الاتحاد الدولي للاتصالات

ITU-T X.1257

(2016/03)

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – إدارة الهوية

تصنيف إدارة الهوية والنفاذ

التوصية ITU-T X.1257

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

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

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

التوصية ITU-T X.1257

تصنيف إدارة الهوية والنفاذ

ملخص

تضع التوصية ITU-T X.1257 مواصفة من أجل ضمان تخصيص معنى العمل اللازم لأدوار إدارة الهوية والنفاذ (IAM) وتصاريحها وأن معنى العمل هذا قابل للتتبع والرجوع إليه طوال دورة حياة عملية الإدارة IAM. وهذا يعني أنه يمكن تخصيص التصاريح بكفاءة للمستعملين وإدارة وسائل التحكم في الفصل بين الواجبات (SoD) بنجاح عبر التطبيقات وتنفيذ عمليات استعراض النفاذ والتوفيق بكفاءة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1257	2016-03-23	17	11.1002/1000/12608

مصطلحات أساسية

إدارة النفاذ، دورة حياة إدارة الهوية والنفاذ، إدارة الهوية والنفاذ، دور، تصاريح، معنى العمل، تصنيف العمل، مهمة عمل.

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

تمهيد

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

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

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

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

ملاحظة

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

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

حقوق الملكية الفكرية

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

وعند الموافقة على هذه التوصية، 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/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1257

تصنيف إدارة الهوية والنفاذ

1 مجال التطبيق

تحدد هذه التوصية متطلبات تخصيص معنى العمل لأدوار إدارة الهوية والنفاذ (IAM) وتصاريح المستعمل وذلك من خلال تعزيز التوصيات [ITU-T X.1252] و[ITU-T X.1254] و[b-ITU-T X.1255] وتوسيعها لاقتراح ما يلي:

- تصنيف إدارة هوية ونفاذ لتحديد عمليات ومراحل إدارة الهوية والنفاذ وتنظيمها دلالياً بغية تقديم دورة حياة شاملة لعملية إدارة الهوية والنفاذ.
- نموذج أنطولوجي لإدارة الهوية والنفاذ وذلك من أجل أن تحدد دلالياً أنواع تصاريح وأدوار إدارة الهوية والنفاذ، وكذلك بنيتها التركيبية، وعلاقات أنواعها المناظرة.

2 المراجع

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

[ITU-T X.1252] التوصية ITU-T X.1252 (2010)، *مصطلحات وتعاريف أساسية تتعلق بإدارة الهوية.*

[ITU-T X.1254] التوصية ITU-T X.1254 (2012)، *إطار ضمان استيقان الكيان.*

3 التعاريف

1.3 مصطلحات معرفة في أماكن أخرى

1.1.3 التحكم في النفاذ [ITU-T X.1252]: إجراء متبع لتحديد ما إذا كان ينبغي منح كيان ما نفاذاً إلى موارد أو مرافق أو خدمات أو معلومات استناداً إلى ما هو محدد مسبقاً من قواعد وحقوق معينة أو إلى سلطة يتمتع بها الطرف الطالب.

2.1.3 نعت [ITU-T X.1252]: معلومات مرتبطة بكيان تحدد إحدى خصائصه.

3.1.3 سياق [ITU-T X.1252]: بيئة محدَّدة الحدود توجد فيها الكيانات وتتفاعل.

4.1.3 أوراق الاعتماد [ITU-T X.1252]: مجموعة بيانات تقدم كدليل على هوية و/أو استحقاقات مزعومة.

5.1.3 كيان [ITU-T X.1252]: شيء له وجود قائم بذاته ومميز ويمكن تعريفه في سياق.

6.1.3 معرّف الهوية [ITU-T X.1254]: نعت واحد أو أكثر يميز هوية كيان ضمن سياق محدد تمييزاً متفرداً.

7.1.3 هوية [b-ISO/IEC 24760-1]: مجموعة من النعوت متعلقة بكيان ما.

ملاحظة – قد يكون للهوية ضمن سياق معين معرّف هوية واحد أو أكثر للتمكن من التعرّف على الكيان بشكل دقيق ومتفرّد ضمن ذلك السياق.

8.1.3 دور [ITU-T X.1252]: مجموعة خصائص أو نعوت تصف المقدرات أو الوظائف التي يؤديها كيان ما.

ملاحظة – كل كيان يستطيع أن يؤدي/يحظى بأدوار كثيرة. والمقدرات قد تكون متأصلة أو ممنوحة.

9.1.3 المستعمل [ITU-T X.1252]: أي كيان يستفيد من مورد، مثل نظام أو معدات أو مطراف أو عملية أو تطبيق أو شبكة مؤسسة.

2.3 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 تخصيص النفاذ: عملية تخصيص حقوق النفاذ للمستعمل/للمستعملين.

2.2.3 إدارة طلب تغيير النفاذ: عملية لإدارة طلبات تغيير النفاذ.

3.2.3 قيود النفاذ: مجموعة من قيود النفاذ قائمة على موقع المستعمل، ومهام مقيدة مؤقتاً، وموارد مقيدة مؤقتاً.

4.2.3 هندسة النفاذ: عملية لإنشاء حقوق النفاذ والحفاظ عليها.

5.2.3 تشغيل النفاذ: عملية تقييم لحقوق نفاذ مستعمل الممنوحة لتنفيذ مهام عمل معينة.

