الثاني أو يساويه طبقاً لعلاقة الترتيب المحددة في "http://www.w3.org/2001/XMLSchema#date". وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False".

الملاحظة 12 – إذا كانت قيمة التاريخ لا تحتوي على قيمة نطاق زمني، يتعين حينئذ تخصيص قيمة نطاق زمني ضمنية بحسب الوصف الوارد في W3C Datatype:2001.

9.3.A دالات السلسلة

تعمل الدالات المبينة أدناه على السلاسل ومعرفات URI.

```
urn:oasis:names:tc:xacml:2.0:function:string-concatenate
```

ويتعين أن تأخذ هذه الدالة متغيرين أو أكثر من نمط المعطيات "http://www.w3.org/2001/XMLSchema#string" وأن تعيد "http://www.w3.org/2001/XMLSchema#string". ويتعين أن تكون النتيجة تسلسل المتغيرات بحسب الترتيب.

```
urn:oasis:names:tc:xacml:2.0:function:url-string-concatenate
```

ويتعين أن تأخذ هذه الدالة متغيراً واحداً من نمط المعطيات "http://www.w3.org/2001/XMLSchema#anyURI" ومتغيراً واحداً أو أكثر من نمط "http://www.w3.org/2001/XMLSchema#string" وأن تعيد "http://www.w3.org/2001/XMLSchema#anyURI". ويتعين أن تتمثل النتيجة في تكوين معرف URI عن طريق إلحاق متغيرات "string" بحسب الترتيب بالمتغير "anyURI".

10.3.A دالات المجموعة غير المرتبة

تعمل هذه الدالات على مجموعة غير مرتبة من قيم 'type'، حيث النمط هو أحد الأنماط الأولية للمعطيات. وتؤدي بعض الشروط الإضافية المحددة لكل واحدة من الدالات المبينة أدناه إلى تقييم التعبير على أنه "Indeterminate".

```
urn:oasis:names:tc:xacml:1.0:function:type-one-and-only
```

ويتعين أن تأخذ هذه الدالة طقم قيم 'type' كمتغير وأن تعيد قيمة 'type-'. ويتعين أن تعيد القيمة الوحيدة في المجموعة. وفي حال عدم وجود قيمة واحدة ووحيدة في المجموعة، يُقيّم التعبير عندئذ على أنه "Indeterminate".

```
urn:oasis:names:tc:xacml:1.0:function:type-bag-size
```

ويتعين أن تأخذ هذه الدالة طقم قيم 'type' كمتغير وأن تعيد "http://www.w3.org/2001/XMLSchema#integer" مبينة عدد القيم الموجودة في المجموعة.

```
urn:oasis:names:tc:xacml:1.0:function:type-is-in
```

ويتعين أن تأخذ هذه الدالة متغير من نمط 'type' بوصفه المتغير الأول وطقم قيم نمط بوصفه المتغير الثاني وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تُقيّم الدالة على أنها "True" إذا، وفقط إذا كان المتغير الأول مطابقاً بموجب أي قيمة من قيم "urn:oasis:names:tc:xacml:x.x:function:type-equal" في المجموعة. وبخلاف ذلك، يتعين أن تعيد الدالة قيمة "False".

```
urn:oasis:names:tc:xacml:1.0:function:type-bag
```

ويتعين أن تأخذ هذه الدالة عدداً غير محدد من متغيرات 'type' وتعيد طقم قيم 'type' الحاوي على قيم المتغيرات. ويؤدي تطبيق هذه الدالة على متغيرات صفرية إلى الحصول على مجموعة غير مرتبة خالية من نمط المعطيات المحدد.

11.3.A دالات المجموعة

تعمل هذه الدالات على أطقم تحاكي المجموعات من خلال حذف العناصر المزدوجة من أحد الأطقم.

```
urn:oasis:names:tc:xacml:1.0:function:type-intersection
```

ويتعين أن تأخذ هذه الدالة متغيرين يمثلان كليهما طقم قيم 'type'، وأن تعيد طقم قيم 'type' بحيث لا يحتوي إلا على عناصر مشتركة بين الطقمين، وهو أمر يحدده "urn:oasis:names:tc:xacml:x.x:function:type-equal". ويتعين ألا تحتوي النتيجة على عناصر مزدوجة بحسب ما يحدده "urn:oasis:names:tc:xacml:x.x:function:type-equal".

```
urn:oasis:names:tc:xacml:1.0:function:type-at-least-one-member-of
```

ويتعين أن تأخذ هذه الدالة متغيرين يمثلان كليهما طقم قيم 'type'، وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تُقيّم الدالة على أنها "True" إذا، وفقط إذا وجد عنصر واحد على الأقل من عناصر المتغير الأول في المتغير الثاني بحسب ما هو محدد في "urn:oasis:names:tc:xacml:x.x:function:type-equal".

```
urn:oasis:names:tc:xacml:1.0:function:type-union
```

ويتعين أن تأخذ هذه الدالة متغيرين يمثلان كليهما طقم قيم 'type'. ويتعين أن يعيد التعبير طقم 'type' يحتوي على جميع عناصر الطقمين كليهما. ويتعين ألا تحتوي النتيجة على عناصر مزدوجة بحسب ما يحدده "urn:oasis:names:tc:xacml:x.x:function:type-equal".

```
urn:oasis:names:tc:xacml:1.0:function:type-subset
```

ويتعين أن تأخذ هذه الدالة متغيرين يمثلان كليهما طقم قيم 'type'، وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول مجموعة فرعية من الثاني. وينبغي النظر إلى كل متغير على أنه مجرد من العناصر المزدوجة بحسب ما هو محدد في "urn:oasis:names:tc:xacml:x.x:function:type-equal"، وذلك قبل حساب المجموعة الفرعية.

```
urn:oasis:names:tc:xacml:1.0:function:type-set-equals
```

ويتعين أن تأخذ هذه الدالة متغيرين يمثلان كليهما طقم قيم 'type'، وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة نتيجة تطبيق "urn:oasis:names:tc:xacml:1.0:function:and" على تطبيق "urn:oasis:names:tc:xacml:x.x:function:type-subset" إلى المتغيرين الأول والثاني وتطبيق "urn:oasis:names:tc:xacml:x.x:function:type-subset" على المتغيرين الثاني والأول.

12.3.A دالات الأطقم العالية الرتبة

تناقش هذه الفقرة دالات XACML التي تجري عمليات على الأطقم بطريقة تكفل تطبيق هذه الدالات على الأطقم عموماً.

ويمكن الاستفادة من إحدى اللغات الوظيفية ذات الأغراض العامة في تحديد دلالات معاني هذه الدالات (انظر التذييل III للاطلاع على مثال تعليمي لكيفية استعمال اللغة الوظيفية).

(1) urn:oasis:names:tc:xacml:1.0:function:any-of

تطبق هذه الدالة، دالة بولانية بين قيمة أولية محددة وطقم قيم، ويتعين أن تعيد قيمة "True" إذا، وفقط إذا كانت العبارة المنطقية "True" في عنصر واحد على الأقل من عناصر الطقم.

ويتعين أن تأخذ هذه الدالة ثلاثة متغيرات، ينبغي أن يكون أولها عنصر <xacml:Function> يسمي دالة بولانية تأخذ متغيرين من أنماط أولية. ويتعين أن يكون المتغير الثاني قيمة من نمط معطيات أولي. أما المتغير الثالث، فيتعين أن يكون طقم من نمط معطيات أولي. ويتعين تقييم التعبير وكأن الدالة المُسماة في المتغير <xacml:Function> قد طُبقت على المتغير الثاني وعلى جميع عناصر المتغير الثالث (الطقم)، والنتائج قد جُمِعت في "urn:oasis:names:tc:xacml:1.0:function:or".

(2) urn:oasis:names:tc:xacml:1.0:function:all-of

تطبق هذه الدالة، دالة بولانية بين قيمة أولية محددة وطقم قيم، وتعيد قيمة "True" إذا، وفقط إذا كانت العبارة المنطقية "True" في جميع عناصر الطقم.

ويتعين أن تأخذ هذه الدالة ثلاثة متغيرات، ينبغي أن يكون أولها عنصر <xacml:Function> يسمي دالة بولانية تأخذ متغيرين من أنماط أولية. ويتعين أن يكون المتغير الثاني قيمة من نمط معطيات أولي. أما المتغير الثالث، فيتعين أن يكون طقم من نمط معطيات أولي. ويتعين تقييم التعبير وكأن الدالة المُسماة في المتغير <xacml:Function> قد طُبقت على المتغير الثاني وعلى جميع عناصر المتغير الثالث (الطقم)، والنتائج قد جُمِعت في "urn:oasis:names:tc:xacml:1.0:function:and".

(3) urn:oasis:names:tc:xacml:1.0:function:any-of-any

تطبق هذه الدالة، دالة بولانية بين كل عنصر من عناصر إحدى أطقم القيم وكل عنصر من عناصر طقم قيم آخر، وتعيد قيمة "True" إذا، وفقط إذا كانت العبارة المنطقية "True" في مقارنة واحدة على الأقل.

ويتعين أن تأخذ هذه الدالة ثلاثة متغيرات، ينبغي أن يكون أولها عنصر <xacml:Function> يسمي دالة بولانية تأخذ متغيرين من أنماط أولية. ويتعين أن يكون المتغيران الثاني والثالث طقمين من نمط معطيات أولي. ويتعين تقييم التعبير وكأن الدالة المُسماة في المتغير <xacml:Function> قد طُبقت على جميع عناصر المتغيرين الثاني والثالث، والنتائج قد جُمِعت باستعمال "urn:oasis:names:tc:xacml:1.0:function:or". وتتمثل دلالات المعاني في ضرورة أن تكون نتيجة التعبير "True"، إذا، وفقط إذا كانت العبارة المنطقية المطبقة "True" في مقارنة واحدة على الأقل من مقارنات عناصر الطقمين كليهما.

(4) urn:oasis:names:tc:xacml:1.0:function:all-of-any

تطبق هذه الدالة، دالة بولانية بين عناصر الطقمين. ويتعين أن يكون التعبير "True" إذا، وفقط إذا كانت العبارة المنطقية المزودة "True" في جميع عناصر الطقم الأول وأي من عناصر الطقم الثاني.

ويتعين أن تأخذ هذه الدالة ثلاثة متغيرات، ينبغي أن يكون أولها عنصر <xacml:Function> يسمي دالة بولانية تأخذ متغيرين من أنماط أولية. ويتعين أن يكون المتغيران الثاني والثالث طقمين من نمط معطيات أولي. ويتعين تقييم التعبير وكأن الدالة "urn:oasis:names:tc:xacml:1.0:function:any-of" قد طُبقت على كل قيمة من قيم الطقم الأول وعلى كامل الطقم الثاني باستعمال الدالة المزودة xacml:Function، والنتائج قد جُمِعت بعدئذ باستعمال "urn:oasis:names:tc:xacml:1.0:function:and".

(5) urn:oasis:names:tc:xacml:1.0:function:any-of-all

تطبق هذه الدالة، دالة بولانية بين عناصر الطقمين كليهما. ويتعين أن يكون التعبير "True" إذا، وفقط إذا كانت العبارة المنطقية المزودة "True" بين كل عنصر من عناصر الطقم الثاني وأي من عناصر الطقم الأول.

ويتعين أن تأخذ هذه الدالة ثلاثة متغيرات، ينبغي أن يكون أولها عنصر <xacml:Function> يسمي دالة بولانية تأخذ متغيرين من أنماط أولية. ويتعين أن يكون المتغيران الثاني والثالث طقمين من نمط معطيات أولي. ويتعين تقييم التعبير وكأن الدالة "urn:oasis:names:tc:xacml:1.0:function:any-of" قد طُبقت على كل قيمة من قيم الطقم الثاني وعلى كامل الطقم الأول باستعمال الدالة المزودة xacml:Function، والنتائج قد جُمِعت بعدئذ باستعمال "urn:oasis:names:tc:xacml:1.0:function:and".

(6 urn:oasis:names:tc:xacml:1.0:function:all-of-all

تطبق هذه الدالة، دالة بولانية بين عناصر الطقمين. ويتعين أن يكون التعبير "True" إذا، وفقط إذا كانت العبارة المنطقية المزودة "True" بين كل عنصر من عناصرالطقم الأول بمقارنتها مجتمعة مع عناصر الطقم الثاني كافة.

ويتعين أن تأخذ هذه الدالة ثلاثة متغيرات، ينبغي أن يكون أولها عنصر <xacml:Function> يسمي دالة بولانية تأخذ متغيرين من أنماط أولية. ويتعين أن يكون المتغيران الثاني والثالث طقمين من نمط معطيات أولي. ويتعين تقييم التعبير وكأن الدالة المُسماة في عنصر <xacml:Function> قد طُبقت بين كل عنصر من عناصر المتغير الثاني وجميع عناصر المتغير الثالث، والنتائج قد جُمِعت باستعمال "urn:oasis:names:tc:xacml:1.0:function:and". وتتمثل دلالات المعاني في ضرورة أن تكون نتيجة التعبير "True" إذا، وفقط إذا كانت العبارة المنطقية المطبقة "True" في جميع عناصر الطقم الأول مقارنة بجميع عناصر الطقم الثاني.

(7 urn:oasis:names:tc:xacml:1.0:function:map

تحول هذه الدالة طقم قيم إلى طقم قيم آخر.

ويتعين أن تأخذ هذه الدالة متغيرين، ينبغي أن يكون أولهما عنصر <xacml:Function> يسمي دالة تأخذ متغيراً وحيداً من نمط معطيات أولي، وتعيد قيمة من نمط معطيات أولي. أما المتغير الثاني، فيتعين أن يكون طقم من نمط معطيات أولي. ويتعين تقييم التعبير وكأن الدالة المُسماة في عنصر <xacml:Function> قد طُبقت على كل عنصر من عناصر الطقم، بحيث يُحصل منها على طقم القيمة المحولة. ويتعين أن تكون النتيجة طقم من نمط معطيات أولي تعيدها الدالة المُسماة في عنصر <xacml:Function>.

13.3.A الدالات القائمة على التعابير العادية

تعمل هذه الدالات على أنماط عديدة تستعمل تعابير عادية وتقيَّم على أنها "http://www.w3.org/2001/XMLSchema#boolean".

urn:oasis:names:tc:xacml:1.0:function:string-regexp-match

وتحدد هذه الدالة مطابق التعبير العادي. ويتعين أن تأخذ متغيرين من نمط "http://www.w3.org/2001/XMLSchema#string" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". وينبغي أن يكون المتغير الأول تعبيراً عادياً والثاني سلسلة عامة. ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الثاني مطابقاً للقيمة الموجودة في مخطط التعبير العادي في المتغير الأول. ويتعين أن تكون قواعد تركيب المتغير الأول تلك المحددة في التذييل F من W3C Datatypes:2001، تكملها تعابير المخطط وقواعده الإضافية التالية:

- X?? لا تطابق X أكثر من مرة واحدة
- X*? تطابق X بعدد غير محدد من المرات، بما فيها الصفر
- X+? تطابق X مرة واحدة على الأقل
- X{n}? تطابق n X مرة بالضبط
- X(n,}? تطابق n X مرة على الأقل
- X{n,m}? تطابق n X مرة على الأقل، ولكنها لا تزيد على m مرة

وفي حال استعمال أحد تعابير المخطط الإضافية هذه، يتعين أن يطابق التعبير العادي أقصر سلسلة فرعية ممكنة من المتغير الأول المتساوق مع المخطط.

وفيما عدا هذه التعابير الإضافية، يتعين أن يطابق التعبير العادي أطول سلسلة فرعية ممكنة من المتغير الأول المتساوق مع المخطط.

وباستثناء الحالات التي يُثبّت فيها المخطط بوضوح في بداية السلسة أو نهايتها باستعمال رمزي السلسلة "^" و"$" على التوالي، يُعتبر المخطط مطابقاً إذا كان متساوقاً مع أي سلسلة من سلاسل المتغير الأول الفرعية.

ويتعين أن تدعم جميع حالات التنفيذ المطابقة مخططات التعبير العادي المحددة. ويمكن أن تدعم حالة التنفيذ المطابقة المزيد من مخططات التعبير العادي.

urn:oasis:names:tc:xacml:2.0:function:anyURI-regexp-match

وتحدد هذه الدالة مطابق التعبير العادي. ويتعين أن تأخذ متغيرين؛ أولهما من نمط "http://www.w3.org/2001/XMLSchema#string" والثاني من نمط "http://www.w3.org/2001/XMLSchema#anyURI". ويتعين أن تعيد "http://www.w3.org/2001/XMLSchema#boolean". وينبغي أن يكون المتغير الأول تعبيراً عادياً والثاني معرف URI. ويتعين أن تحول الدالة المتغير الثاني إلى نمط "http://www.w3.org/2001/XMLSchema#string"، ومن ثم تطبق "urn:oasis:names:tc:xacml:1.0:function:string-regexp-match".

```
urn:oasis:names:tc:xacml:2.0:function:ipAddress-regexp-match
```

وتحدد هذه الدالة مطابق التعبير العادي. ويتعين أن تأخذ متغيرين؛ أولهما من نمط "http://www.w3.org/2001/XMLSchema#string" والثاني من نمط "urn:oasis:names:tc:xacml:2.0:data-type:ipAddress". ويتعين أن تعيد "http://www.w3.org/2001/XMLSchema#boolean". وينبغي أن يكون المتغير الأول تعبيراً عادياً والثاني عنوان IPv4 أو عنوان IPv6. ويتعين أن تحول الدالة المتغير الثاني إلى نمط "http://www.w3.org/2001/XMLSchema#string"، ومن ثم تطبق "urn:oasis:names:tc:xacml:1.0:function:string-regexp-match".

```
urn:oasis:names:tc:xacml:2.0:function:dnsName-regexp-match
```

وتحدد هذه الدالة مطابق التعبير العادي. ويتعين أن تأخذ متغيرين؛ أولهما من نمط "http://www.w3.org/2001/XMLSchema#string" والثاني من نمط "urn:oasis:names:tc:xacml:2.0:data-type:dnsName". ويتعين أن تعيد "http://www.w3.org/2001/XMLSchema#boolean". وينبغي أن يكون المتغير الأول تعبيراً عادياً والثاني اسم DNS. ويتعين أن تحول الدالة المتغير الثاني إلى نمط "http://www.w3.org/2001/XMLSchema#string"، ومن ثم تطبق "urn:oasis:names:tc:xacml:1.0:function:string-regexp-match".

```
urn:oasis:names:tc:xacml:2.0:function:rfc822Name-regexp-match
```

وتحدد هذه الدالة مطابق التعبير العادي. ويتعين أن تأخذ متغيرين؛ أولهما من نمط "http://www.w3.org/2001/XMLSchema#string" والثاني من نمط "urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name". ويتعين أن تعيد "http://www.w3.org/2001/XMLSchema#boolean". وينبغي أن يكون المتغير الأول تعبيراً عادياً والثاني اسم RFC 822. ويتعين أن تحول الدالة المتغير الثاني إلى نمط "http://www.w3.org/2001/XMLSchema#string"، ومن ثم تطبق "urn:oasis:names:tc:xacml:1.0:function:string-regexp-match".

```
urn:oasis:names:tc:xacml:2.0:function:x500Name-regexp-match
```

وتحدد هذه الدالة مطابق التعبير العادي. ويتعين أن تأخذ متغيرين؛ أولهما من نمط "http://www.w3.org/2001/XMLSchema#string" والثاني من نمط "urn:oasis:names:tc:xacml:1.0:data-type:x500Name". ويتعين أن تعيد "http://www.w3.org/2001/XMLSchema#boolean". وينبغي أن يكون المتغير الأول تعبيراً عادياً والثاني اسم دليل X.500. ويتعين أن تحول الدالة المتغير الثاني إلى نمط "http://www.w3.org/2001/XMLSchema#string"، ومن ثم تطبق "urn:oasis:names:tc:xacml:1.0:function:string-regexp-match".

14.3.A دالات التطابق الخاصة

تعمل هذه الدالات على أنماط عديدة وتقيَّم على أنها "http://www.w3.org/2001/XMLSchema#boolean" بالاستناد إلى خوارزمية التطابق المعيارية الخاصة.

```
urn:oasis:names:tc:xacml:1.0:function:x500Name-match
```

ويتعين أن تأخذ هذه الدالة متغيرين من نمط "urn:oasis:names:tc:xacml:2.0:data-type:x500Name" وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا، وفقط إذا كان المتغير الأول يطابق تتابعاً مطرافياً معيناً لأسماء RDN من المتغير الثاني عند مقارنتها باستعمال x500Name-equal.

```
urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match
```

ويتعين أن تأخذ هذه الدالة متغيرين؛ أولهما من نمط المعطيات "http://www.w3.org/2001/XMLSchema#string" والثاني من نمط "urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name"، وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تُقيّم الدالة على أنها "True" إذا كان المتغير الأول مطابقاً للثاني وفقاً لأحكام الفقرة 1.2.3 من W3C Datatypes:2001.

ويتكون اسم IETF RFC 822 من جزء محلي تتبعه علامة "@" يليها جزء ميدان. والجزء المحلي حساس من حيث وضعية الحرف، بينما جزء الميدان ليس كذلك (الذي يكون عادة اسم DNS).

ويتضمن المتغير الثاني اسم rfc822 كامل. ويكون المتغير الأول اسم rfc822 كامل أو جزئي يُستعمل لانتقاء قيم مناسبة في المتغير الثاني على غرار ما يرد أدناه.

ولمطابقة عنوان معين في المتغير الثاني، يجب أن يحدد المتغير الأول العنوان البريدي الكامل المقرر مطابقته. ولمطابقة أي عنوان في ميدان محدد في المتغير الثاني، يجب ألا يحدد المتغير الأول سوى أحد أسماء الميدان (الذي يكون عادة اسم DNS). ولمطابقة أي عنوان في ميدان معين في المتغير الثاني، يجب أن يحدد المتغير الأول جزء الميدان المرغوب المسبوق بمقدمة ".".

15.3.A الدالات القائمة على XPath

تحدد هذه الفقرة الدالات التي تأخذ تعابير XPath في المتغيرات. ويقيّم تعبير XPath على أنه مجموعة عقد مكونة من عقد XML تطابق التعبير. ولا تندرج العقدة أو مجموعة العقد ضمن نطاق نظام XACML الرسمي لنمط المعطيات. وتُجرى جميع المقارنات أو العمليات الأخرى على مجموعات العقد بمعزل عن الدالة المعينة تحديداً، ما يعني أن تعابير XPath الموجودة في هذه الدالات مقيدة بسياق طلب XACML. ويمثل عنصر `<xacml-context:Request>` عقدة سياق كل تعبير من تعابير XPath. وفيما يلي الدالات المحددة هاهنا:

`urn:oasis:names:tc:xacml:1.0:function:xpath-node-count`

ويتعين أن تأخذ هذه الدالة "http://www.w3.org/2001/XMLSchema#string" كمتغير يُفسر على أنه أحد تعابير XPath، ويُقيم على أنه "http://www.w3.org/2001/XMLSchema#integer". ويتعين أن تكون القيمة التي تعيدها الدالة عدد العقد الموجودة داخل مجموعة العقد المطابقة لتعبير XPath معين.

`urn:oasis:names:tc:xacml:1.0:function:xpath-node-equal`

ويتعين أن تأخذ هذه الدالة متغيرين من نمط "http://www.w3.org/2001/XMLSchema#string"، يُفسران على أنهما تعبيرا XPath، وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". ويتعين أن تعيد الدالة قيمة "True" إذا كانت أي عقدة من عقد XML الموجودة في مجموعة العقد المطابقة للمتغير الأول، عقدة تساوي أي عقدة من عقد XML الموجودة في مجموعة العقد المطابقة للمتغير الثاني. وتُعتبر العقدتان متساويتان إذا كانتا متماثلتا الهوية.

`urn:oasis:names:tc:xacml:1.0:function:xpath-node-match`

ويتعين أن تأخذ هذه الدالة متغيرين من نمط "http://www.w3.org/2001/XMLSchema#string"، يُفسران على أنهما تعبيرا XPath، وأن تعيد "http://www.w3.org/2001/XMLSchema#boolean". وتُقيّم هذه الدالة على أنها "True" إذا استُوفي أحد الشرطين التاليين:

1) إذا كانت أي عقدة من عقد XML الموجودة في مجموعة العقد المطابقة للمتغير الأول، عقدة تساوي أي عقدة من عقد XML الموجودة في مجموعة العقد المطابقة للمتغير الثاني؛

2) إذا كانت أي عقدة نعت وعنصر تحت إحدى عقد XML الموجودة في مجموعة العقد المطابقة للمتغير الأول، عقدة تساوي أي عقدة من عقد XML الموجودة في مجموعة العقد المطابقة للمتغير الثاني.

وتُعتبر العقدتان متساويتان إذا كانتا متماثلتا الهوية.

ملاحظة – يكافئ الشرط الأول تعبير "xpath-node-equal"، ويكفل لهذا التعبير أن يكون حالة خاصة من "xpath-node-match".

16.3.A دالات التمديد والأنماط الأولية

تُحدّد الدالات والأنماط الأولية بواسطة معرفات سلاسل تفسح المجال أمام استقدام دالات معينة بالإضافة إلى الدالات التي تحددها XACML. ويمكّن هذا النهج الفرد من تمديد زجلة XACML بدالات خاصة وأنماط معطيات أولية خاصة.

وللحفاظ على تكامل استراتيجية التقييم XACML، يتعين ألا تعتمد نتيجة إحدى دالات التمديد إلا على قيم متغيراتها. وينبغي ألا تؤثر المعلمات العامة والمخفية على تقييم أحد التعابير. ويتعين ألا يكون للدالات آثار جانبية، لأن من المتعذر ضمان ترتيب التقييم بطريقة معيارية.

الملحق B

معرفات XACML

يحدد هذا الملحق معرفات معيارية لكيانات شائعة الاستعمال.

1.B مجالات اسم XACML

يوجد حالياً مجالان محددان من مجالات اسم XACML.

وتُحدد السياسات باستعمال هذا المعرف.

```
urn:oasis:names:tc:xacml:2.0:policy:schema:os
```

ويُحدد سياقا الطلب والإجابة باستعمال هذا المعرف.

```
urn:oasis:names:tc:xacml:2.0:context:schema:os
```

2.B فئات موضوع النفاذ

يبين هذا المعرف كيان النظام الذي استهل طلب النفاذ، أي الكيان الأولي في إحدى سلاسل الطلب. وفي حال عدم تحديد فئة الموضوع، فإن قيمة التغيب هي الواردة أدناه.

```
urn:oasis:names:tc:xacml:1.0:subject-category:access-subject
```

ويبين هذا المعرف كيان النظام الذي يستقبل نتائج الطلب (ويُستعمل عندما يكون مميزاً عن موضوع النفاذ).

```
urn:oasis:names:tc:xacml:1.0:subject-category:recipient-subject
```

ويبين هذا المعرف كيان نظام يمر عبره طلب النفاذ. وقد يكون هناك أكثر من كيان واحد منها. ولا تُتاح أية وسيلة لتحديد الترتيب الذي تمرر به الكيانات الرسالة.

```
urn:oasis:names:tc:xacml:1.0:subject-category:intermediary-subject
```

ويبين هذا المعرف كيان نظام مصاحب لقاعدة شفرة محلية أو بعيدة تكوّن الطلب. وقد تتضمن نعوت الموضوع المطابقة معرف URL الذي حُمّل منه الطلب و/أو حُصِل منه على هوية موقّع الشفرة. وقد يكون هناك أكثر من كيان واحد. ولا تُتاح أية وسيلة لتحديد الترتيب الذي تعالج به الكيانات الطلب.

```
urn:oasis:names:tc:xacml:1.0:subject-category:codebase
```

ويبين هذا المعرف كيان نظام مصاحب للحاسوب الذي استهل طلب ***النفاذ***. ومثال ذلك هوية IPSEC.

```
urn:oasis:names:tc:xacml:1.0:subject-category:requesting-machine
```

3.B أنماط المعطيات

تبين المعرفات الواردة أدناه أنماط معطيات تحددها الفقرة 2.A.

```
urn:oasis:names:tc:xacml:2.0:data-types:dayTimeDuration
urn:oasis:names:tc:xacml:2.0:data-types:yearMonthDuration
urn:oasis:names:tc:xacml:1.0:data-type:x500Name.
urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name
urn:oasis:names:tc:xacml:2.0:data-type:ipAddress
urn:oasis:names:tc:xacml:2.0:data-type:dnsName
```

ويحدد المرجع W3C DataTypes:2001 معرفات أنماط المعطيات التالية.

```
http://www.w3.org/2001/XMLSchema#string
http://www.w3.org/2001/XMLSchema#boolean
http://www.w3.org/2001/XMLSchema#integer
http://www.w3.org/2001/XMLSchema#double
http://www.w3.org/2001/XMLSchema#time
http://www.w3.org/2001/XMLSchema#date
http://www.w3.org/2001/XMLSchema#dateTime
http://www.w3.org/2001/XMLSchema#anyURI
```

```
http://www.w3.org/2001/XMLSchema#hexBinary
http://www.w3.org/2001/XMLSchema#base64Binary
```

4.B نعوت الموضوع

تبين هذه المعرفات نعوت أحد المواضيع. ويتعين عند استعمالها أن تظهر داخل أحد عناصر <Subject> سياق الطلب. وينبغي أن يُنفذ إليها بواسطة عنصر <SubjectAttributeDesignator>، أو عنصر <AttributeSelector> يشير إلى أحد عناصر <Subject> سياق الطلب.

ويتصاحب على الأكثر كل نعت من هذه النعوت مع كل موضوع. ويرتبط كل نعت مصاحب لاستيقان مدرج في داخل عنصر <Subject> وحيد، بصلة، بحدث الاستيقان نفسه.

ويبين هذا المعرف اسم الموضوع. ونسق التغيب هو "http://www.w3.org/2001/XMLSchema#string". ولبيان أنساق أخرى، تُستعمل نعوت DataType الواردة في الفقرة 3.B.

```
urn:oasis:names:tc:xacml:1.0:subject:subject-id
```

ويبين هذا المعرف فئة الموضوع. وقيمة التغيب هي "access-subject".

```
urn:oasis:names:tc:xacml:1.0:subject-category
```

ويبين هذا المعرف ميدان أمن الموضوع، ويحدد المدير والسياسة التي تدير مجال الاسم الذي يُدار فيه معرف id الموضوع.

```
urn:oasis:names:tc:xacml:1.0:subject:subject-id-qualifier
```

ويبين هذا المعرف مفتاح عام يُستعمل لإثبات هوية الموضوع.

```
urn:oasis:names:tc:xacml:1.0:subject:key-info
```

ويبين هذا المعرف وقت استيقان الموضوع.

```
urn:oasis:names:tc:xacml:1.0:subject:authentication-time
```

ويبين هذا المعرف الطريقة المُستعملة لاستيقان الموضوع.

```
urn:oasis:names:tc:xacml:1.0:subject:authn-locality:authentication-method
```

ويبين هذا المعرف الوقت الذي استهل فيه الموضوع طلب النفاذ وفقاً لبروتوكول PEP.

```
urn:oasis:names:tc:xacml:1.0:subject:request-time
```

ويبين هذا المعرف الوقت الذي بدأت فيه دورة الموضوع الحالية وفقاً لبروتوكول PEP.

```
urn:oasis:names:tc:xacml:1.0:subject:session-start-time
```

وتبين المعرفات الواردة أدناه موقع تنشيط معطيات اعتماد التوثيق. والغرض منها دعم الكيانات المطابقة المُستمدة من بيان استيقان SAML.

ويبين هذا المعرف أن الموقع مُعبر عنه كعنوان بروتوكول IP.

```
urn:oasis:names:tc:xacml:1.0:subject:authn-locality:ip-address
```

ويتعين أن يكون النعت المطابق من نمط المعطيات "http://www.w3.org/2001/XMLSchema#string".

ويبين هذا المعرف أن الموقع مُعبر عنه كاسم DNS.

```
urn:oasis:names:tc:xacml:1.0:subject:authn-locality:dns-name
```

ويتعين أن يكون النعت المطابق من نمط المعطيات "http://www.w3.org/2001/XMLSchema#string".

وفي حال حُدد بالفعل نعت مناسب في LDAP، يتعين تكوين معرف XACML بإضافة اسم النعت إلى معرف URI الوثيقة IETF LDAP RFC (انظر IETF RFC 2256). ويتعين مثلاً أن يكون اسم نعت userPassword المُحدد في IETF RFC 2256 كالتالي:

```
http://www.ietf.org/rfc/rfc2256.txt#userPassword
```

5.B نعوت المورد

تبين هذه المعرفات نعوت المورد. ويمكن أن تظهر النعوت المطابقة في عنصر <Resource> سياق الطلب، ويمكن النفاذ إليها بواسطة عنصر <ResourceAttributeDesignator>، أو عنصر <AttributeSelector> يشير إلى أحد عناصر <Resource> سياق الطلب.

ويعرف هذا النعت المورد الذي يُطلب النفاذ إليه. وفي حال تقديم عنصر <xacml-context:ResourceContent>، يكون عندئذ المورد الذي يُطلب النفاذ إليه كامل المورد المُقدم في العنصر المذكور أو جزءاً منه.

```
urn:oasis:names:tc:xacml:1.0:resource:resource-id
```

ويعرف هذا النعت مجال اسم أعلى عنصر من محتويات العنصر <xacml-context:ResourceContent>. وفي حال تزويد سياق الطلب بمحتويات المورد وتحديد مجال اسم المورد في المورد، يتعين أن يثبت بروتوكول PDP أن مجال الاسم الذي يحدده هذا النعت هو نفس مجال الاسم المحدد في المورد. ويتعين أن يكون النعت المطابق هو "http://www.w3.org/2001/XMLSchema#anyURI".

```
urn:oasis:names:tc:xacml:2.0:resource:target-namespace
```

6.B نعوت الفعل

تبين هذه المعرفات نعوت الفعل المطلوبة. ويتعين عند استعمالها أن تظهر داخل أحد عناصر <Action> سياق الطلب. وينبغي أن يُنفذ إليها بواسطة عنصر <ActionAttributeDesignator>، أو عنصر <AttributeSelector> يشير إلى أحد عناصر <Action> سياق الطلب.

ويعرف هذا النعت الفعل الذي يُطلب النفاذ إليه.

```
urn:oasis:names:tc:xacml:1.0:action:action-id
```

وفي حال كان الفعل ضمنياً، يتعين أن تكون قيمة نعت action-id كالآتي:

```
urn:oasis:names:tc:xacml:1.0:action:implied-action
```

ويعرف هذا النعت مجال الاسم الذي يُحدد فيه نعت action-id.

```
urn:oasis:names:tc:xacml:1.0:action:action-namespace
```

7.B نعوت البيئة

تبين هذه المعرفات نعوت البيئة التي يُقيم داخلها طلب القرار. ويتعين عند استعمالها في طلب القرار أن تظهر داخل أحد عناصر <Environment> سياق الطلب. وينبغي أن يُنفذ إليها بواسطة عنصر <EnvironmentAttributeDesignator>، أو عنصر <AttributeSelector> يشير إلى أحد عناصر <Environment> سياق الطلب.

ويبين هذ المعرف الوقت الحالي في مدير السياق. وهذا الوقت في الواقع هو وقت تكوين سياق الطلب. ولهذا السبب، إذا ظهرت هذه المعرفات في عدة مواقع داخل عنصر <Policy> أو <PolicySet>، يتعين عندئذ تخصيص القيمة نفسها لكل حالة حدوث في عملية التقييم، بصرف النظر عن طول الفترة الزمنية المستغرقة بين معالجة حالات الحدوث.

```
urn:oasis:names:tc:xacml:1.0:environment:current-time
```

ويتعين أن يكون النعت المطابق من نمط المعطيات "http://www.w3.org/2001/XMLSchema#time".

```
urn:oasis:names:tc:xacml:1.0:environment:current-date
```

ويتعين أن يكون النعت المطابق من نمط المعطيات "http://www.w3.org/2001/XMLSchema#date".

```
urn:oasis:names:tc:xacml:1.0:environment:current-dateTime
```

ويتعين أن يكون النعت المطابق من نمط المعطيات "http://www.w3.org/2001/XMLSchema#dateTime".

8.B شفرات الحالة

ترد أدناه قيم شفرة الحالة.

ويبين هذا المعرف مدى النجاح.

```
urn:oasis:names:tc:xacml:1.0:status:ok
```

ويبين هذا المعرف عدم تيسر جميع النعوت اللازمة لاتخاذ قرار سياسي.

```
urn:oasis:names:tc:xacml:1.0:status:missing-attribute
```

ويبين هذا المعرف أن بعض قيم النعت تحتوي على خطأ في قواعد التركيب، كرسالة ترد في مجال رقمي.

```
urn:oasis:names:tc:xacml:1.0:status:syntax-error
```

ويبين هذا المعرف حدوث خطأ أثناء تقييم السياسة. ومثال ذلك القسمة على صفر.

```
urn:oasis:names:tc:xacml:1.0:status:processing-error
```

9.B خوارزميات التوليف

فيما يلي قيمة خوارزمية توليف القواعد deny-overrides لنعت ruleCombiningAlgId:

```
urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides
```

وفيما يلي قيمة خوارزمية توليف السياسات deny-overrides لنعت policyCombiningAlgId:

```
urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides
```

وفيما يلي قيمة خوارزمية توليف القواعد permit-overrides لنعت ruleCombiningAlgId:

```
urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides
```

وفيما يلي قيمة خوارزمية توليف السياسات permit-overrides لنعت policyCombiningAlgId:

```
urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides
```

وفيما يلي قيمة خوارزمية توليف القواعد first-applicable لنعت ruleCombiningAlgId:

```
urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable
```

وفيما يلي قيمة خوارزمية توليف السياسات first-applicable لنعت policyCombiningAlgId:

```
urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:first-applicable
```

وفيما يلي قيمة خوارزمية توليف السياسات only-one-applicable-policy لنعت policyCombiningAlgId:

```
urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:only-one-applicable
```

وفيما يلي قيمة خوارزمية توليف القواعد ordered-deny-overrides لنعت ruleCombiningAlgId:

```
urn:oasis:names:tc:xacml:1.1:rule-combining-algorithm:ordered-deny-overrides
```

وفيما يلي قيمة خوارزمية توليف السياسات ordered-deny-overrides لنعت policyCombiningAlgId:

```
urn:oasis:names:tc:xacml:1.1:policy-combining-algorithm:ordered-deny-overrides
```

وفيما يلي قيمة خوارزمية توليف القواعد ordered-permit-overrides لنعت ruleCombiningAlgId:

```
urn:oasis:names:tc:xacml:1.1:rule-combining-algorithm:ordered-permit-overrides
```

وفيما يلي قيمة خوارزمية توليف السياسات ordered- permit -overrides لنعت policyCombiningAlgId:

```
urn:oasis:names:tc:xacml:1.1:policy-combining-algorithm:ordered-permit-
overrides
```

الملحق C

خوارزميات التوليف

يرد في هذا الملحق وصف لخوارزميات توليف القواعد والسياسات التي تحددها XACML.

1.C Deny-overrides

1.1.C تعرف هذه الفقرة خوارزمية توليف قواعد "Deny-overrides" إحدى السياسات.

وإذا تم تقييم أي قاعدة من كامل مجموعة قواعد السياسة، على أنها "Deny" (رفض)، يتعين عندئذ أن تكون نتيجة توليف القواعد "Deny". وإذا تم تقييم أي قاعدة منها على أنها "Permit"، وتقييم جميع القواعد الأخرى على أنها "NotApplicable"، يتعين عندئذ أن تكون نتيجة توليف القواعد "Permit". وبعبارة أخرى، تأخذ "Deny" الأسبقية، بغض النظر عن نتيجة تقييم أي قاعدة من قواعد التوليف الأخرى. وإذا رؤي أن جميع القواعد "NotApplicable" (لا تنطبق على) على طلب القرار، يتعين حينها تقييم توليفة القواعد على أنها "NotApplicable".

وإذا حصل خطأ عند تقييم هدف أو حالة إحدى القواعد الحاوية على قيمة أثر "Deny"، يتعين حينئذ مواصلة التقييم من أجل تقييم القواعد اللاحقة بحثاً عن نتيجة "Deny". وفي حال عدم تقييم أي قاعدة أخرى على أنها "Deny"، يتعين حينئذ تقييم التوليف على أنه "Indeterminate" بالاقتران مع حالة الخطأ المناسبة.

وإذا تم تقييم قاعدة واحدة على الأقل على أنها "Permit" وتقييم جميع القواعد الأخرى التي ليس فيها أخطاء تقييم على أنها "Permit" أو "NotApplicable"، واحتوت جميع القواعد التي فيها أخطاء تقييم فعلية على آثار "Permit"، يتعين حينئذ أن تكون نتيجة التوليف "Permit".

وتمثل شبه الشفرة الواردة أدناه إستراتيجية تقييم خوارزمية توليف القواعد هذه.

```
Decision denyOverridesRuleCombiningAlgorithm(Rule rule[])
{
   Boolean atLeastOneError  = false;
   Boolean potentialDeny    = false;
   Boolean atLeastOnePermit = false;
   for( i=0 ; i < lengthOf(rules) ; i++ )
   {
          Decision decision = evaluate(rule[i]);
          if (decision == Deny)
          {
                return Deny;
          }
          if (decision == Permit)
          {
                atLeastOnePermit = true;
                continue;
          }
          if (decision == NotApplicable)
          {
                continue;
          }
          if (decision == Indeterminate)
          {
                atLeastOneError = true;

                if (effect(rule[i]) == Deny)
                {
                      potentialDeny = true;
                }
                continue;
          }
   }
   if (potentialDeny)
   {
          return Indeterminate;
   }
   if (atLeastOnePermit)
   {
          return Permit;
   }
   if (atLeastOneError)
```

```
    {
          return Indeterminate;
    }
    return NotApplicable;
}
```

2.1.C تعرف هذه الفقرة خوارزمية توليف سياسات "Deny-overrides" إحدى مجموعات السياسات.

وإذا تم تقييم أي سياسة في كامل مجموعة السياسات، على أنها "Deny" (رفض)، يتعين عندئذ أن تكون نتيجة توليف السياسات "Deny". وبعبارة أخرى، تأخذ "Deny" الأسبقية، بصرف النظر عن نتيجة تقييم أي سياسة من سياسات التوليف الأخرى في مجموعة السياسات. وإذا رؤي أن جميع السياسات "NotApplicable" (لا تنطبق) على طلب القرار، يتعين حينها تقييم مجموعة السياسات على أنها "NotApplicable".

وإذا حصل خطأ عند تقييم هدف إحدى السياسات، أو اعتُبِرت إحدى الإشارات الدالة على سياسة معينة غير صحيحة، أو حُصِل من تقييم السياسة على نتيجة "Indeterminate"، يتعين حينئذ تقييم مجموعة السياسات على أنها "Deny".