6.2.3 سياسة النفاذ: آلية تقييد التحكم في النفاذ (وتشير إلى تصاريح العمل التي يستطيع المستعمل استخدامها خلال وقت التنفيذ).

7.2.3 توفيق النفاذ: عملية تغيير حقوق نفاذ مستعمل طبقاً لمتطلبات حقوق نفاذ مقرَّرة لتحاشي نفاذ مميز (أو مهضوم) لمستعمل.

8.2.3 استعراض النفاذ: عملية استعراض حقوق نفاذ مستعمل لأغراض توفيق وإصدار شهادات لاحق فيما يخص النفاذ.

9.2.3 سياسة التخصيص: آلية تقييد تخصيص التصاريح (أي المهام التي يمكن تخصيصها لمستعمل).

10.2.3 هندسة منطق الترخيص: عملية وضع منطق الترخيص عبر تطبيقات مترابطة والحفاظ عليه.

11.2.3 متصفّح: تطبيق على جهاز يستخدمه المستعملون للتفاعل مع مقدم خدمة.

12.2.3 دور عمل: مجموعة من المهام (بتصاريح أو بدونها) يمكن أن يكون للمستعمل الحق في أدائها.

13.2.3 تسجيل النفاذ إلى مهمة عمل: عملية تسجيل تنفيذ مهمة مكتملة بنجاح أو مستخدم غير مصرح له بأداء مهمة (مهام) معينة.

14.2.3 ترخيص بتنفيذ مهمة عمل: عملية ترخيص لمستعمل لأداء مهمة عمل محددة على مورد محدد.

15.2.3 تنفيذ مهمة عمل: عملية تنفيذ مهمة (مهام) عمل محددة.

16.2.3 هندسة تصنيف عمل: عملية إنشاء وحفظ وتصنيف عملية عمل ومنتج عمل.

17.2.3 تصنيف عملية عمل: تصنيف يحدد وينظم دلالياً عمليات عمل وعمليات عمل فرعية في بنية تراتبية.

18.2.3 قناة: أسلوب اتصال يختاره المستعمل للتفاعل مع مقدّم خدمة.

19.2.3 جهاز: آلة يستخدمها المستعمل ليتمكن من التفاعل مع مقدم خدمة.

20.2.3 استحقاق: مجموعة من المهام والتصاريح المخصصة للمستعمل.

21.2.3 دورة حياة إدارة الهوية والنفاذ: دورة حياة العمليات والعمليات الفرعية لإدارة الهوية والنفاذ (IAM).

22.2.3 هندسة أدوار إدارة الهوية والنفاذ: عملية إنشاء وحفظ أدوار وتصاريح إدارة الهوية والنفاذ.

23.2.3 النية: غرض أو حجة المستعمل لبدء تفاعل مع مقدم خدمة.

24.2.3 تصريح: مجموعة من مهام النفاذ إلى موارد عمل محجوبة بسياسات ضبط النفاذ المناظرة.

25.2.3 مورد: عقدة ورقية (متفرعة) خاصة بتصنيف منتج عمل، ويُعرف أيضاً باسم منتج عمل.

26.2.3 دورة: المدة الزمنية الخاصة بنعوت الاستيقان والترخيص.

27.2.3 مهمة: عقدة ورقية (متفرعة) خاصة بتصنيف عملية عمل وتُعرف أيضاً باسم مهمة عمل.

28.2.3 فريق: مجموعة من الموارد البشرية خاصة بأدوار عمل يتقاسمها كل أعضاء الفريق.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

APQC المركز الأمريكي للجودة والإنتاجية *(American Productivity and Quality Center)*

CPC تصنيف منتجات مركزي *(Central Product Classification)*

eTOM خريطة عمليات الاتصالات المعززة *(enhanced Telecom Operations Map)*

HTTP بروتوكول نقل النصوص المترابطة *(Hypertext Transfer Protocol)*

IAM إدارة الهوية والنفاذ *(Identity and Access Management)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IT تكنولوجيا المعلومات *(Information Technology)*

JSON ترميز الأشياء باستخدام جافاسكريبت *(JavaScript Object Notation)*

JSON-LD تسلسل البيانات المترابطة القائم على ترميز جافاسكريبت *(JSON-based Serialization for Linked Data)*

MAC التحكم في النفاذ إلى الوسائط *(Media Access Control)*

PCF إطار تصنيف العملية *(Process Classification Framework)*

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

REST النقل التمثيلي للحالة *(Representational State Transfer)*

SCIM نظام لإدارة الهوية عبر الميادين *(System for Cross-domain Identity Management)*

SDLC دورة حياة تطوير البرمجيات *(Software Development Life Cycle)*

SKOS نظام بسيط لتنظيم المعرفة *(Simple Knowledge Organization System)*

SOAP بروتوكول النفاذ البسيط إلى الأشياء *(Simple Object Access Protocol)*

SoD الفصل بين الواجبات *(Separation of Duties)*

URL موقع الموارد الموحّد *(Uniform Resource Locator)*

XACML لغة ترميز التحكم في النفاذ القابلة للتوسيع *(extensible Access Control Markup Language)*

5 الاصطلاحات

تستخدم الاصطلاحات التالية في هذه التوصية:

تشير الكلمات التي ترد في وسط الجملة وكُتِبَ أولها بحرف كبير إلى استخدام مصطلح ما يمثل جزءاً من نموذج (مثل "IAM ontology model أو "IAM taxonomy model") مثل "Business Role" أو "IAM Role Engineering"، كما يمكن أن ترد أيضاً في الرسوم المقابلة (بحسب النص الإنكليزي). كما يرد مصطلحا "مهمة عمل" و"مهمة" بمعنى واحد وذلك بغرض تسهيل قراءة النص؛ وكذلك الحال بالنسبة لمصطلحي "مورد عمل" و"مورد".

6 مقدمة

إن غياب معنى العمل في أدوار إدارة الهوية والنفاذ الحالية (IAM) وتصاريح المستعمل يترك أثراً سلبياً على دورة عمر إدارة الهوية والنفاذ. وبالرغم من أن أدوار إدارة الهوية والنفاذ مثل "مسؤول رئيسي" و"تحديث رئيسي" و"نفاذ خاص إلى النظام XYZ" تعد مصطلحات ملتبسة وضاربة في التقنية وملغّزة فإنها شائعة في كثير من المشروعات. وبطبيعة الحال، فبدلاً من إعادة استخدام هذه الأدوار الملتبسة، يقوم مهندس قائم بدور إدارة الهوية والنفاذ مرة تلو أخرى بإيجاد أدوار جديدة. إلا أن ذلك يسفر في المحصلة عن عدد ضخم من الأدوار الخاصة بإدارة الهوية والنفاذ يصعب إدارتها والتي لا تنقل المقصد من العمل المراد.

هذا العدد الضخم من الأدوار إلى جانب صياغتها الفقيرة دلالياً يترك أثراً سلبياً على مراحل رئيسية من دورة حياة إدارة الهوية والنفاذ مثل تخصيص النفاذ وترخيص النفاذ واستعراض النفاذ وتوفيق النفاذ. وخلال تخصيص النفاذ، فإن أخصائي إدارة النفاذ، الذي لا يفهم معنى الأدوار القائمة، قد يخصص منح امتيازات خاطئة للمستعمل. ولتعويض هذا النقص في معنى العمل في التطبيق الخاص بأدوار إدارة الهوية والنفاذ، ينبغي للمطورين أن يشفروا منطق الترخيص بطريقة معقّدة في تطبيقاتهم. كما أن مزامنة الحفاظ على شفرة مصدر منطق الترخيص عبر التطبيقات تمثل مشكلة وتكون معرضة للخطأ. بالإضافة إلى ذلك من الصعب (إن لم يكن مستحيلاً) تنفيذ ضوابط الفصل بين الواجبات (SoD) عبر تطبيقات كثيرة. وخلال استعراض النفاذ، وللسبب ذاته المتمثل في غياب معنى العمل في أدوار إدارة الهوية والنفاذ وكذلك الضغوط الناجمة عن الالتزام بالمواعيد النهائية، فإن مستعرضي النفاذ يؤكدون بطريق الخطأ (أو يلغون) حقوق نفاذ خاصة بمستعمل ما. وهذا المعدل العالي من أخطاء استعراض النفاذ وتنفيذ منطق الترخيص المعرض للأخطاء يزيدان من مخاطر الإضرار بالسمعة والتسبب في خسائر مالية، ويفرضان شواغل تنظيمية، ويؤثران تأثيراً سلبياً على إنتاجية فريق عمليات إدارة الهوية والنفاذ، ويعيقان القدرة على توصيل حلول مشاريع واسعة النطاق مثل العملية والتطبيق وترشيد الدور.

وحيث إن المواصفات المعيارية الحالية للتحكم في النفاذ لا تعرّف الدلالات الخاصة بأدوار إدارة الهوية والنفاذ وتصاريحها، ثمة حاجة إلى تحديد مجموعة تكميلية من متطلبات إدارة النفاذ. ومثل هذه المتطلبات سوف تضمن أن المعنى الضروري للعمل قد خُصص لأدوار وتصاريح الإدارة، وأنه قابل للتتبع والرجوع إليه طوال دورة حياة عملية الإدارة، بحيث يتسنى تخصيص التصاريح بكفاءة للمستعملين، وتنفيذ ضبط الفصل بين الواجبات تنفيذاً ناجحاً عبر التطبيقات، وإمكانية تنفيذ عمليات توفيق النفاذ ومراجعته بكفاءة.

7 لمحة عن العملية

بناءً على أن مجال تطبيق التوصية يتمثل في وضع مجموعة من المتطلبات لتحديد معنى عمل أدوار الإدارة، فإننا نورد أدناه تفاصيل النهج التالي. وكما أشرنا في الفقرة 6، يحتاج فريق هندسة دور إدارة الهوية والنفاذ لتحديد معنى عمل مطلوب لأدوار جديدة لإدارة الهوية والنفاذ. ولكن أين ينشأ أصل هذا المعنى ومن بوسعه إنتاجه؟ فلدى مهندسي الأعمال اليوم استراتيجية عمل وهم مكلفون بوضع عملية العمل وتصنيف منتج العمل.