وتمثل شبه الشفرة الواردة أدناه إستراتيجية تقييم خوارزمية توليف السياسات هذه.

```
Decision denyOverridesPolicyCombiningAlgorithm(Policy policy[])
{
    Boolean atLeastOnePermit = false;
    for( i=0 ; i < lengthOf(policy) ; i++ )
    {
          Decision decision = evaluate(policy[i]);
          if (decision == Deny)
          {
                return Deny;
          }
          if (decision == Permit)
          {
                atLeastOnePermit = true;
                continue;
          }
          if (decision == NotApplicable)
          {
                continue;
          }
          if (decision == Indeterminate)
          {
                return Deny;
          }
    }
    if (atLeastOnePermit)
    {
          return Permit;
    }
    return NotApplicable;
}
```

ويتعين توحيد التزامات السياسات الفردية على غرار الوصف الوارد في الفقرة 14.6.7.

Ordered-deny-overrides 2.C

تعرف الفقرة الواردة أدناه خوارزمية توليف قواعد "Ordered-deny-overrides" إحدى السياسات.

وسلوك هذه الخوارزمية مطابق لسلوك خوارزمية توليف قواعد "Deny-overrides"، مع وجود استثناء واحد. ويتعين أن يكون الترتيب الذي تقيّم بموجبه مجموعة القواعد مطابقاً للترتيب الوارد في السياسة.

وتعرف الفقرة الواردة أدناه خوارزمية توليف سياسات "Ordered-deny-overrides" إحدى مجموعات السياسات.

وسلوك هذه الخوارزمية مطابق لسلوك خوارزمية توليف سياسات "Deny-overrides"، مع وجود استثناء واحد. ويتعين أن يكون الترتيب الذي تقيّم بموجبه مجموعة السياسات مطابقاً للترتيب المبين في مجموعة السياسات.

Permit-overrides 3.C

1.3.C تعرف هذه الفقرة خوارزمية توليف قواعد "Permit-overrides" إحدى السياسات.

وإذا تم تقييم أي قاعدة من كامل مجموعة قواعد السياسة، على أنها "Permit"، يتعين عندئذ أن تكون نتيجة توليف القواعد "Permit". وإذا تم تقييم أي قاعدة منها على أنها "Deny"، وتقييم جميع القواعد الأخرى على أنها "NotApplicable"، يتعين عندئذ تقييم السياسة على أنها

"Deny". وبعبارة أخرى، تأخذ "Permit" الأسبقية، بغض النظر عن نتيجة تقييم أي قاعدة من القواعد الأخرى في السياسة. وإذا رؤي أن جميع القواعد "NotApplicable" (لا تنطبق) على طلب القرار، يتعين حينها تقييم السياسة على أنها "NotApplicable".

وإذا حصل خطأ عند تقييم هدف أو حالة إحدى القواعد الحاوية على أثر "Permit"، يتعين حينئذ مواصلة التقييم بحثاً عن نتيجة "Permit". وفي حال عدم تقييم أي قاعدة أخرى على أنها "Permit"، يتعين حينئذ تقييم السياسة على أنها "Indeterminate" بالاقتران مع حالة الخطأ المناسبة.

وإذا تم تقييم قاعدة واحدة على الأقل على أنها "Deny" وتقييم جميع القواعد الأخرى التي ليس فيها أخطاء تقييم على أنها "Deny" أو "NotApplicable"، واحتوت جميع القواعد التي فيها أخطاء تقييم فعلية على قيمة أثر "Deny"، يتعين حينئذ تقييم السياسة على أنها "Deny".

وتمثل شبه الشفرة الواردة أدناه استراتيجية تقييم خوارزمية توليف القواعد هذه.

```
Decision permitOverridesRuleCombiningAlgorithm(Rule rule[])
{
   Boolean atLeastOneError  = false;
   Boolean potentialPermit  = false;
   Boolean atLeastOneDeny   = false;
   for( i=0 ; i < lengthOf(rule) ; i++ )
   {
          Decision decision = evaluate(rule[i]);
          if (decision == Deny)
          {
                 atLeastOneDeny = true;
                 continue;
          }
          if (decision == Permit)
          {
                 return Permit;
          }
          if (decision == NotApplicable)
          {
                 continue;
          }
          if (decision == Indeterminate)
          {
                 atLeastOneError = true;

                 if (effect(rule[i]) == Permit)
                 {
                        potentialPermit = true;
                 }
                 continue;
          }
   }
   if (potentialPermit)
   {
          return Indeterminate;
   }
   if (atLeastOneDeny)
   {
          return Deny;
   }
   if (atLeastOneError)
   {
          return Indeterminate;
   }
   return NotApplicable;
}
```

2.3.C تعرف هذه الفقرة خوارزمية توليف سياسات "Permit-overrides" إحدى مجموعات السياسات.

وإذا تم تقييم أي سياسة في كامل مجموعة السياسات، على أنها "Permit"، يتعين عندئذ أن تكون نتيجة توليف السياسات "Permit". وبعبارة أخرى، تأخذ "Permit" الأسبقية، بصرف النظر عن نتيجة تقييم أي سياسة من السياسات الأخرى في مجموعة السياسات. وإذا رؤي أن جميع السياسات "NotApplicable" (لا تنطبق) على طلب القرار، يتعين حينها تقييم مجموعة السياسات على أنها "NotApplicable".

وإذا حصل خطأ عند تقييم هدف إحدى السياسات، أو اعتُبرت إحدى الإشارات الدالة على سياسة معينة غير صحيحة، أو حُصِل من تقييم السياسة على نتيجة "Indeterminate"، يتعين حينئذ تقييم مجموعة السياسات على أنها "Indeterminate" بالاقتران مع حالة الخطأ المناسبة، شريطة عدم تقييم سياسات أخرى على أنها "Permit" أو "Deny".

وتمثل شبه الشفرة الواردة أدناه استراتيجية تقييم خوارزمية توليف السياسات هذه.

```
Decision permitOverridesPolicyCombiningAlgorithm(Policy policy[])
{
   Boolean atLeastOneError = false;
   Boolean atLeastOneDeny  = false;
   for( i=0 ; i < lengthOf(policy) ; i++ )
   {
          Decision decision = evaluate(policy[i]);
          if (decision == Deny)
          {
                atLeastOneDeny = true;
                continue;
          }
          if (decision == Permit)
          {
                return Permit;
          }
          if (decision == NotApplicable)
          {
                continue;
          }
          if (decision == Indeterminate)
          {
                atLeastOneError = true;
                continue;
          }
   }
   if (atLeastOneDeny)
   {
          return Deny;
   }
   if (atLeastOneError)
   {
          return Indeterminate;
   }
   return NotApplicable;
}
```

ويتعين توحيد التزامات السياسات الفردية بحسب الوصف الوارد في الفقرة 14.6.7.

4.C Ordered-permit-overrides

تعرف الفقرة الواردة أدناه خوارزمية توليف قواعد "Ordered-permit-overrides" إحدى السياسات.

وسلوك هذه الخوارزمية مطابق لسلوك خوارزمية توليف قواعد "Permit-overrides"، مع وجود استثناء واحد. ويتعين أن يكون الترتيب الذي يتم بموجبه تقييم مجموعة القواعد مطابقاً للترتيب الوارد في السياسة.

وتعرف الفقرة الواردة أدناه خوارزمية توليف سياسات "Ordered-permit-overrides" إحدى مجموعات السياسات.

وسلوك هذه الخوارزمية مطابق لسلوك خوارزمية توليف سياسات Permit-overrides، مع وجود استثناء واحد. ويتعين أن يكون الترتيب الذي تقيّم بموجبه مجموعة السياسات مطابقاً للترتيب المبين في مجموعة السياسات.

5.C First-applicable

1.5.C تعرف هذه الفقرة خوارزمية توليف قواعد "First-applicable" إحدى السياسات.

ويتعين تقييم كل قاعدة بالترتيب الذي تظهر فيه في السياسة. وفي حال كان الهدف مطابقاً في قاعدة معينة وتم تقييم الحالة فيها على أنها "True"، يتعين حينئذ أن ينتهي تقييم السياسة وأن يكون أثر القاعدة المطابق نتيجة تقييم السياسة (أي، "Permit" أو "Deny"). أما إذا تم تقييم الهدف أو الحالة على أنها "False" في قاعدة منتقاة معينة، يتعين عندئذ تقييم القاعدة التالية في الترتيب. وفي حال عدم وجود أي قاعدة أخرى في الترتيب، يتعين حينها تقييم السياسة على أنها "NotApplicable".

وإذا حصل خطأ عند تقييم هدف القاعدة أو حالتها، يتعين عندئذ أن ينتهي التقييم، وأن تُقيّم السياسة على أنها "Indeterminate" بالاقتران مع حالة الخطأ المناسبة.

وتمثل شبه الشفرة الواردة أدناه استراتيجية تقييم خوارزمية توليف القواعد هذه.

```
Decision firstApplicableEffectRuleCombiningAlgorithm(Rule rule[])
{
   for( i = 0 ; i < lengthOf(rule) ; i++ )
   {
          Decision decision = evaluate(rule[i]);
          if (decision == Deny)
          {
                return Deny;
          }
          if (decision == Permit)
          {
                return Permit;
          }
          if (decision == NotApplicable)
          {
                continue;
          }
          if (decision == Indeterminate)
          {
                return Indeterminate;
          }
   }
   return NotApplicable;
}
```

2.5.C تعرف هذه الفقرة خوارزمية توليف سياسات "First-applicable" إحدى مجموعات السياسات.

ويتعين تقييم كل سياسة بالترتيب الذي تظهر فيه في مجموعة السياسات. وإذا تم تقييم الهدف في سياسة معينة على أنه "True"، وتقييم السياسة على قيمة محددة من قيم "Permit" أو "Deny"، يتعين حينئذ أن ينتهي التقييم وأن تُقيّم مجموعة السياسات على أنها قيمة أثر هذه السياسة. أما إذا تم تقييم الهدف في سياسة معينة على أنه "False"، أو تقييم السياسة على أنها "NotApplicable"، يتعين عندئذ تقييم السياسة التالية في الترتيب. وفي حال عدم وجود أي سياسة أخرى في الترتيب، يتعين حينها تقييم مجموعة السياسات على أنها "NotApplicable".

وإذا حصل خطأ عند تقييم الهدف، أو عند تقييم سياسة معينة، أو اعتبار الإشارة الدالة على السياسة غير صحيحة، أو عند تقييم السياسة بحد ذاتها على أنها "Indeterminate"، يتعين حينئذ أن ينتهي تقييم خوارزمية توليف السياسات، وأن تقيّم مجموعة السياسات على أنها "Indeterminate" بالاقتران مع حالة الخطأ المناسبة.

وتمثل شبه الشفرة الواردة أدناه استراتيجية تقييم خوارزمية توليف السياسات هذه.

```
Decision firstApplicableEffectPolicyCombiningAlgorithm(Policy policy[])
{
    for( i = 0 ; i < lengthOf(policy) ; i++ )
    {
        Decision decision = evaluate(policy[i]);
        if(decision == Deny)
        {
            return Deny;
        }
        if(decision == Permit)
        {
            return Permit;
        }
        if (decision == NotApplicable)
        {
            continue;
        }
        if (decision == Indeterminate)
        {
            return Indeterminate;
        }
    }
    return NotApplicable;
}
```

ويتعين توحيد التزامات السياسات الفردية بحسب الوصف الوارد في الفقرة 14.6.7.

6.C Only-one-applicable

تعرف هذه الفقرة خوارزمية توليف سياسات "Only-one-applicable" إحدى مجموعات السياسات.

وإذا لم يُنظر إلى أي سياسة في كامل مجموعة السياسات على أنها قابلة للانطباق بفضل هدفها، يتعين عندئذ أن تكون نتيجة خوارزمية توليف السياسات "NotApplicable". وفي حال النظر إلى أكثر من سياسة واحدة على أنها قابلة للانطباق بفضل هدفها، يتعين عندئذ أن تكون نتيجة خوارزمية توليف السياسات "Indeterminate".

وإذا رؤي أن هناك سياسة واحدة فقط قابلة للانطباق بفضل هدفها، يتعين عندئذ أن تكون نتيجة خوارزمية توليف السياسات نتيجة تقييم السياسة.

وإذا حصل خطأ عند تقييم هدف إحدى السياسات، أو اعتُبِرت إحدى الإشارات الدالة على سياسة معينة غير صحيحة، أو حُصِل من تقييم السياسة على نتيجة "Indeterminate"، يتعين حينئذ تقييمَ مجموعة السياسات على على أنها "Indeterminate" بالاقتران مع حالة الخطأ المناسبة.

وتمثل شبه الشفرة الواردة أدناه استراتيجية تقييم خوارزمية توليف السياسات هذه.

```
Decision onlyOneApplicablePolicyPolicyCombiningAlogrithm(Policy policy[])
{
  Boolean          atLeastOne     = false;
  Policy           selectedPolicy = null;
  ApplicableResult appResult;

  for ( i = 0; i < lengthOf(policy) ; i++ )
  {
     appResult = isApplicable(policy[I]);

     if ( appResult == Indeterminate )
     {
         return Indeterminate;
     }
     if( appResult == Applicable )
     {
         if ( atLeastOne )
         {
             return Indeterminate;
         }
         else
         {
             atLeastOne     = true;
             selectedPolicy = policy[i];
         }
     }
     if ( appResult == NotApplicable )
     {
         continue;
     }
  }
  if ( atLeastOne )
  {
      return evaluate(selectedPolicy);
  }
  else
  {
      return NotApplicable;
  }
}
```

الملحق D

خطة اللغة XACML

1.D خطة السياق XACML

تعرض هذه الفقرة خطة السياق XACML.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified" attributeFormDefault="unqualified">
   <xs:import namespace="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
   schemaLocation="http://docs.oasis-open.org/xacml/access_control-xacml-2.0-policy-
schema-os.xsd"/>
   <!--   -->
   <xs:element name="Request" type="xacml-context:RequestType"/>
   <xs:complexType name="RequestType">
         <xs:sequence>
               <xs:element ref="xacml-context:Subject" maxOccurs="unbounded"/>
               <xs:element ref="xacml-context:Resource" maxOccurs="unbounded"/>
               <xs:element ref="xacml-context:Action"/>
               <xs:element ref="xacml-context:Environment"/>
         </xs:sequence>
   </xs:complexType>
   <!-- -->
   <xs:element name="Response" type="xacml-context:ResponseType"/>
   <xs:complexType name="ResponseType">
         <xs:sequence>
               <xs:element ref="xacml-context:Result" maxOccurs="unbounded"/>
         </xs:sequence>
   </xs:complexType>
   <!-- -->
   <xs:element name="Subject" type="xacml-context:SubjectType"/>
   <xs:complexType name="SubjectType">
         <xs:sequence>
               <xs:element ref="xacml-context:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
         </xs:sequence>
         <xs:attribute name="SubjectCategory" type="xs:anyURI"
         default="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"/>
   </xs:complexType>
   <!-- -->
   <xs:element name="Resource" type="xacml-context:ResourceType"/>
   <xs:complexType name="ResourceType">
         <xs:sequence>
               <xs:element ref="xacml-context:ResourceContent" minOccurs="0"/>
               <xs:element ref="xacml-context:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
         </xs:sequence>
   </xs:complexType>
   <!-- -->
   <xs:element name="ResourceContent" type="xacml-context:ResourceContentType"/>
   <xs:complexType name="ResourceContentType" mixed="true">
         <xs:sequence>
               <xs:any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
         </xs:sequence>
         <xs:anyAttribute namespace="##any" processContents="lax"/>
   </xs:complexType>
   <!-- -->
   <xs:element name="Action" type="xacml-context:ActionType"/>
   <xs:complexType name="ActionType">
         <xs:sequence>
```

```
                <xs:element ref="xacml-context:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
    </xs:complexType>
    <!-- -->
    <xs:element name="Environment" type="xacml-context:EnvironmentType"/>
    <xs:complexType name="EnvironmentType">
          <xs:sequence>
                <xs:element ref="xacml-context:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
    </xs:complexType>
    <!-- -->
    <xs:element name="Attribute" type="xacml-context:AttributeType"/>
    <xs:complexType name="AttributeType">
          <xs:sequence>
                <xs:element ref="xacml-context:AttributeValue"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="AttributeId" type="xs:anyURI" use="required"/>
          <xs:attribute name="DataType" type="xs:anyURI" use="required"/>
          <xs:attribute name="Issuer" type="xs:string" use="optional"/>
    </xs:complexType>
    <!-- -->
    <xs:element name="AttributeValue" type="xacml-context:AttributeValueType"/>
    <xs:complexType name="AttributeValueType" mixed="true">
          <xs:sequence>
                <xs:any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <!-- -->
    <xs:element name="Result" type="xacml-context:ResultType"/>
    <xs:complexType name="ResultType">
          <xs:sequence>
                <xs:element ref="xacml-context:Decision"/>
                <xs:element ref="xacml-context:Status" minOccurs="0"/>
                <xs:element ref="xacml:Obligations" minOccurs="0"/>
          </xs:sequence>
          <xs:attribute name="ResourceId" type="xs:string" use="optional"/>
    </xs:complexType>
    <!-- -->
    <xs:element name="Decision" type="xacml-context:DecisionType"/>
    <xs:simpleType name="DecisionType">
          <xs:restriction base="xs:string">
                <xs:enumeration value="Permit"/>
                <xs:enumeration value="Deny"/>
                <xs:enumeration value="Indeterminate"/>
                <xs:enumeration value="NotApplicable"/>
          </xs:restriction>
    </xs:simpleType>
    <!-- -->
    <xs:element name="Status" type="xacml-context:StatusType"/>
    <xs:complexType name="StatusType">
          <xs:sequence>
                <xs:element ref="xacml-context:StatusCode"/>
                <xs:element ref="xacml-context:StatusMessage" minOccurs="0"/>
                <xs:element ref="xacml-context:StatusDetail" minOccurs="0"/>
          </xs:sequence>
    </xs:complexType>
    <!-- -->
    <xs:element name="StatusCode" type="xacml-context:StatusCodeType"/>
    <xs:complexType name="StatusCodeType">
          <xs:sequence>
                <xs:element ref="xacml-context:StatusCode" minOccurs="0"/>
          </xs:sequence>
          <xs:attribute name="Value" type="xs:anyURI" use="required"/>
    </xs:complexType>
    <!-- -->
    <xs:element name="StatusMessage" type="xs:string"/>
    <!-- -->
```