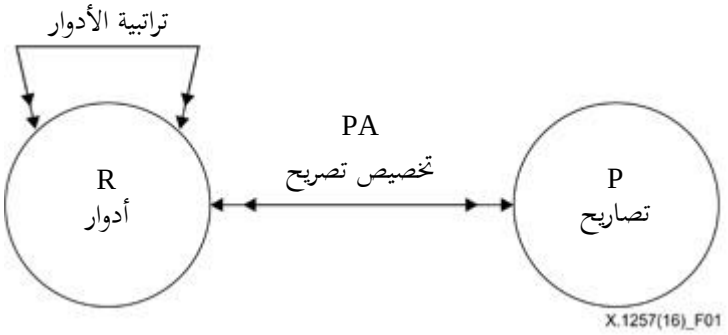
ويحدد تصنيف عملية العمل من الناحية الدلالية عمليات العمل وعمليات العمل الفرعية في بنية تراتبية (لأغراض تصفح مخزون العملية) تبدأ مع الصناعة كجذر لها ثم تتشعب إلى مجال العمل، وعملية العمل، وإجراء العمل، ومهام العمل (لمزيد من التفاصيل، انظر التذييل VI – معايير تصنيف عملية العمل). وسيشمل تصنيف عملية العمل أيضاً تسلسلاً هرمياً لمنتجات العمل وعادةً ما يقوم مهندسو منتج العمل بالاحتفاظ بها في ملفات من نوع الجداول أو الوثائق.

وخلال دورة حياة تطوير البرمجيات (SDLC)، يقوم محللو الأعمال بنسخ ولصق أجزاء محتوى التسلسل الهرمي لإنشاء الوثائق المتعلقة بمتطلبات العمل، التي تسلّم لفريق هندسة أدوار إدارة الهوية والنفاذ وفريق تطوير التطبيقات للتحرك نحو خطوات التنفيذ التالية. وبما أن مهندس الدور لا يستطيع أن يحيل مهمات عمل محددة تبعاً لمعرّف هويتها، فإنه يقوم عادةً بإنشاء أدوار لإدارة الهوية والنفاذ بتعريف أو بدون تعريف طبقاً لتفسيره المؤرخ لمهام العمل التي يمكن لمستعمل أن يؤديها. وفي النهاية، يضيع معنى العمل الخاص بأدوار الهوية والنفاذ أو يساعد فهمه من جانب مطور التطبيق. فأنى لنا حل تلك المعضلة؟

ولحلها ينبغي لمعنى العمل في أدوار إدارة IAM أن يكون قابلاً للتتبع والرجوع إليه نظير مهام العمل الحالية طوال دورة حياة عملية إدارة IAM. وتلك هي سمة الجودة التأسيسية الرئيسة التي بوسعها أن تحسن دورة حياة عملية إدارة الهوية والنفاذ برمتها. فكيف يتسنى تنفيذ سمة الجودة تلك؟ يوجد عدد من نُهُج التمثيل الدلالي لتنفيذ واجهة برمجة تطبيق خاصة بتصنيف العمل (انظر التذييل V – آليات ممكنة لتنفيذ واجهة تصنيف العمل).

إلا أن هذا لا يكفي للحصول على معنى عمل قابل للتتبع والرجوع طوال دورة حياة عملية إدارة الهوية والنفاذ. كما أن من الضروري تحديد قواعد التركيب الدلالية لأدوار إدارة الهوية والنفاذ.

وحالياً فإن قواعد التركيب الخاصة بأدوار إدارة IAM محدد من خلال آلية معيارية للتحكم في النفاذ مستخدمة على نطاق واسع يُطلق عليها اسم التحكم في النفاذ على أساس الدور (RBAC) كما هو موضح في الشكل 1.



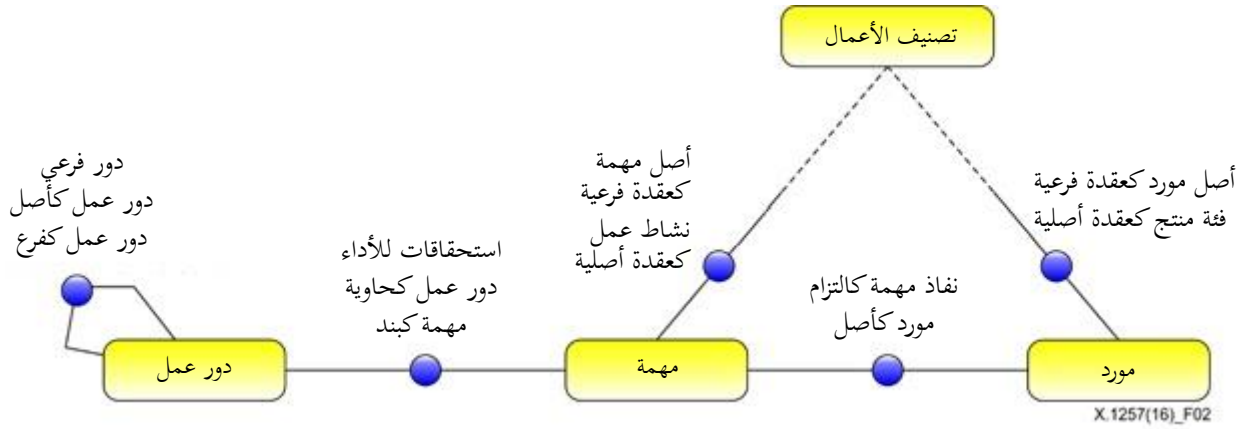
الشكل 1 – نموذج تقليدي للتحكم في النفاذ على أساس الدور

يمكن ملاحظة قواعد التركيب الخاصة بالدور كما يلي:

- يمكن للأدوار أن تحتوى على أدوار أخرى . بمعنى أنها تشكل بنية هرمية للدور.
- الأدوار مكوّنة من تصاريح.