```
   <xs:element name="StatusDetail" type="xacml-context:StatusDetailType"/>
   <xs:complexType name="StatusDetailType">
          <xs:sequence>
                 <xs:any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
   </xs:complexType>
   <!-- -->
   <xs:element name="MissingAttributeDetail" type="xacml-
context:MissingAttributeDetailType"/>
   <xs:complexType name="MissingAttributeDetailType">
          <xs:sequence>
                 <xs:element ref="xacml-context:AttributeValue" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="AttributeId" type="xs:anyURI" use="required"/>
          <xs:attribute name="DataType" type="xs:anyURI" use="required"/>
          <xs:attribute name="Issuer" type="xs:string" use="optional"/>
   </xs:complexType>
   <!-- -->
</xs:schema>
```

2.D خطة السياسة

تعرض هذه الفقرة خطة السياسة XACML.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
elementFormDefault="qualified" attributeFormDefault="unqualified">
   <!-- -->
   <xs:element name="PolicySet" type="xacml:PolicySetType"/>
   <xs:complexType name="PolicySetType">
          <xs:sequence>
                 <xs:element ref="xacml:Description" minOccurs="0"/>
                 <xs:element ref="xacml:PolicySetDefaults" minOccurs="0"/>
                 <xs:element ref="xacml:Target"/>
                 <xs:choice minOccurs="0" maxOccurs="unbounded">
                        <xs:element ref="xacml:PolicySet"/>
                        <xs:element ref="xacml:Policy"/>
                        <xs:element ref="xacml:PolicySetIdReference"/>
                        <xs:element ref="xacml:PolicyIdReference"/>
                        <xs:element ref="xacml:CombinerParameters"/>
                        <xs:element ref="xacml:PolicyCombinerParameters"/>
                        <xs:element ref="xacml:PolicySetCombinerParameters"/>
                 </xs:choice>
                 <xs:element ref="xacml:Obligations" minOccurs="0"/>
          </xs:sequence>
          <xs:attribute name="PolicySetId" type="xs:anyURI" use="required"/>
          <xs:attribute name="Version" type="xacml:VersionType" default="1.0"/>
          <xs:attribute name="PolicyCombiningAlgId" type="xs:anyURI" use="required"/>
   </xs:complexType>
   <!-- -->
   <xs:element name="CombinerParameters" type="xacml:CombinerParametersType"/>
   <xs:complexType name="CombinerParametersType">
          <xs:sequence>
                 <xs:element ref="xacml:CombinerParameter" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
   </xs:complexType>
   <!-- -->
   <xs:element name="CombinerParameter" type="xacml:CombinerParameterType"/>
   <xs:complexType name="CombinerParameterType">
          <xs:sequence>
                 <xs:element ref="xacml:AttributeValue"/>
          </xs:sequence>
          <xs:attribute name="ParameterName" type="xs:string" use="required"/>
   </xs:complexType>
   <!-- -->
```

```
   <xs:element name="RuleCombinerParameters"
type="xacml:RuleCombinerParametersType"/>
   <xs:complexType name="RuleCombinerParametersType">
          <xs:complexContent>
                 <xs:extension base="xacml:CombinerParametersType">
                        <xs:attribute name="RuleIdRef" type="xs:string"
use="required"/>
                 </xs:extension>
          </xs:complexContent>
   </xs:complexType>
   <!-- -->
   <xs:element name="PolicyCombinerParameters"
type="xacml:PolicyCombinerParametersType"/>
   <xs:complexType name="PolicyCombinerParametersType">
          <xs:complexContent>
                 <xs:extension base="xacml:CombinerParametersType">
                        <xs:attribute name="PolicyIdRef" type="xs:anyURI"
use="required"/>
                 </xs:extension>
          </xs:complexContent>
   </xs:complexType>
   <!-- -->
   <xs:element name="PolicySetCombinerParameters"
type="xacml:PolicySetCombinerParametersType"/>
   <xs:complexType name="PolicySetCombinerParametersType">
          <xs:complexContent>
                 <xs:extension base="xacml:CombinerParametersType">
                        <xs:attribute name="PolicySetIdRef" type="xs:anyURI"
use="required"/>
                 </xs:extension>
          </xs:complexContent>
   </xs:complexType>
   <!-- -->
   <xs:element name="PolicySetIdReference" type="xacml:IdReferenceType"/>
   <xs:element name="PolicyIdReference" type="xacml:IdReferenceType"/>
   <!-- -->
   <xs:element name="PolicySetDefaults" type="xacml:DefaultsType"/>
   <xs:element name="PolicyDefaults" type="xacml:DefaultsType"/>
   <xs:complexType name="DefaultsType">
          <xs:sequence>
                 <xs:choice>
                        <xs:element ref="xacml:XPathVersion"/>
                 </xs:choice>
          </xs:sequence>
   </xs:complexType>
   <!-- -->
   <xs:element name="XPathVersion" type="xs:anyURI"/>
   <!-- -->
   <xs:complexType name="IdReferenceType">
          <xs:simpleContent>
                 <xs:extension base="xs:anyURI">
                        <xs:attribute name="Version" type="xacml:VersionMatchType"
use="optional"/>
                        <xs:attribute name="EarliestVersion"
type="xacml:VersionMatchType" use="optional"/>
                        <xs:attribute name="LatestVersion"
type="xacml:VersionMatchType" use="optional"/>
                 </xs:extension>
          </xs:simpleContent>
   </xs:complexType>
   <!-- -->
   <xs:simpleType name="VersionType">
          <xs:restriction base="xs:string">
                 <xs:pattern value="(\d+\.)*\d+"/>
          </xs:restriction>
   </xs:simpleType>
   <!-- -->
   <xs:simpleType name="VersionMatchType">
          <xs:restriction base="xs:string">
                 <xs:pattern value="((\d+|\*)\.)*(\d+|\*|\+)"/>
          </xs:restriction>
   </xs:simpleType>
```

```
<!-- -->
<xs:element name="Policy" type="xacml:PolicyType"/>
<xs:complexType name="PolicyType">
       <xs:sequence>
              <xs:element ref="xacml:Description" minOccurs="0"/>
              <xs:element ref="xacml:PolicyDefaults" minOccurs="0"/>
              <xs:element ref="xacml:CombinerParameters" minOccurs="0"/>
              <xs:element ref="xacml:Target"/>
              <xs:choice maxOccurs="unbounded">
                     <xs:element ref="xacml:CombinerParameters" minOccurs="0"/>
                     <xs:element ref="xacml:RuleCombinerParameters" minOccurs="0"/>
                     <xs:element ref="xacml:VariableDefinition"/>
                     <xs:element ref="xacml:Rule"/>
              </xs:choice>
              <xs:element ref="xacml:Obligations" minOccurs="0"/>
       </xs:sequence>
       <xs:attribute name="PolicyId" type="xs:anyURI" use="required"/>
       <xs:attribute name="Version" type="xacml:VersionType" default="1.0"/>
       <xs:attribute name="RuleCombiningAlgId" type="xs:anyURI" use="required"/>
</xs:complexType>
<!-- -->
<xs:element name="Description" type="xs:string"/>
<!-- -->
<xs:element name="Rule" type="xacml:RuleType"/>
<xs:complexType name="RuleType">
       <xs:sequence>
              <xs:element ref="xacml:Description" minOccurs="0"/>
              <xs:element ref="xacml:Target" minOccurs="0"/>
              <xs:element ref="xacml:Condition" minOccurs="0"/>
       </xs:sequence>
       <xs:attribute name="RuleId" type="xs:string" use="required"/>
       <xs:attribute name="Effect" type="xacml:EffectType" use="required"/>
</xs:complexType>
<!-- -->
<xs:simpleType name="EffectType">
       <xs:restriction base="xs:string">
              <xs:enumeration value="Permit"/>
              <xs:enumeration value="Deny"/>
       </xs:restriction>
</xs:simpleType>
<!-- -->
<xs:element name="Target" type="xacml:TargetType"/>
<xs:complexType name="TargetType">
       <xs:sequence>
              <xs:element ref="xacml:Subjects" minOccurs="0"/>
              <xs:element ref="xacml:Resources" minOccurs="0"/>
              <xs:element ref="xacml:Actions" minOccurs="0"/>
              <xs:element ref="xacml:Environments" minOccurs="0"/>
       </xs:sequence>
</xs:complexType>
<!-- -->
<xs:element name="Subjects" type="xacml:SubjectsType"/>
<xs:complexType name="SubjectsType">
       <xs:sequence>
              <xs:element ref="xacml:Subject" maxOccurs="unbounded"/>
       </xs:sequence>
</xs:complexType>
<!-- -->
<xs:element name="Subject" type="xacml:SubjectType"/>
<xs:complexType name="SubjectType">
       <xs:sequence>
              <xs:element ref="xacml:SubjectMatch" maxOccurs="unbounded"/>
       </xs:sequence>
</xs:complexType>
<!-- -->
<xs:element name="Resources" type="xacml:ResourcesType"/>
<xs:complexType name="ResourcesType">
       <xs:sequence>
              <xs:element ref="xacml:Resource" maxOccurs="unbounded"/>
       </xs:sequence>
</xs:complexType>
<!-- -->
```

```
<xs:element name="Resource" type="xacml:ResourceType"/>
<xs:complexType name="ResourceType">
       <xs:sequence>
              <xs:element ref="xacml:ResourceMatch" maxOccurs="unbounded"/>
       </xs:sequence>
</xs:complexType>
<!-- -->
<xs:element name="Actions" type="xacml:ActionsType"/>
<xs:complexType name="ActionsType">
       <xs:sequence>
              <xs:element ref="xacml:Action" maxOccurs="unbounded"/>
       </xs:sequence>
</xs:complexType>
<!-- -->
<xs:element name="Action" type="xacml:ActionType"/>
<xs:complexType name="ActionType">
       <xs:sequence>
              <xs:element ref="xacml:ActionMatch" maxOccurs="unbounded"/>
       </xs:sequence>
</xs:complexType>
<!-- -->
<xs:element name="Environments" type="xacml:EnvironmentsType"/>
<xs:complexType name="EnvironmentsType">
       <xs:sequence>
              <xs:element ref="xacml:Environment" maxOccurs="unbounded"/>
       </xs:sequence>
</xs:complexType>
<!-- -->
<xs:element name="Environment" type="xacml:EnvironmentType"/>
<xs:complexType name="EnvironmentType">
       <xs:sequence>
              <xs:element ref="xacml:EnvironmentMatch" maxOccurs="unbounded"/>
       </xs:sequence>
</xs:complexType>
<!-- -->
<xs:element name="SubjectMatch" type="xacml:SubjectMatchType"/>
<xs:complexType name="SubjectMatchType">
       <xs:sequence>
              <xs:element ref="xacml:AttributeValue"/>
              <xs:choice>
                     <xs:element ref="xacml:SubjectAttributeDesignator"/>
                     <xs:element ref="xacml:AttributeSelector"/>
              </xs:choice>
       </xs:sequence>
       <xs:attribute name="MatchId" type="xs:anyURI" use="required"/>
</xs:complexType>
<!-- -->
<xs:element name="ResourceMatch" type="xacml:ResourceMatchType"/>
<xs:complexType name="ResourceMatchType">
       <xs:sequence>
              <xs:element ref="xacml:AttributeValue"/>
              <xs:choice>
                     <xs:element ref="xacml:ResourceAttributeDesignator"/>
                     <xs:element ref="xacml:AttributeSelector"/>
              </xs:choice>
       </xs:sequence>
       <xs:attribute name="MatchId" type="xs:anyURI" use="required"/>
</xs:complexType>
<!-- -->
<xs:element name="ActionMatch" type="xacml:ActionMatchType"/>
<xs:complexType name="ActionMatchType">
       <xs:sequence>
              <xs:element ref="xacml:AttributeValue"/>
              <xs:choice>
                     <xs:element ref="xacml:ActionAttributeDesignator"/>
                     <xs:element ref="xacml:AttributeSelector"/>
              </xs:choice>
       </xs:sequence>
       <xs:attribute name="MatchId" type="xs:anyURI" use="required"/>
</xs:complexType>
<!-- -->
<xs:element name="EnvironmentMatch" type="xacml:EnvironmentMatchType"/>
```

```
   <xs:complexType name="EnvironmentMatchType">
          <xs:sequence>
                 <xs:element ref="xacml:AttributeValue"/>
                 <xs:choice>
                        <xs:element ref="xacml:EnvironmentAttributeDesignator"/>
                        <xs:element ref="xacml:AttributeSelector"/>
                 </xs:choice>
          </xs:sequence>
          <xs:attribute name="MatchId" type="xs:anyURI" use="required"/>
   </xs:complexType>
   <!-- -->
   <xs:element name="VariableDefinition" type="xacml:VariableDefinitionType"/>
   <xs:complexType name="VariableDefinitionType">
          <xs:sequence>
                 <xs:element ref="xacml:Expression"/>
          </xs:sequence>
          <xs:attribute name="VariableId" type="xs:string" use="required"/>
   </xs:complexType>
   <!-- -->
   <xs:element name="Expression" type="xacml:ExpressionType" abstract="true"/>
   <xs:complexType name="ExpressionType" abstract="true"/>
   <!-- -->
   <xs:element name="VariableReference"
   type="xacml:VariableReferenceType" substitutionGroup="xacml:Expression"/>
   <xs:complexType name="VariableReferenceType">
          <xs:complexContent>
                 <xs:extension base="xacml:ExpressionType">
                        <xs:attribute name="VariableId" type="xs:string"
use="required"/>
                 </xs:extension>
          </xs:complexContent>
   </xs:complexType>
   <!-- -->
   <xs:element name="AttributeSelector"
   type="xacml:AttributeSelectorType" substitutionGroup="xacml:Expression"/>
   <xs:complexType name="AttributeSelectorType">
          <xs:complexContent>
                 <xs:extension base="xacml:ExpressionType">
                        <xs:attribute name="RequestContextPath" type="xs:string"
use="required"/>
                        <xs:attribute name="DataType" type="xs:anyURI"
use="required"/>
                        <xs:attribute name="MustBePresent" type="xs:boolean"
use="optional" default="false"/>
                 </xs:extension>
          </xs:complexContent>
   </xs:complexType>
   <!-- -->
   <xs:element name="ResourceAttributeDesignator"
   type="xacml:AttributeDesignatorType" substitutionGroup="xacml:Expression"/>
   <xs:element name="ActionAttributeDesignator"
   type="xacml:AttributeDesignatorType" substitutionGroup="xacml:Expression"/>
   <xs:element name="EnvironmentAttributeDesignator"
   type="xacml:AttributeDesignatorType" substitutionGroup="xacml:Expression"/>
   <!-- -->
   <xs:complexType name="AttributeDesignatorType">
          <xs:complexContent>
                 <xs:extension base="xacml:ExpressionType">
                        <xs:attribute name="AttributeId" type="xs:anyURI"
use="required"/>
                        <xs:attribute name="DataType" type="xs:anyURI"
use="required"/>
                        <xs:attribute name="Issuer" type="xs:string" use="optional"/>
                        <xs:attribute name="MustBePresent" type="xs:boolean"
use="optional" default="false"/>
                 </xs:extension>
          </xs:complexContent>
   </xs:complexType>
   <!-- -->
   <xs:element name="SubjectAttributeDesignator"
   type="xacml:SubjectAttributeDesignatorType" substitutionGroup="xacml:Expression"/>
   <xs:complexType name="SubjectAttributeDesignatorType">
```

```
          <xs:complexContent>
                <xs:extension base="xacml:AttributeDesignatorType">
                      <xs:attribute name="SubjectCategory" type="xs:anyURI"
                      use="optional" default="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject"/>
                </xs:extension>
          </xs:complexContent>
    </xs:complexType>
    <!-- -->
    <xs:element name="AttributeValue" type="xacml:AttributeValueType"
          substitutionGroup="xacml:Expression"/>
    <xs:complexType name="AttributeValueType" mixed="true">
          <xs:complexContent mixed="true">
                <xs:extension base="xacml:ExpressionType">
                      <xs:sequence>
                            <xs:any namespace="##any" processContents="lax"
minOccurs="0"
                                  maxOccurs="unbounded"/>
                      </xs:sequence>
                      <xs:attribute name="DataType" type="xs:anyURI"
use="required"/>
                      <xs:anyAttribute namespace="##any" processContents="lax"/>
                </xs:extension>
          </xs:complexContent>
    </xs:complexType>
    <!-- -->
    <xs:element name="Function" type="xacml:FunctionType"
substitutionGroup="xacml:Expression"/>
    <xs:complexType name="FunctionType">
          <xs:complexContent>
                <xs:extension base="xacml:ExpressionType">
                      <xs:attribute name="FunctionId" type="xs:anyURI"
use="required"/>
                </xs:extension>
          </xs:complexContent>
    </xs:complexType>
    <!-- -->
    <xs:element name="Condition" type="xacml:ConditionType"/>
    <xs:complexType name="ConditionType">
          <xs:sequence>
                <xs:element ref="xacml:Expression"/>
          </xs:sequence>
    </xs:complexType>
    <!-- -->
    <xs:element name="Apply" type="xacml:ApplyType"
substitutionGroup="xacml:Expression"/>
    <xs:complexType name="ApplyType">
          <xs:complexContent>
                <xs:extension base="xacml:ExpressionType">
                      <xs:sequence>
                            <xs:element ref="xacml:Expression" minOccurs="0"
maxOccurs="unbounded"/>
                      </xs:sequence>
                      <xs:attribute name="FunctionId" type="xs:anyURI"
use="required"/>
                </xs:extension>
          </xs:complexContent>
    </xs:complexType>
    <!-- -->
    <xs:element name="Obligations" type="xacml:ObligationsType"/>
    <xs:complexType name="ObligationsType">
          <xs:sequence>
                <xs:element ref="xacml:Obligation" maxOccurs="unbounded"/>
          </xs:sequence>
    </xs:complexType>
    <!-- -->
    <xs:element name="Obligation" type="xacml:ObligationType"/>
    <xs:complexType name="ObligationType">
          <xs:sequence>
                <xs:element ref="xacml:AttributeAssignment" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
```

```
          <xs:attribute name="ObligationId" type="xs:anyURI" use="required"/>
          <xs:attribute name="FulfillOn" type="xacml:EffectType" use="required"/>
   </xs:complexType>
   <!-- -->
   <xs:element name="AttributeAssignment" type="xacml:AttributeAssignmentType"/>
   <xs:complexType name="AttributeAssignmentType" mixed="true">
          <xs:complexContent mixed="true">
                <xs:extension base="xacml:AttributeValueType">
                      <xs:attribute name="AttributeId" type="xs:anyURI"
use="required"/>
                </xs:extension>
          </xs:complexContent>
   </xs:complexType>
   <!-- -->
</xs:schema>
```

3.D خطة البروتوكول XACML SAML

تعرض هذه الفقرة خطة البروتوكول XACML SAML.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema
    targetNamespace="urn:oasis:xacml:2.0:saml:protocol:schema:os"
    xmlns:xs="http://www.23.org/2001/XMLSchema"
    xmlns="http://www.w3.org/2001/XMLSchema"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
    xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
      schemaLocation="http://www.oasis-
open.org/committees/tc_home.php?wg_abbrev=security"/>
  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:protocol"
      schemaLocation="http://www.oasis-
open.org/committees/tc_home.php?wg_abbrev=security"/>
  <xs:import namespace="urn:oasis:names:tc:xacml:2.0:context:schema:os"
      schemaLocation="http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-
context-schema-os.xsd"/>
  <xs:import namespace="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
      schemaLocation="http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-
policy-schema-os.xsd"/>
  <xs:annotation>
    <xs:documentation>
        Document identifier: access_control-xacml-2.0-saml-protocol-schema-os.xsd
        Location: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-saml-
protocol-schema-os.xsd
    </xs:documentation>
  </xs:annotation>
  <!--    -->
  <xs:element name="XACMLAuthzDecisionQuery"
           type="XACMLAuthzDecisionQueryType"/>
  <xs:complexType name="XACMLAuthzDecisionQueryType">
    <xs:complexContent>
      <xs:extension base="samlp:RequestAbstractType">
        <xs:sequence>
          <xs:element ref="xacml-context:Request"/>
        </xs:sequence>
        <xs:attribute name="InputContextOnly"
                      type="boolean"
                      use="optional"
                      default="false"/>
        <xs:attribute name="ReturnContext"
                      type="boolean"
                      use="optional"
                      default="false"/>
      </xs:extension>
    </xs:complexContent>
```

```
  </xs:complexType>
  <!--    -->
  <xs:element name="XACMLPolicyQuery"
           type="XACMLPolicyQueryType"/>
  <xs:complexType name="XACMLPolicyQueryType">
    <xs:complexContent>
      <xs:extension base="samlp:RequestAbstractType">
        <xs:choice minOccurs="0" maxOccurs="unbounded">>
          <xs:element ref="xacml-context:Request"/>
          <xs:element ref="xacml:Target"/>
          <xs:element ref="xacml:PolicySetIdReference"/>
          <xs:element ref="xacml:PolicyIdReference"/>
        </xs:choice>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
</schema>
```

4.D خطة الزعم XACML SAML

تعرض هذه الفقرة خطة الزعم XACML SAML.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema
    targetNamespace="urn:oasis:xacml:2.0:saml:assertion:schema:os"
    xmlns="http://www.w3.org/2001/XMLSchema"
    xmlns:xs="http://www.23.org/2001/XMLSchema"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
    xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
      schemaLocation="http://www.oasis-
open.org/committees/tc_home.php?wg_abbrev=security"/>
  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:protocol"
      schemaLocation="http://www.oasis-
open.org/committees/tc_home.php?wg_abbrev=security"/>
  <xs:import namespace="urn:oasis:names:tc:xacml:2.0:context:schema:os"
      schemaLocation="http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-
context-schema-os.xsd"/>
  <xs:import namespace="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
      schemaLocation="http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-
policy-schema-os.xsd"/>
  <xs:annotation>
    <xs:documentation>
       Document identifier: access_control-xacml-2.0-saml-assertion-schema-cd-02.xsd
       Location: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-saml-
assertion-schema-cd-os.xsd
    </xs:documentation>
  </xs:annotation>
  <!--    -->
  <xs:element name="XACMLAuthzDecisionStatement"
           type="XACMLAuthzDecisionStatementType"/>
  <xs:complexType name="XACMLAuthzDecisionStatementType">
    <xs:complexContent>
      <xs:extension base="samlp:StatementAbstractType">
        <xs:sequence>
          <xs:element ref="xacml-context:Response"/>
          <xs:element ref="xacml-context:Request"  MinOccurs="0"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
  <!--    -->
  <xs:element name="XACMLPolicyStatement"
           type="XACMLPolicyStatementType"/>
  <xs:complexType name="XACMLPolicyStatementType">
```

```
    <xs:complexContent>
      <xs:extension base="samlp:StatementAbstractType">
        <xs:choice minOccurs="0" maxOccurs="unbounded">>
          <xs:element ref="xacml:Policy"/>
          <xs:element ref="xacml:PolicySet"/>
        </xs:choice>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
</schema>
```

التذييل I

الاعتبارات الأمنية

يحدد هذا التذييل السيناريوهات التوفيقية الممكنة للأمن والسرية والتي ينبغي أخذها بعين الاعتبار لدى تطبيق النظام القائم على اللغة XACML. وتقع على عاتق المنفذ مسؤولية تحديد درجة عملية هذه السيناريوهات التوفيقية في بيئتها واختيار الحراسة الملائمة لها.

1.I نموذج التهديد

نفترض هنا أن المهاجم قادر على النفاذ إلى قناة الاتصالات بين مستعملي النظام XACML وعلى تفسير الرسائل أو أجزاء الرسائل وإدراجها وحذفها وتغييرها.

وعلاوة على ذلك قد يستخدم مستعمل ما بدافع الإيذاء معلومات من رسالة سابقة في تعاملات لاحقة. ويفترض أيضاً أن القواعد والسياسات موثوقة بنفس درجة موثوقية من يضعها ويستخدمها. ولذا لا بد من أن يبني كل مستعمل الثقة الملائمة للجهات المستعملة الأخرى التي يتصل بها. والآليات المتعلقة ببناء الثقة لا تدخل ضمن نطاق هذه التوصية.

والرسائل التي تتناولها الجهات المستعملة في النموذج XACML معرضة للهجمات من قبل أطراف خارجية مسيئة. وتتمثل العوامل الحساسة الأخرى في النقاط PEP وPDP وPAP. ونظراً إلى أن بعض هذه الكيانات لا تقع تماماً ضمن نطاق هذه التوصية فقد يؤدي تعريضها للخطر إلى تعريض التحكم في النفاذ الذي توفره النقطة PEP.

ويجدر بالذكر احتمال تعريض مكونات أخرى من الأنظمة مثل نظام التشغيل ونظام أسماء المجال (DNS) التي لا تدخل في إطار دراسة نماذج الهجوم هذه. وقد ينجم عن تعريض هذه المكونات للخطر انتهاكاً للسياسة.

وتقدم الفقرات التالية سيناريوهات توفيقية محددة ومفصلة تتعلق بالنظام XACML.

1.1.I الإفشاء غير المسموح

لا يحدد النظام XACML أي آليات ملازمة من أجل حماية سرية الرسائل المتبادلة بين الجهات المستعملة للنظام. لذا بمقدور طرف عدائي مراقبة الرسائل لدى عبورها. وتعتبر بعض سياسات الأمن أن إفشاء المعلومات الواردة في هذه الرسائل انتهاكاً. وقد يشكل البوح بنعوت طلبات القرار أو بأنماطها التي تقدمها جهة مستعملة خرقاً لسياسة السرية. وتتراوح النتائج المترتبة على إفشاء معطيات شخصية غير مسموح في القطاع التجاري بين تسبيب الإزعاج للجهة الحارسة وعقوبة السجن وقد تسفر عن غرامات مالية كبيرة في حال المعطيات الطبية أو المالية.