ومع ذلك، فإن أي آلية ضبط للتحكم في النفاذ على أساس الدور تلك يعتريها جانب قصور معروف، هو أنها لا تحدد دلالات التصريحات (بمعنى "طبيعة التصريحات"). بل إن التحديد يعني أن دلالات التصريح مفتوحة للتفسير، إذ "يمكن تعريف التصريحات من منظور عمليات بدائية مثل القراءة والكتابة، أو عمليات مجردة، مثل دائن ومدين" [b-NIST-RBAC 2000]. ومع ذلك فإنه على مستوى الممارسة كما هو موضح في الفقرة 6، هناك أدوار إدارة ملتبسة لإدارة الهوية والنفاذ صيغت دونما إحالة إلى مهام العمل المناظرة.

ومن أجل تخصيص معنى عمل لأدوار إدارة IAM يلزم تحديد قواعد تركيب دلالية لأدوار الإدارة. وسيأتي معنى العمل من أكثر العقد الورقية والمهام والموارد تفصيلاً في تصنيف العمل. ويصف الشكل 2 قواعد التركيب الدلالية لدور إدارة IAM.



الشكل 2 – إدارة النفاذ القائم على المهمة، مخطط مفاهيمي

يمكن ملاحظة ما يلي:

- تستطيع الأدوار (ولا تزال) احتواء أدوار أخرى من خلال علاقة "الدور الفرعي"، أي تشكيل بنية تراتبية للأدوار.
- قواعد التركيب الدلالية الرئيسية لأدوار إدارة IAM:
  - دور عمل يمنح المستعمل حق أداء مهمة (مهمات) عمل من خلال علاقة "الحق في الأداء". وهذا يمكّن أي دور إدارة IAM من أن يتولى ضمنياً معنى عمله من مهمات العمل المناظرة.
  - تقوم مهمة عمل (وليس المستعمل أو الدور) بالنفاذ إلى مورد محدد (أي "منتج عمل"). وعلاقة النفاذ هي علاقة اختيارية وتحتاج إلى حالات يطلب فيها تحكم أكثر دقة في النفاذ.
  - والمهمة والمورد بوصفهما عقد ورقية لتصنيف العمل يعملان كلبنات أساسية إضافية خلال هندسة دور الإدارة IAM ويُرجع إليهما خلال دورة حياة عملية الإدارة IAM.

ولا يعرض الشكل 2 الأنواع الأساسية الخاصة بمنتج المهمة والمورد لدواعي التبسيط.

ويُظهر الجدول 1 قليلاً من الأمثلة على الاستحقاق المتعلق بقواعد التركيب أعلاه ستساعد في إيضاح هذه النقاط:

الجدول 1– أمثلة على الاستحقاق

دور العمل	المهمة	المورد
صرّاف	إنشاء حساب	حساب متداول متقدم
دكتور	مراجعة تاريخ المريض	تاريخ المريض
مدير النظام	تحديث بيئة النظام	بيئة النظام

إن قواعد التركيب الدلالية أعلاه لأدوار إدارة الهوية والنفاذ ستحقق الهدف الرئيسي لتخصيص معنى العمل لأدوار إدارة IAM. أما الفقرة التالية فستعبر عن العملية المقترحة في شكل متطلبات.

8 المتطلبات الدلالية والتركيبية لدور إدارة الهوية والنفاذ

حددت التوصيات التالية لإعطاء أدوار الإدارة IAM معنى العمل اللازم:

1 تصنيف عمل يعمل كمُدخل أساسي في دورة حياة عملية الإدارة IAM لتوفير معنى العمل في أدوار إدارة الهوية والنفاذ وتصاريح المستعمل خلال دورة حياة الإدارة IAM برمتها.

2 معنى العمل في أدوار إدارة IAM قابل للتتبع ويمكن الرجوع إليه لمهمات العمل المناظرة من تصنيف العمل خلال دورة حياة عملية الإدارة.

3 يكون لأدوار IAM قواعد التركيب الدلالية التالية:

1.3 يتألف دور إدارة IAM من مهمات عمل يكون للمستعمل الحق في أدائها.

2.3 يتكون دور إدارة IAM من مهمات عمل تنفذ اختيارياً إلى موارد عمل محددة إن كان ثمة حاجة لتحكم أكثر دقة في النفاذ.

4 تنفيذ ناجح لمهمات العمل فضلاً عن طلبات تنفيذ مهمات عمل غير مصرح بها يتم تسجيل الدخول إليها من خلال الإحالة إلى معرفي هوية مهمات العمل المناظرة.

الملحق A

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية)

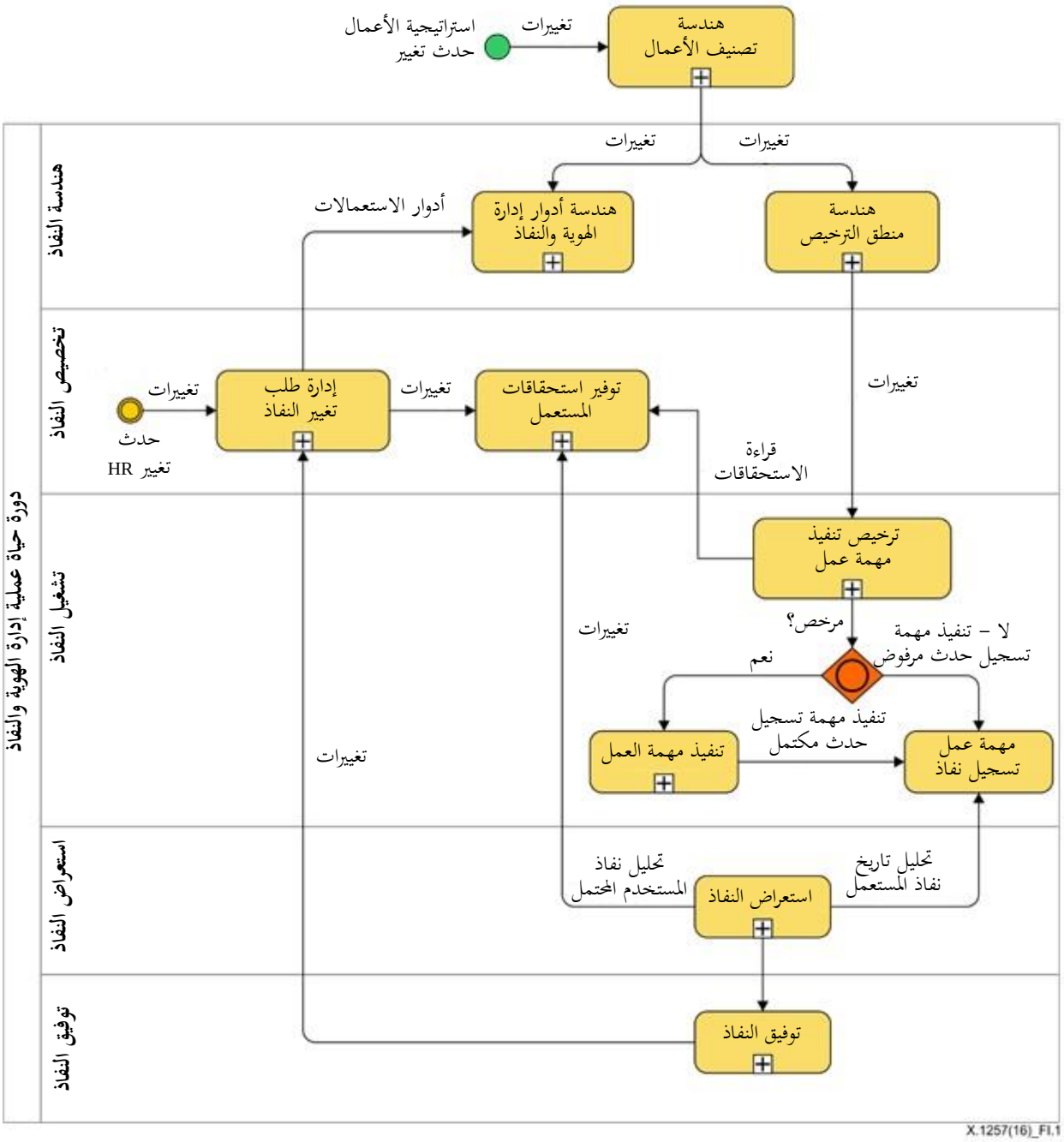
ترك هذا الملحق فارغاً بغرض تقديم سيناريوهات تنفيذ قادمة محتملة لإدارة النفاذ القائم على مهمة إدارة الهوية والنفاذ.

التذييل I

دورة حياة عملية تصنيف إدارة الهوية والنفاذ

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يؤكد الشكل 1.I حقيقة أن دورة حياة عملية إدارة الهوية والنفاذ برمتها تتأثر بشكل أساسي بالتغيرات الناشئة في تصنيف العمل. وتغيرات تصنيف العمل تلك تلقي دعماً واهتماماً من فريق هندسة دور إدارة الهوية والنفاذ وفريق هندسة دور إدارة الهوية والنفاذ. وسوف تحتوي التغيرات على معرفات هوية لمهمة العمل في العناصر الأساسية المناظرة مثل أدوار الإدارة، وشفرة مصدر منطق الترخيص، وتنفيذ مهمة العمل وملفات تسجيل الترخيص.



الشكل 1.I – العناصر التي تعتمد عليها دورة حياة عملية إدارة الهوية والنفاذ

المصدر الثاني للتغيير هو الأحداث الخاصة بالموارد البشرية مثل التعيين أو الإجازة أو النقل وأحداث أخرى من هذه الأنواع. وتعالج هذه الأحداث عملية إدارة طلب تغيير النفاذ وتقدم استحقاقات المستعمل المناظرة إلى أدلة استحقاقات المستعمل. ومن الملاحظ أن هذه الاستحقاقات سوف تشمل إحالات معرف الهوية إلى مهام العمل التي تقدم معنى عمل وبعدها يتم الإحالة خلال ترخيص مدة عمل التطبيق. وبمجرد استيقان المستعمل (لم تُعرض العملية رغبة في التبسيط) فإن ضوابط وقائية للفصل بين الواجبات سوف تمنع تنفيذ مهمات العمل المتضاربة خلال وقت الترخيص. وخلال عملية ترخيص تنفيذ مهمة عمل يكون المستعمل مخوّلاً لأداء هذه المهمة وتنفيذها، أو غير مخوّل لأداء هذه المهمة. وفي كلتا الحالتين فإن التطبيق يسجل هذه الأحداث بالإحالة إلى معرفات هوية مهمات العمل المناظرة. ويوجد أدناه مثال محتمل لنسق التسجيل هذا:

2016-02-08 22:20:02,165 ait:AppID1 192.168.0.1 UserID123 **btt:TaskID1 btr:456:355** bttes:200 "تمت العملية بنجاح"

2016-02-08 22:24:02,165 ait:AppID1 192.168.0.1 UserID123 **btt:TaskID2** bttes:401 "المستعمل غير مرخص له تنفيذ المهمة"

حيث:

- **btt** – اسم حيز الاسم يشير إلى سابقة موقع الموارد الموحد لبروتوكول نقل النصوص المترابطة مثل: **http://example.com/mylob/businesstaxonomy/task/**
- **btt:TaskID1** – معرف هوية مهمة العمل. وعندما يُلحق معرف هوية مهمة العمل بحيز الاسم **btt**، فإنه يمكن استخدامه لاسترجاع معلومات مهمة عمل إضافية مثل اسم المهمة ووصف المهمة وإحصائيات استعمال المهمة.
- **bttes** – اسم لحيز اسم يشير إلى سابقة موقع الموارد الموحد لبروتوكول نقل النصوص المترابطة مثل: **http://example.com/mylob/businesstaxonomy/task/execution/state**
- **bttes:200** – شفرة حالة تنفيذ مهمة تشير إلى تنفيذ ناجح لمهمة.
- **bttes:401** – شفرة حالة تنفيذ مهمة تشير إلى تنفيذ مهمة غير مرخص به.

وحيث إن مهمات العمل يُشار إليها دلالياً في ملفات السجل، فإنه من الممكن لمستعرض نفاذ أن يحلل التاريخ الخاص بنفاذ المستعمل فضلاً عن نفاذ مستعمل محتمل من حيث تنفيذ مهمة العمل. وبمجرد تحليل نفاذ المستعمل واستعراضه بشكل شامل، يُعاد إرسال تغييرات التوفيق المناظرة إلى إدارة طلب تغيير النفاذ لتصويب أي حقوق نفاذ مستعمل مميزة أو غير مستحقة. وتعتبر تغييرات التوفيق هذه هي آلية عروة الرجعة التي تميز أي عملية مثل دور الحياة، مثلاً دورة حياة عملية إدارة IAM. ومع ذلك، ليست كل المراحل مطلوبة للمشروعات المتوسطة والصغيرة. فعلى سبيل المثال أهملت هندسة منطق ترخيص التطبيق أو ينفذها مكوّن دليل المستعمل. ولا يضم الشكل 1.I إلا الأجزاء الرئيسية من دورة حياة عملية إدارة IAM برمتها.

والقائمة المرقمة التراتبية التالية هي تمثيل نصي لدورة حياة عملية إدارة IAM. وكل عقدة تصنيفية معرفة أيضاً في الفقرة 2.3. وللاطلاع على تمثيل مشفر، يرجى النظر في مخطط النظام البسيط (SKOS) لتنظيم المعرفة [b-Antonie].

1 إدارة تغيير العمل
- 1.1 هندسة تصنيف العمل
  - 1.1.1 تغيير عملية العمل
  - 2.1.1 تغيير منتج العمل

2 هندسة النفاذ
- 1.2 هندسة أدوار إدارة IAM
- 2.2 هندسة منطق الترخيص

3 إدارة هوية الكيان
- 1.3 ITU-T X.1254 "مرحلة الالتحاق" (التحاق الكيان)

1.1.3 التطبيق والبدء
2.1.3 تدقيق الهوية
3.1.3 التحقق من الهوية
4.1.3 تسجيل الأرشفة
5.1.3 تسجيل
2.3 ITU-T X.1254 "مرحلة إدارة أوراق الاعتماد" (إدارة أوراق الاعتماد)
1.2.3 إنشاء أوراق الاعتماد
2.2.3 ما قبل إنشاء أوراق الاعتماد
3.2.3 استهلال أوراق الاعتماد
4.2.3 إسناد أوراق الاعتماد
5.2.3 إصدار أوراق الاعتماد
6.2.3 تفعيل أوراق الاعتماد
7.2.3 تخزين أوراق الاعتماد
8.2.3 تعليق أوراق الاعتماد
9.2.3 إبطال أوراق الاعتماد
10.2.3 تدمير أوراق الاعتماد
11.2.3 تجديد أوراق الاعتماد
12.2.3 إبدال أوراق الاعتماد
13.2.3 الأرشفة
4 تخصيص النفاذ
1.4 إدارة طلب تغيير النفاذ
2.4 إدارة تصريح المستعمل
3.4 توفير استحقاقات المستعمل
5 تشغيل النفاذ
1.5 "مرحلة استيقان الكيان" ITU-T X.1254 (الاستيقان)
1.1.5 الأرشفة
2.1.5 استيقان الدورة
2.5 الترخيص
1.2.5 ترخيص تنفيذ مهمة العمل
3.5 تسجيل النفاذ إلى مهمة العمل
6 استعراض النفاذ
1.6 التحليل
1.1.6 تحليل حقوق النفاذ المحتملة
2.1.6 تحليل تاريخ نفاذ المستعمل
2.6 مراجعة النفاذ
7 توفيق النفاذ