وتعالج مسألة الإفشاء غير المسموح من خلال الحفاظ على السرية.

2.1.I تكرار الرسالة

هجوم تكرار الرسالة هو هجوم يقوم فيه بتسجيل وتكرار رسائل نظامية بين مستعملي النظام XACML. وقد يؤدي هذا الهجوم إلى رفض الخدمة أو استخدام معلومات باطلة أو انتحال شخصية.

وتستدعي الوقاية من هجمات التكرار الحفاظ على الرسائل طازجة.

ويلاحظ أن تجفير الرسالة لا يساهم في منع هجوم التكرار إذ إن جهة الهجوم لا تحتاج إلى فهم الرسالة بل تكرارها فقط.

3.1.I إدراج الرسائل

هجوم إدراج الرسائل هو هجوم يدرج فيه المهاجم رسائل دخيلة في تتابع رسائل تتبادلها أطراف تستعمل النظام XACML.

ويكمن التصدي لهجوم إدراج الرسائل في استعمال حماية الاستيقان المتبادل وتكاملية تتابعات الرسائل المتبادلة بين المستعملين. ويجدر بالملاحظة أن استعمال الاستيقان المتبادل SSL بمفرده ليس كافياً، بل هو مجرد إثبات على أن الطرف الآخر هو نفس الطرف الذي يحدده موضوع الشهادة X.509. ولا بد حرصاً على الفعالية من التأكيد على أن موضوع الشهادة حاصل على رخصة إرسال الرسالة.

4.1.I حذف الرسائل

هجوم حذف الرسائل هجوم يحذف فيه المهاجم رسائل من تتابع الرسائل المتبادلة بين الأطراف المستعملة للنظام XACML. وقد يفضي حذف الرسائل إلى رفض الخدمة. غير أن نظاماً XACML حسن التصميم ينبغي ألاّ يصدر قرار ترخيص خاطئ إثر هجوم حذف رسائل.

ويكمن التصدي لهجوم حذف الرسائل في استعمال حماية تكاملية لتتابعات الرسائل المتبادلة بين الأطراف المستعملة.

5.1.I تعديل الرسالة

إذا كان طرف مهاجم قادر على اختراق رسالة وتغيير محتوياتها فإنه يكون قادراً أيضاً على تغيير قرار الترخيص. وبإمكانه حماية تكاملية الرسالة أن تمنع هجوماً لتغيير الرسالة بنجاح.

6.1.I نتائج غير قابلة للتطبيق (NotApplicable)

تعني النتيجة "NotApplicable" عدم قدرة النقطة PDP على تحديد سياسة يتواءم هدفها مع المعلومات الواردة في طلب القرار. وعموماً يوصى بشدة استعمال سياسة الرد "بالرفض" وبهذا تعيد النقطة PDP بدلاً من "غير قابل للتطبيق" النتيجة "مرفوض".

غير أن بعض نماذج الأمن مثل تلك المتداولة في الكثير من خدمات الويب، يكافئ قرار ترخيص "غير قابل للتطبيق" نتيجة "مسموح". وثمة إجراءات أمنية خاصة يجب مراعاتها لضمان أمن هذه العملية. الأمر الذي تشرحه الفقرات التالية.

وإذا تم تفسير "غير قابل للتطبيق" على أنه "مسموح" فمن الضروري أن تتوافق خوارزميات التواؤم التي تستخدمها السياسة في تقابل العناصر في طلب القرار توافقاً وثيقاً مع قواعد تركيب المعطيات التي تستخدمها التطبيقات التي ستقدم طلب القرار. ويسفر خلل التواؤم عن النتيجة "غير قابل للتطبيق" ويعالج على أنه "مسموح". وبذلك قد يفضي خلل غير مقصود إلى نفاذ غير مقصود.

وتوفر أجهزة الإجابة http التجارية معالجة أنواع كثيرة من قواعد التركيب بطريقة مكافئة. ويمكن استعمال "%" لتمثيل السمات بالقيمة الست عشرية. ويقدم المسار URL "../../" عدة طرق لتحديد نفس القيمة. وقد يسمح بعدة مجموعات من السمات، وفي بعض الحالات يمكن تمثيل نفس السمة المطبوعة من خلال قيم اثنينية مختلفة. وقد يتم السماح بنفاذ عن غير قصد إذا لم تكن خوارزمية التواؤم التي تستخدمها السياسة متطورة بالقدر الكافي الذي يسمح لها بتمييز هذه التغيرات.

ومن غير الأمين تفسير "غير قابل للتطبيق" "بمسموح" إلا في بيئة مغلقة حيث تتمكن جميع التطبيقات التي تصيغ طلب القرار من الحصول على ضمانات في استعمال القواعد الصحية التي تتوقعها السياسات. أما في بيئة أكثر انفتاحاً حيث تأتي طلبات القرارات من تطبيقات تستعمل أي قاعدة تركيب نظامية، فإنه يوصى بشدة أن لا تعتبر قيمة "غير قابل للتطبيق" كقيمة "مسموح" إلاّ إذا كانت قواعد التواؤم مصممة بحرص شديد لكي توائم جميع المدخلات المطبقة الممكنة بغض النظر عن تغييرات قاعدة تركيبها أو نمطها. ويجب أن ترفض النقطة PEP النفاذ إلاّ في حال استلامها لقرار الترخيص الصريح "مسموح".

7.1.I قواعد سلبية

القاعدة السلبية قاعدة تستند إلى عبارة غير "صحيحة". وقد تؤدي القواعد السلبية في حال استعمالها دون الحيطة اللازمة، إلى انتهاك السياسة، لذا فإن بعض السلطات توصي بعدم استعمالها. غير أنها قد تكون بالغة الأهمية في بعض الحالات مما دعا النظام XACML إلى اختيار إدراجها. وعلى الرغم من ذلك يوصى بالتزام الحيطة لدى استعمالها وبتجنبها إن أمكن.

ومن الاستعمالات الشائعة للقواعد السلبية رفض النفاذ إلى فرد أو مجموعة فرعية ما، بينما يسمح لأعضاء آخرين من المجموعة بهذا النفاذ. فقد نريد مثلاً وضع قاعدة تتيح لجميع نواب الرؤساء أن يطلعوا على البيانات المالية غير المنشورة باستثناء "جو" وهو مجرد نائب رئيس فخري ولا يتحلى بالسرية اللازمة في اتصالاته. وإذا كنا نمتلك كامل التحكم في إدارة نعوت الجهة المستعملة فالطريقة المثلى تكون بتحديد "نائب رئيس" و"نائب رئيس فخري" كمجموعتين مختلفتين ثم تحديد القواعد وفقاً لذلك. غير أن هذه الطريقة تتعذر في بعض البيئات. (يجدر بالملاحظة في هذا الصدد أن الإحالة إلى حالات إفرادية في القواعد غير مستصوبة ويفضل عادة التعامل مع نعوت مشتركة).

وقد تؤدي القواعد السلبية إذا أسيء استخدامها إلى الضرر بالسياسة في حالتين منتشرتين هما: حذف النعوت وتغيير المجموعة الأساسية. ففي حالة حذف النعوت يمكن إعطاء مثال حالة السياسة بنفاذ مسموح شريطة ألا تكون الجهة المستعملة في حالة إفلاس. وإذا لسبب ما كان احتمال عدم كشف النقطة PDP لنعت حالة الإفلاس فسينتج عن ذلك عندئذٍ نفاذ غير مسموح. وقد تكون الجهة المستعملة في بعض البيئات قادرة على حذف ظهور النعوت باستخدام أوامر التحكم في السرية أو قد يكون المخدم أو المستودع الذي يشتمل على المعلومات غير متيسر لأسباب طارئة أو مقصودة.

أما في حالة تغيير المجموعة الأساسية فيمكن إعطاء مثال حالة سياسة يستطيع بموجبها كل عامل في الدائرة الهندسية ما عدا السكرتيرات تغيير شفرة مصدر البرمجية. ولنفترض أنه ينبغي دمج تلك الدائرة مع دائرة هندسية أخرى مع الإبقاء على نفس السياسة. لكن الدائرة الجديدة تضم أيضاً أفراداً عاملين كمساعدين إداريين ينبغي معاملتهم معاملة السكرتيرات. وإذا لم تتغير السياسة سيسمح من غير قصد لهؤلاء العاملين بتغيير شفرة مصدر البرمجيات. ويسهل تجنب مشاكل من هذا النوع في حال إدارة فرد واحد لجميع السياسات، أما عندما تكون الإدارة موزعة كما هي الحال في النظام XACML فيجب التحذير صراحة من الحالات من هذا القبيل.

2.I أسباب الوقاية

1.2.I الاستيقان

يوفر الاستيقان لأحد طرفي المعاملة السبل الكفيلة بتحديد هوية الطرف الآخر في هذه المعاملة. ويمكن للاستيقان أن يكون من جانب واحد أو ثنائي الأطراف.

ونظراً إلى الطبيعة الحساسة لأنظمة التحكم في النفاذ من الهام أن تستيقن النقطة PEP هوية النقطة PDP التي ترسل لها طلبات القرار. وإلاّ فإن احتمال إدراج مهاجم ما لقرارات ترخيص مزورة أو غير صالحة قائم مما يؤدي إلى انتهاك السياسة.

كما أنه من الهام أيضاً بالنسبة للنقطة PDP أن تستيقن هوية النقطة PEP وتتأكد من سوية الموثوقية التي تحدد مرور المعطيات الحساسة إن وجدت. وينبغي عدم نسيان أن إجابات بسيطة مثل "مسموح" أو "مرفوض" قد يستغلها مهاجم إذا سمح له أن يطرح طلبات دون قيود على النقطة PDP.

ويمكن استخدام تقنيات أخرى من أجل توفير الاستيقان مثل شفرة موقع مشترك أو شبكة خاصة أو شبكة خاصة تقديرية (VPN) أو تواقيع رقمية. ويجوز أيضاً إجراء الاستيقان كجزء من بروتوكول الاتصالات المستخدم في تبادل السياق. ويجري الاستيقان في هذه الحالة إما على مستوى الرسالة وإما على مستوى الجلسة.

2.2.I إدارة السياسة

إذا قدمت محتويات السياسات خارج إطار نظام التحكم في النفاذ، قد تستخدم بعض الجهات المستعملة هذه المعلومات في تحديد كيفية الحصول على نفاذ غير مرخص له.

ومنعاً لهذا الهجوم يجوز لنفس مستودع المستخدم في تخزين السياسات أن يشترط تحكماً بالنفاذ. وعلاوة على ذلك، لا ينبغي استعمال العنصر <Status> لإعادة قيم النعوت المفقودة إلاّ عندما لا يعرِّض عرض هويات هذه النعوت الأمن للخطر.

3.2.I السرية

تتضمن آليات السرية منع إمكانية قراءة محتويات رسالة ما إلا من قبل جهات مرغوب بها وليس من قبل أي عابر سبيل يصادفها. وينبغي مراعاة السرية في حالتين اثنتين، الأولى أثناء الإرسال والأخرى داخل العنصر <Policy>.

1.3.2.I سرية الاتصال

من المستحسن في بعض البيئات معاملة جميع المعطيات الواردة في نظام تحكم بالنفاذ على أنها سرية. ويجوز في بيئات أخرى ترك السياسات مفتوحة للتوزيع والبحث والتدقيق. والغرض من إبقاء معلومات السياسة سرية هو تصعيب مهمة المهاجم في معرفة الخطوات التي تمكنه من الحصول على نفاذ غير مسموح. وبغض النظر عند النهج المعتمد ينبغي عدم ربط أمن نظام التحكم في النفاذ بسرية السياسة.

ولا تدخل أي اعتبارات أمنية تتعلق بإرسال العناصر <Policy> XACML وتبادلها ضمن نطاق المعيار XACML. وبما أنه غالباً ما يكون من المهم ضمان تكاملية العناصر <Policy> وسريتها لدى تبادلها بين طرفين، يترك للمنفذين أمر تحديد الآليات المناسبة للبيئة التي يعملون معها.

ويمكن توفير سرية الاتصالات باستخدام آلية سرية مثل SSL. ولكن استعمال نظام من طرف إلى طرف مثل SSL قد يسفر عن مشاكل أخرى عندما تكون إحدى النقاط الطرفية معرضة للخطر.

2.3.2.I سرية سوية البيانات

قد يريد تطبيق ما أحياناً أن يجفر بعض أجزاء من عنصر <Policy> XACML دون غيرها.

ويمكن استخدام التجفير W3C Encryption:2002 في تجفير كامل الوثيقة XML أو بعض أجزائها. ويوصى بهذا النظام لاستعماله مع النظام XACML.

ومن البديهي أنه في حال استخدام مستودع لتسهيل اتصالات سياسة النص الواضح (أي غير المجفر) بين النقطيتن PAP وPDP ينبغي عندئذٍ استعمال مستودع آمن لتخزين هذه المعطيات الحساسة.

4.2.I تكاملية السياسة

تشكل السياسة XACML، التي تستعملها النقطة PDP لتقييم سياق الطلب صحيح النظام. لذلك فإن المحافظة على التكاملية أمر أساسي. وهناك جانبان للمحافظة على تكاملية السياسة. الأول التأكد من عدم اعتلال تلك العناصر <Policy> منذ أن استحدثتها النقطة PAP في البداية. والآخر التأكد من عدم إدراج بعض عناصر <Policy> في مجموعة السياسات أو حذفها منها.

ويتحقق الجانبان في كثير من الأحيان من خلال ضمان تكاملية الجهات العاملة وتطبيق آليات الجلسة من أجل تأمين الاتصالات بين هذه الجهات العاملة. أما اختيار الآليات المناسبة فأمر يضطلع به المنفذون. لكن عندما تتوزع السياسة بين تنظيمات ستطبقها فيما بعد أو عندما تنتقل مع الموارد المحمية، فقد يستحسن توقيع السياسة. وفي هذه الحالة يوصى باستعمال قواعد التوقيع XML ومعيار W3C مع النظام XACML.

وينبغي استعمال التواقيع الرقمية لضمان تكاملية البيانات. وينبغي عدم استخدام التواقيع الرقمية كطريقة لانتقاء السياسة أو لتقييمها. أي ينبغي ألاّ تطلب النقطة PDP سياسة تستند إلى هوية الجهة الموقعة أو ما إذا وقعت أم لا (لأن معياراً للانتقاء من هذا القبيل بحد ذاته مسألة من مسائل السياسة). بيد أن النقطة PDP يجب أن تتحقق من أن المفتاح المستخدم في توقيع السياسة هو مفتاح من قبل الجهة المنتجة للسياسة. ويتوقف تحقيق ذلك على تكنولوجيا التوقيع الخاص المتبع ولا يدخل ضمن نطاق موضوع هذه التوصية.

5.2.I معرفات هوية السياسة

نظراً إلى إمكانية الإحالة للسياسات من خلال معرفتها فإنه يتعين على النقطة PAP أن تتأكد من أنها معرفات فريدة. وقد يؤدي اللبس بين المعرفات إلى عدم التعرف على السياسة التي يمكن استخدامها. ولا تتناول هذه التوصية موضوع ضرورة إنتاج النقطة PAP لمعرف جديد في حال تعديل سياسة ما أم إمكانية استخدام نفس المعرف في السياسة بعد تعديلها. وهذه مسألة تتعلق بالممارسات الإدارية. غير أنه يجب اتباع الحذر في كلتا الحالتين. ففي حالة استعمال نفس المعرف هناك خطر إلى أن السياسات أو مجموعات السياسات التي تحيل إليه قد تتأثر. أما في حال استخدام معرف جديد فقد تستمر هذه السياسات الأخرى في استعمال السياسة الأولى إلا إذا حذفت. وفي كلتا الحالتين قد لا تتوافق النتائج مع توقعات إدارة السياسة.

6.2.I نموذج الثقة

لا بد أن تفترض النقاشات بشأن الاستيقان وحماية التكاملية والسرية نموذجاً ضمنياً للثقة: فكيف للمستعمل أن يتأكد من أن مفتاحاً ما يرتبط حصراً بمستعمل خاص محدد على نحو يمكن من استعمال المفتاح لتجفير معطيات ذلك المستعمل أو للتحقق من تواقيعه (أو بنى تكاملية أخرى) ترد من ذلك المستعمل؟ وتوجد أنواع مختلفة كثيرة من نماذج الثقة. منها التراتبيات الصارمة والسلطات الموزعة والويب والجسور وغير ذلك.

ويستحسن مراعاة العلاقات بين مختلف الجهات العاملة في نظام التحكم في النفاذ من حيث الارتباط فيما بينها.

- لا يرتبط أي كيان من كيانات نظام الترخيص بالنقطة PEP. وقد يحصل منها على معطيات كمعطيات الاستيقان مثلاً لكنه مسؤول عن التحقق منها بنفسه.
- يرتبط التشغيل الصحيح للنظام بقدرة النقطة PEP على تطبيق قرارات السياسة فعلياً.
- تعتمد النقطة PEP على النقطة PDP في تقييم السياسات تقييماً سليماً. وذلك يفترض بالمقابل أن النقطة PDP تمتلك معطيات صحيحة. وفيما عدا ذلك فإن النقطة PDP لا ترتبط بالنقطة PEP.
- تعتمد النقطة PDP على النقطة PAP في توفير سياسات ملائمة. ولا ترتبط النقطة PAP بمكونات أخرى.

7.2.I الخصوصية

من الهام إدراك أن كل معاملة تتعلق بالتحكم في النفاذ قد تضم معلومات شخصية عن الجهات التي تجريها. مثال، تنص سياسة XACML على أن بعض المعطيات لا يجوز قراءتها إلاّ من قبل الجهات التي تتمتع بكيان "العضوية متميزة" وبالتالي فإن أي معاملة تسمح لجهة مستعملة أن تنفذ فيها إلى تلك المعطيات تسرب معلومات إلى طرف غريب عن كيان الجهة المستعملة. لذلك قد ينجم عن اعتبارات الخصوصية متطلبات تجفير و/أو تحكم في النفاذ تحيط باستطباقات السياسة XACML ذاتها: قنوات مع حماية السرية لرسائل بروتوكول الطلب/الاستجابة وحماية نعوت الجهات المستعملة عند التخزين والعبور إلى غير ذلك.

ولا تتناول XACML مسألة انتقاء أو استعمال آليات الخصوصية الملائمة لبيئة ما. وتقع مسؤولية اتخاذ القرار المتعلق بكيفية ووقت نشر آليات من هذا القبيل على عاتق المنفذين وفقاً للبيئة.

التذييل II

أمثلة لاستعمال اللغة XACML

يضم هذا التذييل لأغراض توضيحية مثالين لاستعمال اللغة XACML. المثال الأول هو بسيط نسبياً يوضح استعمال الهدف والسياق ووظائف المواءمة ونعوت الجهة المستعملة. ويوضح المثال الثاني استعمال خوارزمية جمع القواعد والظروف والالتزامات.

1.II المثال الأول

تضم هذه الفقرة المثال الأول.

1.1.II سياسة المثال

لنفترض شركة اسمها Medi Corp (تعرف باسم مجالها: med.example.com) تعتمد سياسة تحكم في النفاذ تنص بالعربية على ما يلي:

يجوز لأي مستعمل يقع اسم بريده الإلكتروني ضمن مكان الاسم "med.example.com" أن يقوم بأي إجراء بشأن أي مورد.

وتكون سياسة XACML من معلومات الرأسية ووصف خياري لنص السياسة و**هدف** و**قاعدة** واحدة أو أكثر ومجموعة خيارية من **الالتزامات**.

```
[a02]  <?xml version="1.0" encoding="UTF-8"?>
[a03]  <Policy
[a04]  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
[a05]  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
[a06]  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
http://docs.oasis-open.org/xacml/access_control-xacml-2.0-policy-schema-
os.xsd"
[a07]  PolicyId="urn:oasis:names:tc:example:SimplePolicy1"
[a08]  RuleCombiningAlgId="identifier:rule-combining-algorithm:deny-
overrides">
[a09]   <Description>
[a10]    Medi Corp access control policy
[a11]   </Description>
[a12]   <Target/>
[a13]   <Rule
[a14]   RuleId= "urn:oasis:names:tc:xacml:2.0:example:SimpleRule1"
[a15]   Effect="Permit">
[a16]    <Description>
[a17]     Any subject with an e-mail name in the med.example.com domain
[a18]     can perform any action on any resource.
[a19]    </Description>
[a20]    <Target>
[a21]     <Subjects>
[a22]      <Subject>
[a23]       <SubjectMatch
[a24]       MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-
match">
[a25]        <AttributeValue
[a26]        DataType="http://www.w3.org/2001/XMLSchema#string">
[a27]         med.example.com
[a28]        </AttributeValue>
[a29]        <SubjectAttributeDesignator
[a30]        AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
[a31]        DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name"/>
[a32]       </SubjectMatch>
[a33]      </Subject>
[a34]     </Subjects>
[a35]    </Target>
[a36]   </Rule>
[a37]  </Policy>
```

[a02] وسم وثيقة XML معيارية يدل على رقم النسخة XML المستخدمة وعلى نوع التشفير.

[a03] يقدم السياسة XACML ذاتها.

[a04] – [a05] بيانات XML لمكان الاسم.

[a06] يعطي اسم URN لمخطط السياسات XACML.

[a07] يعطي اسماً لحالة السياسة هذه. ويكون اسم السياسة فريداً في نقطة PDP بحيث لا يترك أي لبس في حال الإحاله إلى سياسة ما من سياسة أخرى. ويحذف نعت نسخة وتحل محله قيمة التغيب "1.0".

[a08] يحدد الخوارزمية التي ستستخدم في تحليل نتائج القواعد المختلفة التي قد توجد في السياسة. وخوارزمية تجميع القواعد deny-overrides المحددة هنا تقضي بأنه عندما تتخذ أي قاعدة القيمة "Deny"، يتعين على السياسة أن تعيد القيمة "Deny" (رفض). وإذا كانت قيمة جميع القواعد "Permit"، أعادت السياسة القيمة "Permit" (سماح). وتفيد أيضاً خوارزمية جمع القواعد التي يرد وصفها كاملاً في الملحق C، بما يتوجب فعله إذا ما وقع خطأ عند تقييم أي قاعدة وما يتوجب عمله عندما لا تنطبق القواعد على طلب قرار ما.

[a09] – [a11] يقدم وصف نص السياسة. وهذا الوصف خياري.

[a12] يصف طلبات القرارات التي تنطبق عليها هذه السياسة. وإذا لم تتواءم الجهة المستعملة والموارد والإجراءات والبيئة الموجودة في طلب القرار مع القيم المحددة في هدف السياسة، فلا تحتاج مذكرة السياسة إلى التقييم. ويستعمل قسم الهدف هذا لاستحداث دليل لمجموعة السياسات. وفي هذا المثال، يدل قسم الهدف على قابلية تطبيق السياسة على أي طلب قرار.

[a13] يدخل القاعدة الوحيدة في هذه السياسة البسيطة.

[a14] يحدد معرف الهوية الخاص بهذه القاعدة. وكما هو الحال في سياسة ما يجب أن تحمل كل قاعدة معرفاً فريداً (فريداً على الأقل في كل نقطة PDP تستعمل هذه السياسة).

[a15] تدل على تأثير هذه القاعدة إذا كانت قيمتها "True". فتأثير القواعد هو إما "Permit" وإما "Deny". وفي هذه الحالة وإذا تم الوفاء بمتطلبات القاعدة تنتج القيمة "Permit"، مما يعني أنه طالما استخدمت هذه القاعدة بالذات فإن النفاذ المطلوب يكون مسموحاً. وإذا كانت قيمة القاعدة "False"، تعود نتيجة "NotApplicable". وإذا وقع خطأ ما عند تقييم القاعدة فإن القاعدة تعيد النتيجة "Indeterminate". وتحدد خوارزمية جمع القواعد في السياسة كما ورد سابقاً كيفية جمع قيم قواعد مختلفة في قيمة سياسة واحدة.

[a16] – [a19] يقدم وصف نص هذه القاعدة. والوصف خياري.

[a20] يدرج هدف القاعدة. وكما ورد أعلاه في هدف السياسة، يصف هدف القاعدة طلبات القرارات التي تطبق عليها هذه القاعدة. وإذا لم تتواءم الجهة المستعملة والمورد والإجراء والبيئة الواردة في طلب القرار مع القيم المحددة في هدف القاعدة، فإن مذكرة القاعدة لا تحتاج للتقييم وتعاد قيمة "NotApplicable" كنتيجة لتقييم القاعدة.

وهدف القاعدة مشابه لهدف السياسة ذاتها بفارق واحد ولكنه هام. [a23] – [a32] يكشف عن قيمة محددة يتوجب على الجهة المستعملة في طلب القرار أن تتواءم معها. ويحدد العنصر <SubjectMatch> وظيفة تواؤم في النعت MatchId وقيمة حرفية "med.example.com" ومؤشر إلى نعت الجهة المستعملة المحدد في سياق الطلب من خلال العنصر <SubjectAttributeDesignator>. وستستعمل وظيفة التواؤم لمقارنة القيمة الحرفية مع قيمة نعت الجهة المستعملة. ولا تطبق هذه القاعدة على طلب قرار ما إلا إذا أعادت عملية التواؤم القيمة "True". أما إذا أعادت القيمة "False"، فإن هذه القاعدة ستعيد القيمة "NotApplicable".

[a36] ينهي القاعدة. وقد جرى كل ما ورد في العنصر <Target> في هذه القاعدة. وفي القواعد الأكثر تعقيداً فقد يأتي العنصر <Condition> بعد العنصر <Target> (والعنصر <Condition> قد يكون مجموعة من شروط بينها AND أو OR).

[a37] ينهي السياسة. وهذه السياسة، وكما ورد سابقاً، تتضمن قاعدة واحدة فقط غير أن السياسات الأكثر تعقيداً فقد يكون لها أي عدد من القواعد.

2.1.II مثال سياق الطلب

لنتفحص طلب قرار افتراضي يمكن تقديمه إلى نقطة PDP تنفذ السياسة الواردة أعلاه. ويمكن أن يكون نص طلب النفاذ الذي يولد طلب القرار بالعربية على النحو التالي:

يريد بارت سمبسون، وعنوانه الإلكتروني "bs@simpsons.com"، أن يقرأ سجله الطبي في شركة Medi Corp.

وتتخذ المعلومات في طلب القرار حسب اللغة XACML نسق بيان سياق طلب على الشكل التالي:

```
[a38]  <?xml version="1.0" encoding="UTF-8"?>
[a39]  <Request xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
[a40]  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
http://docs.oasis-
open.org/xacml/access_control-xacml-2.0-context-schema-os.xsd">
[a41]   <Subject>
[a42]    <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name">
[a43]     <AttributeValue>
[a44]      bs@simpsons.com
[a45]     </AttributeValue>
[a46]    </Attribute>
[a47]   </Subject>
[a48]   <Resource>
[a49]    <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#anyURI">
[a50]     <AttributeValue>
[a51]      file://example/med/record/patient/BartSimpson
[a52]     </AttributeValue>
[a53]    </Attribute>
[a54]   </Resource>
[a55]   <Action>
[a56]    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-
id"
DataType="http://www.w3.org/2001/XMLSchema#string">
[a57]     <AttributeValue>
[a58]      read
[a59]     </AttributeValue>
[a60]    </Attribute>
[a61]   </Action>
[a62]   <Environment/>
[a63]  </Request>
```

[a38] – [a40] تضم معلومات الرأسية لسياق الطلب وتستخدم بنفس الطريقة التي استخدمت فيها الرأسية في السياسة الواردة أعلاه.

ويضم العنصر <Subject> نعتاً واحداً أو أكثر من الكيان الذي يقدم طلب النفاذ. وقد توجد عدة جهات طالبة وقد تكون لكل جهة عدة نعوت. أما في هذه الحالة من [a41] إلى [a47] فيوجد جهة واحدة ولها نعت واحد: هوية الجهة الطالبة معبر عنها في شكل عنوان إلكتروني هو "bs@simpsons.com". أما النعت subject-category في هذا المثال فمحذوف. لذا تعتمد قيمته بالتغيب وهي "access-subject".

ويضم العنصر <Resource> نعتاً واحداً أو أكثر للمورد الذي تطلب الجهة (أو الجهات) المستعملة النفاذ إليه. وقد يكون هناك مورداً واحداً لكل طلب قرار. وتضم السطور من [a48] إلى [a54] النعت الوحيد للمورد الذي طلب بارت سمبسون النفاذ إليه: ويتحدد المورد أنه خلال معرف ملفه URI، وهو "**file**://medico/record/patient/BartSimpson".

ويضم العنصر <Action> نعتاً واحداً أو أكثر للإجراء الذي تريد الجهة (أو الجهات) المستعملة أن تقوم به في المورد. ولا يوجد إلا إجراء واحد لكل طلب قرار. وتصف السطور من [a55] إلى [a61] هوية الإجراء الذي يريد بارت سمبسون القيام به وهو "قراءة".

العنصر <Environment> [a62]، فارغ.

[a63] ينهي سياق الطلب. وقد يتضمن سياق طلب أكثر تعقيداً بعض النعوت غير المصاحبة للجهة المستعملة أو للمورد أو للإجراء. وقد توضع هذه النعوت في عنصر <Environment> خياري يلي العنصر <Action>.

وتحدد النقطة PDP التي تعالج سياق الطلب هذا موقع السياسة في مستودع سياساتها. وتقارن الجهة المستعملة والمورد والإجراء والبيئة الواردة في سياق الطلب مع الجهات المستعملة والموارد والإجراءات والبيئات الواردة في هدف السياسة. وبما أنه هدف السياسة فارغ فإن السياسة تتواءم مع هذا السياق.

وتقارن النقطة PDP الآن الجهة المستعملة والمورد والإجراء والبيئة الواردة في سياق الطلب مع هدف القاعدة الواحدة في هذه السياسة. ويتواءم المورد المطلوب مع العنصر <Target> والإجراء مع العنصر <Target> لكن نعت هوية الجهة "subject" الطالبة لا تتواءم مع "med.example.com".

3.1.II مثال سياق الإجابة

لا يوجد قاعدة في هذه السياسة تعيد النتيجة "Permit" مجرداً على هذا الطلب وكنتيجة لتقييم السياسة. وتعطي خوارزمية جمع القواعد في السياسة في هذه الحالة أنه ينبغي إعادة النتيجة "NotApplicable". ويأتي سياق الإجابة على النحو التالي:

```
[a64]  <?xml version="1.0" encoding="UTF-8"?>
[a65]  <Response xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
http://docs.oasis-open.org/xacml/xacml-core-2.0-context-schema-os.xsd">
[a66]   <Result>
[a67]    <Decision>NotApplicable</Decision>
[a68]   </Result>
[a69]  </Response>
```

[a64] – [a65] يضم نفس نوع معلومات الرأسية التي سبق وصفها في الإجابة بالنسبة إلى السياسة.

ويضم العنصر <Result> في السطور من [a66] إلى [a68] نتيجة تقييم طلب القرار نسبةً إلى السياسة. وتكون النتيجة في هذه الحالة "NotApplicable". ويجوز للسياسة إعادة "Permit" أو "Deny"، "NotApplicable" أو "Indeterminate". لذا يطلب من النقطة PEP أن ترفض النفاذ.

[a69] ينهي سياق الإجابة.

2.II المثال الثاني

تضم هذه الفقرة مثالاً لوثيقة XML ومثالاً لسياق طلب ومثالاً لقواعد اللغة XACML. والوثيقة XML سجل طبي. وتتحدد أربع قواعد منفصلة تمثل خوارزمية جمع القواعد والظروف والالتزامات.

1.2.II مثال حالة سجل طبي

فيما يلي حالة سجل طبي يمكن تطبيق القواعد XACML عليه. ويتحدد مخطط السجل<record> من خلال أمكنة الأسماء المسجلة التي تديرها الشركة Medi Corp.

```
[a70]  <?xml version="1.0" encoding="UTF-8"?>
[a71]   <record xmlns="urn:example:med:schemas:record"
[a72]   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
[a73]    <patient>
[a74]     <patientName>
[a75]      <first>Bartholomew</first>
[a76]      <last>Simpson</last>
[a77]     </patientName>
[a78]     <patientContact>
[a79]      <street>27 Shelbyville Road</street>
[a80]      <city>Springfield</city>
[a81]      <state>MA</state>
[a82]      <zip>12345</zip>
[a83]      <phone>555.123.4567</phone>
[a84]      <fax/>
[a85]      <email/>
[a86]     </patientContact>
[a87]     <patientDoB>1992-03-21</patientDoB>
[a88]     <patientGender>male</patientGender>
[a89]     <patient-number>555555</patient-number>
[a90]    </patient>
[a91]    <parentGuardian>
[a92]     <parentGuardianId>HS001</parentGuardianId>
[a93]     <parentGuardianName>
[a94]      <first>Homer</first>
[a95]      <last>Simpson</last>
[a96]     </parentGuardianName>
[a97]     <parentGuardianContact>
[a98]      <street>27 Shelbyville Road</street>
[a99]      <city>Springfield</city>
[a100]     <state>MA</state>
[a101]     <zip>12345</zip>
[a102]     <phone>555.123.4567</phone>
[a103]     <fax/>
[a104]     <email>homers@aol.com</email>
```

```
[a105]    </parentGuardianContact>
[a106]   </parentGuardian>
[a107]   <primaryCarePhysician>
[a108]    <physicianName>
[a109]     <first>Julius</first>
[a110]     <last>Hibbert</last>
[a111]    </physicianName>
[a112]    <physicianContact>
[a113]     <street>1 First St</street>
[a114]     <city>Springfield</city>
[a115]     <state>MA</state>
[a116]     <zip>12345</zip>
[a117]     <phone>555.123.9012</phone>
[a118]     <fax>555.123.9013</fax>
[a119]     <email/>
[a120]    </physicianContact>
[a121]     <registrationID>ABC123</registrationID>
[a122]    </primaryCarePhysician>
[a123]    <insurer>
[a124]     <name>Blue Cross</name>
[a125]     <street>1234 Main St</street>
[a126]     <city>Springfield</city>
[a127]     <state>MA</state>
[a128]     <zip>12345</zip>
[a129]     <phone>555.123.5678</phone>
[a130]     <fax>555.123.5679</fax>
[a131]     <email/>
[a132]    </insurer>
[a133]   <medical>
[a134]    <treatment>
[a135]     <drug>
[a136]      <name>methylphenidate hydrochloride</name>
[a137]      <dailyDosage>30mgs</dailyDosage>
[a138]      <startDate>1999-01-12</startDate>
[a139]     </drug>
[a140]     <comment>
[a141]      patient exhibits side-effects of skin coloration and carpal
degeneration
[a142]     </comment>
[a143]    </treatment>
[a144]    <result>
[a145]     <test>blood pressure</test>
[a146]     <value>120/80</value>
[a147]     <date>2001-06-09</date>
[a148]     <performedBy>Nurse Betty</performedBy>
[a149]    </result>
[a150]   </medical>
[a151]  </record>
```

2.2.II مثال سياق الطلب

يوضح المثال التالي سياق طلب قد يمكن تطبيق قواعد المثال عليه. وهو يمثل طلباً قدمه الطبيب يوليوس هيبرت لكي يقرأ تاريخ ميلاد المريض في السجل بارتولومي سمبسون.

```
[a152] <?xml version="1.0" encoding="UTF-8"?>
[a153] <Request xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation=" urn:oasis:names:tc:xacml:2.0:context:schema:os
http://docs.oasis-open.org/xacml/access_control-xacml-2.0-context-schema-
os.xsd">
[a154]  <Subject>
[a155]   <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject-
category"
DataType="http://www.w3.org/2001/XMLSchema#anyURI">
[a156]    <AttributeValue>urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject</AttributeValue>
[a157]   </Attribute>
[a158]   <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
 DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="med.example.com">
```

```
[a159]    <AttributeValue>CN=Julius Hibbert</AttributeValue>
[a160]   </Attribute>
[a161]   <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:name-
format"
DataType="http://www.w3.org/2001/XMLSchema#anyURI"
Issuer="med.example.com">
[a162]    <AttributeValue>
[a163]     urn:oasis:names:tc:xacml:1.0:datatype:x500name
[a164]    </AttributeValue>
[a165]   </Attribute>
[a166]   <Attribute
AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="med.example.com">
[a167]    <AttributeValue>physician</AttributeValue>
[a168]   </Attribute>
[a169]   <Attribute
AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:physician-id"
DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="med.example.com">
[a170]    <AttributeValue>jh1234</AttributeValue>
[a171]   </Attribute>
[a172]  </Subject>
[a173]  <Resource>
[a174]   <ResourceContent>
[a175]    <md:record xmlns:md="urn:example:med:schemas:record"
xsi:schemaLocation="urn:example:med:schemas:record
http:www.med.example.com/schemas/record.xsd">
[a176]     <md:patient>
[a177]      <md:patientDoB>1992-03-21</md:patientDoB>
[a178]      <md:patient-number>555555</md:patient-number>
[a179]     </md:patient>
[a180]    </md:record>
[a181]   </ResourceContent>
[a182]   <Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
[a183]    <AttributeValue>
[a184]     //med.example.com/records/bart-simpson.xml#
[a185] xmlns(md=:Resource/ResourceContent/xpointer
[a186] (/md:record/md:patient/md:patientDoB)
[a187]    </AttributeValue>
[a188]   </Attribute>
[a189] </Resource>
[a190]  <Action>
[a191]   <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-
id"
DataType="http://www.w3.org/2001/XMLSchema#string">
[a192]    <AttributeValue>read</AttributeValue>
[a193]   </Attribute>
[a194]  </Action>
[a195]  <Environment/>
[a196] </Request>
```

[a152] – [a153] بيانات أمكنة اسماء معيارية.

[a154] – [a172] نعوت لجهة مستعملة موضوعة في العنصر <Subject> من العنصر <Request>. ويتكون كل نعت من معطيات النعت الشرحية وقيمة النعت. ولا يضم هذا الطلب إلا جهة مستعملة واحدة.

[a155] – [a157] لكل عنصر <Subject> نعت SubjectCategory. وتصف قيمة هذا النعت الدور الذي تؤديه الجهة المستعملة المقابلة في القيام بطلب القرار. وتعني القيمة "access-subject" الهوية التي صدر بشأنها الطلب.

[a158] – [a160] نعت الجهة المستعملة subject-id.

[a161] – [a165] نسق معرف الجهة المستعملة.

[a166] – [a168] نعت الجهة المستعملة role.

[a169] – [a171] نعت الجهة المستعملة physician-id.

[a173] – [a189] توضع نعوت المورد في العنصر <Resource> التابع للعنصر <Request>. ويتألف كل نعت من معطيات شرحية للنعت وقيمة النعت.

[a174] – [a181] محتوى المورد. حالة المورد XML الذي يطلب النفاذ إلى أجزاء منه أو إلى كامله موجودة هنا.

[a182] – [a188] معرف هوية حالة المورد المطلوب النفاذ إليه وهو تعبير XPath في العنصر <ResourceContent> الذي ينتقي المعطيات المسموح النفاذ إليها.

[a190] – [a194] توضع نعوت الإجراء في العنصر <Action> من العنصر <Request>.

[a192] معرف هوية الإجراء.

[a195] العنصر الفارغ <Environment>.

3.2.II مثال قواعد اللغة الواضحة

فيما يلي قواعد اللغة والوضحة الواجب استخدامها:

1) القاعدة 1: يجوز لشخص معرف برقمه كمريض أن يقرأ أي سجل مخصص له كمريض.
2) القاعدة 2: يجوز لشخص ما أن يقرأ أي سجل مخصص فيه كقريب أو ولي أمر للمريض الذي لا يتجاوز السادسة عشرة من العمر.
3) القاعدة 3: يجوز لطبيب الكتابة بشأن أي موضوع طبي يكون هو الطبيب المسؤول عنه ويرسل بشأنه بريداً إلكترونياً إلى المريض.
4) القاعدة 4: لا يجوز للإداري أن يقرأ أو يكتب أموراً طبية في سجل المريض.

وقد تكون هذه القواعد مكتوبة في نقاط PAP مختلفة تعمل مستقلة عن بعضها البعض أو في نقطة PAP واحدة.

4.2.II مثال حالات القاعدة XACML

1.4.2.II القاعدة 1

تبين القاعدة 1 قاعدة بسيطة تضم عنصر <Condition> واحداً. وتوضح أيضاً استخدام العنصر <VariableDefinition> في تحديد وظيفة يمكن استعمالها في السياسة.

وتعتبر حالة XACML <Rule> التالية عن القاعدة 1:

```
[a197] <?xml version="1.0" encoding="UTF-8"?>
[a198] <Policy
[a199] xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
[a200] xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation=" urn:oasis:names:tc:xacml:2.0:policy:schema:os
http://docs.oasis-open.org/xacml/access_control-xacml-2.0-context-schema-
os.xsd"
[a201] xmlns:md="http://www.med.example.com/schemas/record.xsd"
[a202] PolicyId="urn:oasis:names:tc:xacml:2.0:example:policyid:1"
[a203] RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
algorithm:deny-overrides">
[a204]  <PolicyDefaults>
[a205]         <XPathVersion>http://www.w3.org/TR/1999/Rec-xpath-
19991116</XPathVersion>
[a206]  </PolicyDefaults>
[a207]  <Target/>
[a208]  <VariableDefinition VariableId="17590034">
[a209]   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
[a210]    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
one-and-only">
[a211]     <SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:patient-number"
[a212]     DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a213]    </Apply>
[a214]    <Apply
[a215]    FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-
only">
[a216]     <AttributeSelector
```

```
[a217]     RequestContextPath="//xacml-context:Resource/xacml-
context:ResourceContent/md:record/md:patient/md:patient-number/text()"
[a218]     DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a219]    </Apply>
[a220]   </Apply>
[a221]  </VariableDefinition>
[a222]  <Rule
[a223]  RuleId="urn:oasis:names:tc:xacml:2.0:example:ruleid:1"
[a224]  Effect="Permit">
[a225]   <Description>
[a226]     A person may read any medical record in the
[a227]     http://www.med.example.com/schemas/record.xsd namespace
[a228]     for which he or she is the designated patient
[a229]   </Description>
[a230]   <Target>
[a231]    <Resources>
[a232]     <Resource>
[a233]      <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[a234]       <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">
[a235]         urn:example:med:schemas:record
[a236]       </AttributeValue>
[a237]       <ResourceAttributeDesignator AttributeId=
[a238]       "urn:oasis:names:tc:xacml:2.0:resource:target-namespace"
[a239]       DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a240]      </ResourceMatch>
[a241]      <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:xpath-node-match">
[a242]       <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">
[a243]         /md:record
[a244]       </AttributeValue>
[a245]       <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:xpath"
[a246]        DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a247]      </ResourceMatch>
[a248]     </Resource>
[a249]    </Resources>
[a250]    <Actions>
[a251]     <Action>
[a252]      <ActionMatch
[a253]       MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[a254]       <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">
[a255]          read
[a256]       </AttributeValue>
[a257]       <ActionAttributeDesignator
[a258]        AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
[a259]        DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a260]      </ActionMatch>
[a261]     </Action>
[a262]    </Actions>
[a263]   </Target>
[a264]   <Condition>
[a265]    <VariableReference VariableId="17590034"/>
[a266]   </Condition>
[a267]  </Rule>
[a268] </Policy>
```

[a199] – [a201] بيانات الأسماء XML

[a205] تعابير XPath في السياسة ينبغي تفسيرها بموجب المعيار W3C XPath:1999.

[a208] – [a221] عنصر <VariableDefinition>. وهو يحدد وظيفة تقيم حقيقة البيان: نعت الجهة المستعملة "رقم-المريض" يساوي "رقم-المريض" في المورد.

[a209] يدل النعت FunctionId على الوظيفة التي تستعمل للمقارنة. وفي هذه الحالة تتم الدالة "urn:oasis:names:tc:xacml:1.0:function:string-equal"؛ وتتخذ هذه الدالة عبارتين من النمط "http://www.w3.org/2001/XMLSchema#string".

[a210] العبارة الأولى من التعريف المتغير هي دالة يحددها النعت FunctionId. وبما أن urn:oasis:names:tc:xacml:1.0:function:string-equal يتخذ عبارات من النمط "http://www.w3.org/2001/XMLSchema#string" والنعت SubjectAttributeDesignator ينتقي سلة من النمط "http://www.w3.org/2001/XMLSchema#string"، يستعمل الاسم "urn:oasis:names:tc:xacml:1.0:function:string-one-and-only". وتضمن هذه الدالة أن عبارتها تساوي سلة تحتوي على قيمة واحدة تماماً.

[a211] ينتقي النعت SubjectAttributeDesignator سلة قيم لنعت الجهة المستعملة patient-number في سياق الطلب.

[a215] العبارة الثانية لتعريف المتغير هي دالة يحددها النعت FunctionId. . وبما أن urn:oasis:names:tc:xacml:1.0:function:string-equal يتخذ عبارات من النمط "http://www.w3.org/2001/XMLSchema#string" والنعت SubjectAttributeDesignator ينتقي سلة من النمط "http://www.w3.org/2001/XMLSchema#string"، يستعمل الاسم "urn:oasis:names:tc:xacml:1.0:function:string-one-and-only". وتضمن هذه الدالة أن عبارتها تساوي سلة تحتوي على قيمة واحدة تماماً.

[a216] ينتقي العنصر <AttributeSelector> سلة قيم من سياق الطلب باستعمال تعبير XPath حر الشكل. وينتقي في هذه الحالة القيمة patient-number (رقم المريض) من المورد. ويلاحظ أن سوابق الأسماء في التعبير XPath تتحلل في بيانات الأسماء XML.

[a223] معرف هوية قاعدة.

[a224] بيان تأثير القاعدة. وعندما تساوي قاعدة ما "True"، ترسل قيمة النعت Effect. ثم تجمع هذه القيمة مع القيم Effect في القواعد الأخرى وفقاً لخوارزمية جمع القواعد.

[a225] – [a229] وصف حر للقاعدة.

[a230] – [a263] يحدد هدف القاعدة مجموعة من طلبات القرارات التي يفترض تقييمها بالقاعدة. وفي هذا المثال العنصران <Subjects> و<Environments> محذوفان.

[a231] – [a249] يضم العنصر <Resources> تتابع فصل العناصر <Resource>. ويوجد في هذا المثال واحد فقط.

[a232] – [a248] يضم العنصر <Resource> تتابع فصل العنصر ResourceMatch ويوجد في هذا المثال اثنان.

[a233] – [a240] يقارن العنصر الأول <ResourceMatch> فرعية الأول والثاني وفقاً لدالة التواؤم. ويكون التواؤم ايجابياً إذا كانت العبارة الأولى متوائمة مع أي قيمة تختارها العبارة الثانية. ويقارن هذا التواؤم اسم هدف الوثيقة المطلوبة مع القيمة "urn:example:med:schemas:record".

[a233] يسمى النعت MatchId دالة التواؤم.

[a235] قيمة النعت الحرفية للمواءمة.

[a237] – [a239] ينتقي العنصر <ResourceAttributeDesignator> اسم الهدف من المورد الموجود في سياق الطلب. ويتحدد اسم النعت في AttributeId.

[a241] – [a247] العنصر الثاني <ResourceMatch>. ويقارن عملية التواؤم هذه نتائج العبارتين XPath. والتعبير XPath الثاني هو موقع المسير إلى العنصر XML المطلوب والتعبير Xpath الأول هو القيمة الحرفية "/md:record". وتساوي الدالة "xpath-node-match" القيمة "True" إذا كان العنصر XML المطلوب تحت ترتيب العنصر "/md:record".

[a250] – [a262] يحتوي العنصر <Actions> على تتابع مقطع من العناصر <Action>. وفي هذا المثال لا يوجد إلا عنصر <Action> واحد.

[a251] – [a261] يحتوي العنصر <Action> على تتابع ربط من العناصر <ActionMatch> وفي هذا المثال لا يوجد إلا عنصر <ActionMatch> واحد.

[a252] – [a260] يقارن العنصر <ActionMatch> بين عنصريه الأول والثاني من الفروع وفقاً لدالة التواؤم. ويكون التواؤم ايجابياً إذا كانت قيمة المتغير الأولى متوائمة مع أي قيمة من القيم التي ينتقيها المتغير الثاني. وفي هذا المثال تقارن قيمة نعت الإجراء action-id الموجودة في سياق الطلب مع القيمة الحرفية "read" (قراءة).

[a264] – [a266] العنصر <Condition>. ويجب أن تكون قيمته "True" في القاعدة التي تطبق. ويحتوي هذا الظرف على إحالة إلى تعريف متغير معرف في مكان آخر من السياسة.

2.4.2.II القاعدة 2

تبين القاعدة 2 استخدام دالة رياضية هي العنصر <Apply> مع معرف الدالة "urn:oasis:names:tc:xacml:1.0:function:date-add-yearMonthDuration" من أجل حساب تاريخ الميلاد السادس عشر للمريض. كما توضح استخدام عبارات المنطقية مع معرف الدالة "urn:oasis:names:tc:xacml:1.0:function:and". ولهذا المثال وظيفة مدرجة في العنصر <Condition> ووظيفة أخرى يحيل إليها العنصر <VariableDefinition>.

```
[a269] <?xml version="1.0" encoding="UTF-8"?>
[a270] <Policy
[a271] xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
[a272] xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
http://docs.oasis-open.org/xacml/access_control-xacml-2.0-policy-schema-os.xsd"
[a273] xmlns:xf="urn:oasis:names:tc:xacml:2.0:data-types"
[a274] xmlns:md="http:www.med.example.com/schemas/record.xsd"
[a275] PolicyId="urn:oasis:names:tc:xacml:2.0:example:policyid:2"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides">
[a276]  <PolicyDefaults>
[a277]   <XPathVersion>http://www.w3.org/TR/1999/Rec-xpath-19991116</XPathVersion>
[a278]  </PolicyDefaults>
[a279]  <Target/>
[a280]  <VariableDefinition VariableId="17590035">
[a281]   <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:date-less-or-
equal">
[a282]    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-one-and-
only">
[a283]     <EnvironmentAttributeDesignator
[a284]     AttributeId= "urn:oasis:names:tc:xacml:1.0:environment:current-date"
[a285]     DataType="http://www.w3.org/2001/XMLSchema#date"/>
[a286]    </Apply>
[a287]    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-add-
yearMonthDuration">
[a288]     <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-one-and-
only">
[a289]      <AttributeSelector RequestContextPath=
[a290]      "//md:record/md:patient/md:patientDoB/text()"
[a291]      DataType="http://www.w3.org/2001/XMLSchema#date"/>
[a292]     </Apply>
[a293]     <AttributeValue
[a294]     DataType="urn:oasis:names:tc:xacml:2.0:data-types:yearMonthDuration">
[a295]      <xf:dt-yearMonthDuration>
[a296]       P16Y
[a297]      </xf:dt-yearMonthDuration>
[a298]     </AttributeValue>
[a299]    </Apply>
[a300]   </Apply>
[a301]  </VariableDefinition>
[a302]  <Rule
[a303]  RuleId="urn:oasis:names:tc:xacml:2.0:example:ruleid:2"
[a304]  Effect="Permit">
[a305]   <Description>
[a306]    A person may read any medical record in the
[a307]    http://www.med.example.com/records.xsd namespace
[a308]    for which he or she is the designated parent or guardian,
[a309]    and for which the patient is under 16 years of age
[a310]   </Description>
[a311]   <Target>
[a312]    <Resources>
[a313]     <Resource>
[a314]      <ResourceMatch
[a315]      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[a316]       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
[a317]          http://www.med.example.com/schemas/record.xsd
[a318]        </AttributeValue>
[a319]       <ResourceAttributeDesignator AttributeId=
"urn:oasis:names:tc:xacml:2.0:resource:target-namespace"
```

```
[a320]       DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a321]      </ResourceMatch>
[a322]      <ResourceMatch
[a323]      MatchId="urn:oasis:names:tc:xacml:1.0:function:xpath-node-match">
[a324]       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
[a325]         /md:record
[a326]       </AttributeValue>
[a327]       <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:xpath"
[a328]       DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a329]      </ResourceMatch>
[a330]     </Resource>
[a331]    </Resources>
[a332]    <Actions>
[a333]     <Action>
[a334]      <ActionMatch
[a335]      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[a336]       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
[a337]         read
[a338]       </AttributeValue>
[a339]       <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
[a340]       DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a341]     </ActionMatch>
[a342]     </Action>
[a343]    </Actions>
[a344]   </Target>
[a345]   <Condition>
[a346]   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
[a347]    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[a348]     <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-
and-only">
[a349]      <SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:
[a350] parent-guardian-id"
[a351]      DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a352]     </Apply>
[a353]     <Apply
[a354]     FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
[a355]      <AttributeSelector
[a356]      RequestContextPath="//xacml-context:Resource/xacml-
context:ResourceContent/md:record/md:parentGuardian/md:parentGuardianId/text()"
[a357]      DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a358]      </Apply>
[a359]     </Apply>
[a360]     <VariableReference VariableId="17590035"/>
[a361]    </Apply>
[a362]   </Condition>
[a363]  </Rule>
[a364] </Policy>
```

[a280] – [a301] يحتوي العنصر <VariableDefinition> على جزء من الظرف (أي هل المريض تحت سن السادسة عشرة؟). ويكون عمر المريض أقل من 16 سنة إذا كان التاريخ الجاري أقل من التاريخ المحسوب بعد زيادة 16 إلى تاريخ ميلاد المريض.

[a281] – [a300] يستخدم المعرف "urn:oasis:names:tc:xacml:1.0:function:date-less-or-equal" في حساب الفرق بين متغيري التاريخ.

[a282] – [a286] يستعمل أول متغير تاريخ "urn:oasis:names:tc:xacml:1.0:function:date-one-and-only" بغية التأكد من أن سلة القيم التي انتقاها متغيرها تضم تماماً قيمة واحدة من النمط "http://www.w3.org/2001/XMLSchema#date".

[a284] يتم تقدير التاريخ الجاري بانتقاء نعت البيئة "urn:oasis:names:tc:xacml:1.0:environment:current-date".

[a287] – [a299] يستعمل متغير التاريخ الثاني "urn:oasis:names:tc:xacml:1.0:function:date-add-yearMonthDuration" بغية حساب تاريخ الميلاد السادس عشر للمريض بإضافة 16 سنة على تاريخ ميلاد المريض. والمتغير الأول من النمط "http://www.w3.org/2001/XMLSchema#date" والثاني من النمط "urn:oasis:names:tc:xacml:2.0:data-types:yearMonthDuration".

[a289] ينتقي العنصر <AttributeSelector> تاريخ ميلاد المريض بأخذ العبارة XPath في محتوى المورد.

[a293] – [a298] فترة 16 عاماً بالسنوات والشهور.

[a311] – [a344] بيان القاعدة وهدف القاعدة. انظر القاعدة 1 في الفقرة 1.4.2.4.II للحصول على الشرح المفصل لهذه العناصر.

[a345] – [a362] العنصر <Condition>. يجب أن تساوي قيمة الظرف "True" في القاعدة المطبقة. ويقيم هذا الظرف حقيقة البيان: الطالب هو الأب المسمى أو ولي الأمر والمريض تحت سن السادسة عشرة. ويضم عنصر <Apply> مدرج وعنصر <VariableDefinition> محال إليه.

[a346] يستعمل الظرف الدالة "urn:oasis:names:tc:xacml:1.0:function:and" وهي دالة بولانية تتخذ متغير واحد أو أكثر (متغيران في هذه الحالة) وتقوم بالعملية المنطقية "AND"من أجل حساب حقيقة قيمة العبارة.

[a347] – [a359] يقيِّم الجزء الول من الظرف (أي، هل الطالب هو الأب المسمى أو ولي الأمر؟). والدالة هي "urn:oasis:names:tc:xacml:1.0:function:string-equal" وتتخذ متغيرين من النمط "http://www.w3.org/2001/XMLSchema#string".

[a348] يدل على المتغير الأول. وبما أن "urn:oasis:names:tc:xacml:1.0:function:string-equal" يتخذ متغيران من النمط "http://www.w3.org/2001/XMLSchema#string"، فإن الاسم "urn:oasis:names:tc:xacml:1.0:function:string-one-and-only" يستعمل للتأكد من أن نعت الجهة المستعملة "urn:oasis:names:tc:xacml:2.0:example:attribute:parent-guardian-id" الموجود في سياق الطلب يضم قيمة واحدة تماماً.

[a353] يدل على المتغير الثاني. ويجري اختيار قيمة نعت الموضوع "urn:oasis:names:tc:xacml:2.0:example:attribute:parent-guardian-id" من سياق الطلب باستخدام العنصر <SubjectAttributeDesignator>

[a354] يستعمل الاسم "urn:oasis:names:tc:xacml:1.0:function:string-one-and-only" كما ذكر أعلاه للتأكد من أن سلة القيم التي ينتقيها متغيره تضم قيمة واحدة من النمط "http://www.w3.org/2001/XMLSchema#string".

[a355] ينتقي المتغير الثاني قيمة العنصر <md:parentGuardianId> من محتوى المورد الذي يستخدم العنصر <AttributeSelector>. ويضم هذا العنصر تعبير XPath بالشكل الحر مسنداً إلى سياق الطلب. ويلاحظ أن جميع سوابق الأسماء في التعبير XPath محللة في بيانات الأسماء المعيارية. ويساوي AttributeSelector سلة القيم من النمط "http://www.w3.org/2001/XMLSchema#string".

[a360] يحيل إلى العنصر <VariableDefinition> حيث الجزء الثاني من الظرف معرف.

3.4.2.II القاعدة 3

تبين القاعدة 3 استعمال الالتزامات. ولا يضم العنصر <Rule> XACML عنصراً مناسباً لحل التزام ما، لذا فإنه ينبغي أن تتخذ القاعدة 3 نسق عنصر <Policy> كالتالي.

```
[a365] <?xml version="1.0" encoding="UTF-8"?>
[a366] <Policy
[a367]  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
[a368]  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
[a369]  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
http://docs.oasis-open.org/xacml/access_control-xacml-2.0-policy-schema-
os.xsd"
[a370] xmlns:md="http:www.med.example.com/schemas/record.xsd"
[a371]  PolicyId="urn:oasis:names:tc:xacml:2.0:example:policyid:3"
[a372]  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
algorithm:deny-overrides">
[a373]  <Description>
[a374]   Policy for any medical record in the
[a375]   http://www.med.example.com/schemas/record.xsd namespace
[a376]  </Description>
[a377]  <PolicyDefaults>
[a378]   <XPathVersion>http://www.w3.org/TR/1999/Rec-xpath-
19991116</XPathVersion>
[a379]  </PolicyDefaults>
[a380]  <Target>
[a381]   <Resources>
[a382]    <Resource>
[a383]     <ResourceMatch
[a384]     MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

```
[a385]      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">
[a386]       urn:example:med:schemas:record
[a387]      </AttributeValue>
[a388]      <ResourceAttributeDesignator AttributeId=
[a389]      "urn:oasis:names:tc:xacml:1.0:resource:target-namespace"
[a390]      DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a391]     </ResourceMatch>
[a392]    </Resource>
[a393]   </Resources>
[a394]  </Target>
[a395]  <Rule RuleId="urn:oasis:names:tc:xacml:2.0:example:ruleid:3"
[a396]  Effect="Permit">
[a397]   <Description>
[a398]    A physician may write any medical element in a record
[a399]    for which he or she is the designated primary care
[a400]    physician, provided an email is sent to the patient
[a401]   </Description>
[a402]   <Target>
[a403]    <Subjects>
[a404]     <Subject>
[a405]      <SubjectMatch
[a406]      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[a407]       <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">
[a408]         physician
[a409]        </AttributeValue>
[a410]        <SubjectAttributeDesignator AttributeId=
"urn:oasis:names:tc:xacml:2.0:example:attribute:role"
[a411]        DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a412]      </SubjectMatch>
[a413]     </Subject>
[a414]    </Subjects>
[a415]    <Resources>
[a416]     <Resource>
[a417]      <ResourceMatch
[a418]      MatchId="urn:oasis:names:tc:xacml:1.0:function:xpath-node-
match">
[a419]       <AttributeValue
[a420]        DataType="http://www.w3.org/2001/XMLSchema#string">
[a421]          /md:record/md:medical
[a422]        </AttributeValue>
[a423]       <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:xpath"
[a424]       DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a425]      </ResourceMatch>
[a426]     </Resource>
[a427]    </Resources>
[a428]    <Actions>
[a429]     <Action>
[a430]      <ActionMatch
[a431]      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[a432]       <AttributeValue
[a433]       DataType="http://www.w3.org/2001/XMLSchema#string">
[a434]         write
[a435]       </AttributeValue>
[a436]       <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
[a437]       DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a438]      </ActionMatch>
[a439]     </Action>
[a440]    </Actions>
[a441]   </Target>
[a442]   <Condition>
[a443]   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
[a444]    <Apply
[a445]    FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-
only">
[a446]     <SubjectAttributeDesignator
[a447]     AttributeId="urn:oasis:names:tc:xacml:2.0:example:
attribute:physician-id"
```

```
[a448]     DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a449]    </Apply>
[a450]    <Apply
[a451]    FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-
only">
[a452]     <AttributeSelector RequestContextPath=
[a453]     "//xacml-context:Resource/xacml-
context:ResourceContent/md:record/md:primaryCarePhysician/md:registrationID
/text()"
[a454]     DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a455]    </Apply>
[a456]     </Apply>
[a457]   </Condition>
[a458]  </Rule>
[a459]  <Obligations>
[a460]   <Obligation
ObligationId="urn:oasis:names:tc:xacml:example:obligation:email"
[a461]   FulfillOn="Permit">
[a462]    <AttributeAssignment
AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:mailto"
[a463]    DataType="http://www.w3.org/2001/XMLSchema#string">
[a464]     &lt;AttributeSelector RequestContextPath=
[a465]     "//md:/record/md:patient/md:patientContact/md:email"
[a466]     DataType="http://www.w3.org/2001/XMLSchema#string"/&gt ;
[a467]    </AttributeAssignment>
[a468]    <AttributeAssignment
AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:text"
[a469]    DataType="http://www.w3.org/2001/XMLSchema#string">
[a470]      Your medical record has been accessed by:
[a471]    </AttributeAssignment>
[a472]    <AttributeAssignment
AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:text"
[a473]    DataType="http://www.w3.org/2001/XMLSchema#string">
[a474]     &lt;SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
[a475]     DataType="http://www.w3.org/2001/XMLSchema#string"/&gt;
[a476]    </AttributeAssignment>
[a477]   </Obligation>
[a478]  </Obligations>
[a479] </Policy>
```

[a366] – [a372] يضم العنصر <Policy> بيانات مكان الاسم المعياري ومعلمات محددة للسياسة مثل PolicyId وRuleCombiningAlgId.

[a371] معرف هوية السياسة. وتتيح هذه المعلمة إحالة مجموعة سياسات إلى السياسة.

[a372] تحدد خوارزمية جمع القواعد الخوارزمية الخاصة بمجمع نتائج تقييم القاعدة.

[a373] – [a376] وصف غير محدد الشكل للسياسة.

[a379] – [a394] هدف السياسة. يحدد هدف السياسة مجموعة من طلبات القرار القابلة للتطبيق. وتماثل بنية العنصر <Target> في <Policy> بنية العنصر <Target> في العنصر <Rule>. وهدف السياسة في هذه الحالة هو مجموعة جميع الموارد XML التي تطابق مكان الاسم "urn:example:med:schemas:record".

[a395] العنصر <Rule> الوحيد المدرج في هذا العنصر <Policy>. وتتحدد معلمتان في رأسية القاعدة هما: RuleId وEffect.

[a402] – [a441] يزيد هدف القاعدة من تقييد هدف السياسة.

[a405] – [a412] يسدد العنصر <SubjectMatch> القاعدة إلى الجهات المستعملة التي يساوي نعت جهتها "urn:oasis:names:tc:xacml:2.0:example:attribute:role" النعت "physician".

[a417] – [a425] يسدد العنصر <ResourceMatch> القاعدة إلى الموارد التي تتواؤم مع التعبير XPath "/md:record/md:medical".

[a430] – [a438] يسدد العنصر <ActionMatch> القاعدة إلى الإجراءات التي تساوي نعت إجرائها "urn:oasis:names:tc:xacml:1.0:action:action-id" النعت "write".

[a442] – [a457] العنصر <Condition>. فيما يتعلق بالقاعدة التي يمكن تطبيقها على طلب القرار، ينبغي أن تكون قيمة الطرف "True". ويقارن هذا الطرف قيمة نعت الجهة المستعملة "urn:oasis:names:tc:xacml:2.0:example:attribute:physician-id" مع قيمة العنصر <registrationId> في السجل الطبي الذي يتم النفاذ إليه.

[a459] – [a478] العنصر <Obligations>. والتزامات مجموعة عمليات يتعين على النقطة PEP القيام بها بالترابط مع قرار الترخيص. ويمكن إرفاق التزام ما بقرار الترخيص "Permit" أو "Deny". ويضم العنصر التزاماً واحداً.

[a460] – [a477] يتألف العنصر <Obligation> من النعت ObligationId وقيمة قرار الترخيص التي ينبغي أن يستوفيها ومجموعة توزيعات النعوت. ولا تحلل النقطة PDP توزيعات النعوت؛ بل هذا عمل تقوم به النقطة PEP.

[a460] يحدد النعت الالتزام. وفي هذه الحالة يتعين أن ترسل النقطة PEP معرف هوية هذا الالتزام ObligationId.

[a461] يحدد النعت FulfillOn قيمة قرار الترخيص الذي يجب أن يستوفيها هذا الالتزام. وفي هذه الحالة عندما يسمح النفاذ.

[a462] – [a467] تدل المعلمة الأولى على المكان الذي ستجد فيه النقطة PEP العنوان البريدي الإلكتروني في المورد.

[a468] – [a471] تضم المعلمة الثانية نصاً حرفياً لمتن البريد الإلكتروني.

[a472] – [a476] تدل المعلمة الثالثة على المكان الذي ستجد فيه النقطة PEP نصاً إضافياً لمتن البريد الإلكتروني في المورد.

4.4.2.II القاعدة 4

تبين القاعدة 4 استخدام قيمة التأثير "Deny" والعنصر<Rule> دون عنصر <Condition>.

```
[a480] <?xml version="1.0" encoding="UTF-8"?>
[a481] <Policy
[a482] xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
[a483] xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
http://docs.oasis-open.org/xacml/access_control-xacml-2.0-policy-schema-
os.xsd"
[a484] xmlns:md="http:www.med.example.com/schemas/record.xsd"
[a485] PolicyId="urn:oasis:names:tc:xacml:2.0:example:policyid:4"
[a486] RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
algorithm:deny-overrides">
[a487]  <PolicyDefaults>
[a488]   <XPathVersion>http://www.w3.org/TR/1999/Rec-xpath-
19991116</XPathVersion>
[a489]  </PolicyDefaults>
[a490]  <Target/>
[a491]  <Rule
[a492]  RuleId="urn:oasis:names:tc:xacml:2.0:example:ruleid:4"
[a493]  Effect="Deny">
[a494]   <Description>
[a495]    An Administrator shall not be permitted to read or write
[a496]    medical elements of a patient record in the
[a497]    http://www.med.example.com/records.xsd namespace.
[a498]   </Description>
[a499]   <Target>
[a500]    <Subjects>
[a501]     <Subject>
[a502]      <SubjectMatch
[a503]      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[a504]       <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">
[a505]        administrator
[a506]       </AttributeValue>
[a507]       <SubjectAttributeDesignator AttributeId=
[a508]       "urn:oasis:names:tc:xacml:2.0:example:attribute:role"
[a509]       DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a510]      </SubjectMatch>
[a511]     </Subject>
[a512]    </Subjects>
[a513]    <Resources>
[a514]     <Resource>
[a515]      <ResourceMatch
[a516]      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[a517]       <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">
[a518]        urn:example:med:schemas:record
[a519]       </AttributeValue>
```

```
[a520]       <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:target-namespace"
[a521]       DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a522]      </ResourceMatch>
[a523]      <ResourceMatch
[a524]      MatchId="urn:oasis:names:tc:xacml:1.0:function:xpath-node-
match">
[a525]       <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">
[a526]        /md:record/md:medical
[a527]       </AttributeValue>
[a528]       <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:xpath"
[a529]       DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a530]      </ResourceMatch>
[a531]     </Resource>
[a532]    </Resources>
[a533]    <Actions>
[a534]     <Action>
[a535]      <ActionMatch
[a536]      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[a537]       <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">
[a538]        read
[a539]       </AttributeValue>
[a540]       <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
[a541]       DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a542]      </ActionMatch>
[a543]     </Action>
[a544]     <Action>
[a545]      <ActionMatch
[a546]      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[a547]       <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">
[a548]        write
[a549]       </AttributeValue>
[a550]       <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
[a551]       DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a552]      </ActionMatch>
[a553]     </Action>
[a554]    </Actions>
[a555]   </Target>
[a556]  </Rule>
[a557] </Policy>
```

[a492] – [a493] بيان العنصر <Rule>.

[a493] تأثير القاعدة. ترسل كل قاعدة قيمتها "True" تأثير القاعدة كقيمة لها. وتأثير هذه القاعدة هو "Deny" مما يعني حسب هذه القاعدة أنه يجب رفض النفاذ عندما تساوي قيمته "True".

[a494] – [a498] وصف حر الشكل للقاعدة.

[a499] – [a555] هدف القاعدة. يحدد هدف القاعدة مجموعة طلبات القرارات التي يمكن تطبيقها على القاعدة.

[a502] – [a510] يوجه العنصر <SubjectMatch> القاعدة إلى الجهات المستعملة ذات النعت "urn:oasis:names:tc:xacml:2.0:example:attribute:role" الذي يساوي "administrator".

[a513] – [a532] يضم العنصر <Resources> عنصر <Resource> واحداً يضم بدوره عنصرين <ResourceMatch>. ويكون الهدف متوائماً إذا ما تواءم المورد الذي يعرفه سياق الطلب مِعْيارَيْ تواؤم المورد.

[a515] – [a522] يوجه العنصر الأول <ResourceMatch> القاعدة إلى الموارد التي يساوي نعت موردها "urn:oasis:names:tc:xacml:2.0:resource:target-namespace" القيمة "urn:example:med:schemas:record".

[a523] – [a530] يوجه العنصر الثاني <ResourceMatch> القاعدة إلى العناصر XML التي تتواءم مع التعبير XPath "/md:record/md:medical".

[a533] – [a554] يضم العنصر <Actions> عنصرين <Action> يحتوي كل منهما على عنصر <ActionMatch> واحد. ويكون الهدف متوائماً إذا قابل الإجراء المحدد في سياق الطلب كلاً من معايير تقابل الإجراءات.

[a535] – [a552] توجه العناصر <ActionMatch> القاعدة إلى الإجراءات التي يساوي نعت إجرائها "urn:oasis:names:tc:xacml:1.0:action:action-id" القيمة "read" أو "write".

ولا تضم هذه القاعدة العنصر <Condition>.

5.4.2.II مثال مجموعة السياسات (PolicySet)

تستخدم هذه الفقرة الأمثلة الواردة في الفقرات السابقة بهدف توضيح عمليات سياسات التجميع. وتتشكل السياسة التي تحكم النفاذ إلى قراءة العناصر الطبية في سجل ما من كل قاعدة من القواعد الأربع التي ورد وصفها في 3.2.4.II. وفيما يلي القاعدة المجمعة باللغة الواضحة:

- الطالب هو المريض؛ أو
- الطالب هو أب المريض أو ولي أمره والمريض تحت سن السادسة عشرة؛ أو
- الطالب هو الطبيب المعالج الأول والتبليغ مرسل إلى المريض؛ و
- الطالب ليس مسؤولاً إدارياً.

وتبين مجموعة السياسات التالية السياسات المجمعة. وتُضمّن السياسة 3 بالإحالة، أما السياسة 2 فتدرج صراحة.

```
[a558] <?xml version="1.0" encoding="UTF-8"?>
[a559]  <PolicySet
[a560]  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
[a561]  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
http://docs.oasis-open.org/xacml/access_control-xacml-2.0-policy-schema-
os.xsd"
[a562]  PolicySetId=
[a563]  "urn:oasis:names:tc:xacml:2.0:example:policysetid:1"
[a564]  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:
[a565]  policy-combining-algorithm:deny-overrides">
[a566]   <Description>
[a567]    Example policy set.
[a568]   </Description>
[a569]   <Target>
[a570]    <Resources>
[a571]     <Resource>
[a572]      <ResourceMatch
[a573]      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
[a574]       <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">
[a575]         urn:example:med:schema:records
[a576]       </AttributeValue>
[a577]       <ResourceAttributeDesignator AttributeId=
[a578]       "urn:oasis:names:tc:xacml:1.0:resource:target-namespace"
[a579]       DataType="http://www.w3.org/2001/XMLSchema#string"/>
[a580]      </ResourceMatch>
[a581]     </Resource>
[a582]    </Resources>
[a583]   </Target>
[a584]  <PolicyIdReference>
[a585]   urn:oasis:names:tc:xacml:2.0:example:policyid:3
[a586]  </PolicyIdReference>
[a587]  <Policy
[a588]  PolicyId="urn:oasis:names:tc:xacml:2.0:example:policyid:2"
[a589]  RuleCombiningAlgId=
[a590] "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides">
[a591]   <Target/>
[a592]   <Rule RuleId="urn:oasis:names:tc:xacml:2.0:example:ruleid:1"
[a593]   Effect="Permit">
[a594]   </Rule>
[a595]   <Rule RuleId="urn:oasis:names:tc:xacml:2.0:example:ruleid:2"
[a596]   Effect="Permit">
[a597]   </Rule>
[a598]   <Rule RuleId="urn:oasis:names:tc:xacml:2.0:example:ruleid:4"
[a599]   Effect="Deny">
[a600]   </Rule>
[a601]  </Policy>
[a602] </PolicySet>
```

[a559] – [a565] بيان العنصر <PolicySet>. وتدرج بيانات مكان الاسم XML المعياري.

[a562] يستخدم النعت PolicySetId في تحديد هوية مجموعة السياسات هذه بهدف إدراجها في مجموعة سياسة أخرى.

[a564] معرف هوية خوارزمية جمع السياسات. وتجمع السياسات ومجموعات السياسات في هذه المجموعة السياسة بموجب خوارزمية جمع السياسات المحددة عند حساب قرار الترخيص.

[a566] – [a568] وصف حر الشكل لمجموعة السياسات.

[a569] – [a583] يحدد العنصر <Target> لمجموعة السياسات مجموعة طلبات القرارات التي يمكن تطبيقها على هذا العنصر <PolicySet>.

[a584] تضم المعلمة PolicyIdReference سياسة كل معرف id.

[a588] السياسة 2 مدرجة صراحة في مجموعة السياسات هذه. وتحذف القواعد من السياسة 2 لأغراض الوضوح.

التذييل III

مثال وصف دالات السلة من المرتبة العليا

1.III مثال دالات السلة من المرتبة العليا

يصف هذا التذييل الدالات في اللغة XACML التي تقوم بعمليات موجهة إلى السلال كما لو أعلن تطبيق الدالات على السلال عموماً.

وعلى سبيل المثال تستخدم لغة وظيفية عامة تسمى هاسكِل (انظر المرجع [Haskell]) في تحديد دلالات هذه الوظائف. وعلى الرغم من أن الوصف الوارد باللغة الإنكليزية وافٍ لكن مواصفة خاصة للدلالات مفيدة أيضاً.

وبايجاز سريع يتخذ تعريف الوظيفة في ترميز هاسكِل التالي شكل الفقرات التي تطبق على نماذج البنى أي القوائم. فالرمز "[]" يعني القائمة الفارغة بينما تقابل العبارة "(x:xs)" متغيراً من قائمة غير فارغة يمثل "x" فيها العنصر الأول من القائمة و"xs" المتبقي منها وقد يكون قائمة فارغة. ونستعمل مفهوم هاسكِل للقائمة وهو مجموعة مرتبة من العناصر تكون سلات القيم XACML.

ويتحدد تعريف هاسكِل بسيط لوظيفة عادية "urn:oasis:names:tc:xacml:1.0:function:and" تتخذ قائمة من القيم من النمط البولاني على النحو التالي:

```
and:: [Bool]      -> Bool
and []            = True
and (x:xs)        = x && (and xs)
```

والسطر الأول من التعريف الذي يظهر على شكل "::" يصف رسمياً نمط معطيات الدالة التي تأخذ قائمة عناصر بولانية يدل عليها الرمز "[Bool]"، وتعيد عنصراً بولانياً يدل عليه الرمز "Bool". والسطر الثاني من التعريف عبارة عن جملة تنص على أن الوظيفة "and" المطبقة على القائمة الفارغة هي "True". والسطر الثالث من التعريف هو بند ينص على أنه في قائمة غير فارغة كتلك التي تبدأ بالعنصر "x"، هو قيمة من النمط Bool ينبغي جمع الدالة "and" المطبقة على x مع الباقي من القائمة باستعمال وظيفة الربط المنطقية الممثلة في رمز الدابجة "&&"، وهي نتيجة التطبيق للدالة "and" المتكررة. وبالطبع تكون استخدام الدالات "and" صحيحاً "True" إذا كانت القائمة التي تطبق عليها فارغة حصراً أو كل عنصر من القائمة يعادل القيمة "True". مثال تقييم عبارات هاسكِل التالية.

(and []), (and [True]), (and [True,True]), (and [True,True,False])

تساوي "True" و"True" و"True" و"False" على التوالي

(1 urn:oasis:names:tc:xacml:1.0:function:any-of

دلالة هذه العملية في لغة هاسكِل هي التالية:

```
any_of :: ( a -> b -> Bool )      -> a -> [b] -> Bool
any_of  f  a  []                  = False
any_of  f  a69  (x:xs)            = (f  a  x) || (any_of  f  a  xs)
```

وفي الترميز أعلاه "f" هي الدالة الواجب استخدامها، و"a" هي قيمة بدائية، ويمثل "(x:xs)" العنصر الأول على شكل "x" والباقي من القائمة على شكل "xs".

وتعيد العبارة التالية مثلاً القيمة "True":

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
      <Function
            FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-   equal"/>
```

```
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                Paul
        </AttributeValue>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        John
                </AttributeValue>
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        Paul
                </AttributeValue>
                <AttributeValue
                        DataType="http://www.w3.org/2001/XMLSchema#string">George
                </AttributeValue>
                <AttributeValue
                        DataType="http://www.w3.org/2001/XMLSchema#string">
                        Ringo
                </AttributeValue>
        </Apply>
</Apply>
```

وقيمة هذه العبارة "True" لأن متغير الدالة الأول مساوٍ لعنصر واحد على الأقل من عناصر السلة حسب هذه الدالة.

2) urn:oasis:names:tc:xacml:1.0:function:all-of

دلالة هذه العملية في لغة هاسكِل هي التالية:

```
all_of :: ( a -> b -> Bool )        -> a -> [b] -> Bool
all_of  f  a  []                            = True
all_of  f  a  (x:xs)                        = (f  a  x) && (all_of  f  a  xs)
```

في الترميز الوارد أعلاه "f" هي الدالة الواجب استخدامها، و"a" هي قيمة البدائية. وتمثل "(x:xs)" العنصر الأول من القائمة على شكل "x" والباقي من القائمة على شكل "xs".

وتساوي العبارة التالية مثلاً القيمة "True":

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of">
        <Function FunctionId="urn:oasis:names:tc:xacml:2.0:function:integer-
        greater"/>
        <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#integer">10</AttributeValue>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-bag">
                <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#integer">9</AttributeValue>
                <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#integer">3</AttributeValue>
                <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#integer">4</AttributeValue>
                <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#integer">2</AttributeValue>
        </Apply>
</Apply>
```

وقيمة هذه العبارة "True" لأن متغير الدالة الأول (10) أكبر من جميع عناصر السلسلة (9 و3 و4 و2)

3) urn:oasis:names:tc:xacml:1.0:function:any-of-any

دلالات الدالة "any_of_any" في لغة هاسكل مع مراعاة الدالة "any_of" المعرفة أعلاه هي التالية:

```
any_of_any :: ( a -> b -> Bool )    -> [a]-> [b] -> Bool
any_of_any  f  []                   ys          = False
any_of_any  f  (x:xs)               ys          = (any_of  f  x  ys) || (any_of_any  f  xs  ys)
```

و"f" في الترميز أعلاه هي الدالة الواجب استخدامها، ويمثل الرمز "(x:xs)" العنصر الأول من القائمة على شكل "x" والباقي من القائمة على شكل "xs".

ويساوي التعبير التالي على سبيل المثال القيمة "True":

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of-any">
        <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
equal"/>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Ringo</AttributeValue>
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Mary</AttributeValue>
```

```
        </Apply>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">John</AttributeValue>
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Paul</AttributeValue>
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">George</AttributeValue>
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Ringo</AttributeValue>
        </Apply>
</Apply>
```

قيمة هذا التعبير "True" لأن عنصراً واحداً على الأقل من عناصر السلة الأول أي "Ringo"، يساوي عنصراً واحداً على الأقل من عناصر السلة الثانية.

(4 `urn:oasis:names:tc:xacml:1.0:function:all-of-any`

دلالة الدالة "all_of_any" في لغة هاسكل مع مراعاة الدالة "any_of" المعرفة في لغة هاسكل أعلاه هي التالية:

```
all_of_any :: ( a -> b -> Bool )          -> [a]-> [b] -> Bool
all_of_any  f []          ys                    = True
all_of_any  f (x:xs)      ys                    = (any_of  f  x  ys) && (all_of_any f  xs  ys)
```

و"f" في الترميز أعلاه، هي الدالة الواجب استخدامها ويمثل الرمز "(x:xs)" العنصر الأول من القائمة على شكل "x" والباقي منها على شكل "xs".

ويساوي التعبير التالي على سبيل المثال القيمة "True".

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of-any">
        <Function FunctionId="urn:oasis:names:tc:xacml:2.0:function:integer-
greater"/>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-bag">
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">10</AttributeValue>
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">20</AttributeValue>
        </Apply>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-bag">
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">1</AttributeValue>
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">3</AttributeValue>
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">5</AttributeValue>
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">19</AttributeValue>
        </Apply>
</Apply>
```

وقيمة هذا التعبير هي "True" لأن كلاً من عناصر السلة الأولى أكبر من عنصر واحد على الأقل من عناصر السلة الثانية.

(5 `urn:oasis:names:tc:xacml:1.0:function:any-of-all`

دلالات الدالة "any_of_all" في لغة هاسكل ومع استخدام الدالة "all_of" المحددة أعلاه، هي التالية:

```
any_of_all :: ( a -> b -> Bool )      -> [a]-> [b] -> Bool
any_of_all  f []          ys                  = False
any_of_all  f (x:xs)      ys                  = (all_of  f  x  ys) || ( any_of_all  f  xs  ys)
```

و"f" هو اسم الدالة التي ينبغي استخدامها في لغة الترميز أعلاه، ويمثل الرمز "(x:xs)" العنصر الأول من القائمة على شكل "x" والباقي منها على شكل "xs".

ويساوي التعبير التالي على سبيل المثال القيمة "True":

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of-all">
        <Function FunctionId="urn:oasis:names:tc:xacml:2.0:function:integer-
greater"/>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-bag">
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">3</AttributeValue>
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">5</AttributeValue>
        </Apply>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-bag">
```

```
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">1</AttributeValue>
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">2</AttributeValue>
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">3</AttributeValue>
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">4</AttributeValue>
      </Apply>
</Apply>
```

وقيمة هذا التعبير هي "True" لأن هناك قيمة في السلة الأولى أكبر من جميع قيم السلة الثانية.

6) urn:oasis:names:tc:xacml:1.0:function:all-of-all

دلالات الدالة "all_of_all" في لغة هاسكل ومع الإفادة من الدالة "all_of" المعرفة أعلاه، هي التالية:

```
all_of_all :: ( a xs) -> b -> Bool )    -> [a] -> [b] -> Bool
all_of_all  f []            ys                = True
all_of_all  f (x:  ys                = (all_of  f  x  ys) && (all_of_all  f  xs  ys)
```

و"f" هو اسم الدالة التي ينبغي استخدامها في لغة الترميز أعلاه، ويمثل الرمز "(x:xs)" العنصر الأول من القائمة على شكل "x" والباقي منها على شكل "xs".

ويساوي التعبير التالي، على سبيل المثال، القيمة "True":

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of-all">
      <Function FunctionId="urn:oasis:names:tc:xacml:2.0:function:integer-
greater"/>
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-bag">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">6</AttributeValue>
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">5</AttributeValue>
      </Apply>
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-bag">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">1</AttributeValue>
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">2</AttributeValue>
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">3</AttributeValue>
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">4</AttributeValue>
      </Apply>
</Apply>
```

وقيمة هذا التعبير هي "True" لأن جميع عناصر السلة الأولى "5" و"6" أكبر من جميع قيم الأعداد الصحيحة "1" و"2" و"3" و"4" من السلة الثانية.

7) urn:oasis:names:tc:xacml:1.0:function:map

وتعرف هذه الدالة في لغة هاسكل على النحو التالي:

```
map:: (a -> b)     -> [a] -> [b]
map  f  []         = []
map  f  (x:xs)     =  (f x) : (map  f   xs)
```

و"f" في الترميز أعلاه هي الدالة التي ينبغي استخدامها، ويمثل الرمز "(x:xs)" العنصر الأول من القائمة على شكل "x" والباقي منها على شكل "xs".

والتعبير التالي مثلاً:

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:map">
      <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
normalize-to-lower-case">
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Hello</AttributeValue>
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">World!</AttributeValue>
      </Apply>
</Apply>
```

ويساوي قيمة سلة تتضمن "hello" و"world!" .

بيبليوغرافيا

[Haskell] THOMPSON (S.): Haskell: The Craft of Functional Programming (2nd Edition), *Addison Wesley*, ISBN 0-201-34275-8, 1996.

[IEEE 754] IEEE 754-1985, *Binary Floating-Point Arithmetic*, ISBN 1-5593-7653-8, IEEE Product No. SH10116-TBR.

[RBAC] ANSI INCITS 359-2004, *Information technology – Role Based Access Control,* http://csrc.nist.gov/rbac/.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	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 البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2009