التذييل II

مقترح لخصائص توسيع نظام لإدارة الهوية عبر الميادين 2.0

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

تشكل خصائص التوسيع التالية نظاماً مقترحاً كأساس لبروتوكول خدمة الويب للنقل التمثيلي للحالة (REST) الخاصة بالإصدار الثاني لنظام إدارة الهوية عبر الميادين[1] [b-SCIM REST]. ويوضح الشكل 1.II توسيع الخصائص المقترح. وتمثل الخطوط والأشكال باللون الأسود الأجزاء الأساسية من المواصفة الحالية للإصدار الأول [b-IETF SCIM 1.0] لنظام إدارة الهوية عبر الميادين (SCIM). ويمثل الشكلان الزرقاوان ("الأدوار" و"الاستحقاقات") هم نقاط توسيع النظام SCIM. وتمثل الخطوط والأشكال الواردة باللون البرتقالي غير المتقطع التوسيعات المقترحة. وبما أن مواصفات النظام SCIM تترك الطبيعة الدلالية "للأدوار" و"الاستحقاقات" مفتوحة للتفسير والتعريف من خلال التنفيذ،[2] فإنه من المحتمل حدوث تحديد أكثر لنقاط التمديد لتصبح جزءاً من المعيار الرئيسي.

وحتى يتسنى تخصيص معنى العمل لأدوار إدارة IAM، تُقترح التوصيات التالية كخصائص توسيع لمواصفات النظام SCIM الحالي:

- نقطة توسيع "أدوار" النظام SCIM تعمل كحاوية لأدوار العمل، حيث إن أي دور عمل يتشكل من مهمة عمل واحدة أو أكثر.
- نقطة توسيع "استحقاقات" النظام SCIM تعمل كحاوية لمهمات عمل إضافية يمكن للمستعمل أن يؤديها (بالإضافة لمهمات العمل التي يستطيع المستعمل أن يؤديها من خلال أدوار عمل مخصصة).

---

1 "صُممت مواصفة نظام إدارة الهوية عبر الميادين (SCIM) لتسهيل إدارة هويات المستعمل في خدمات وتطبيقات سحابية". نقلاً عن http://www.simplecloud.info/

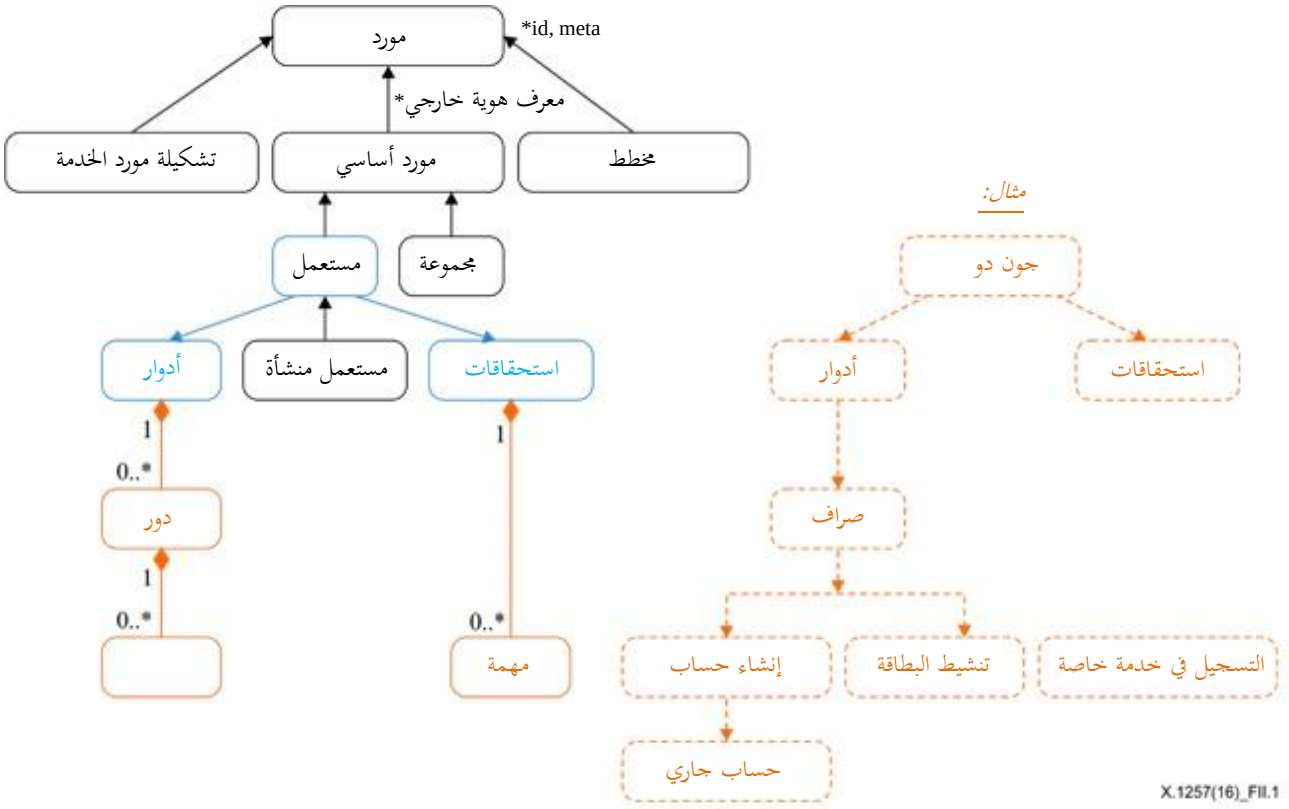
2 يترك نظام إدارة الهوية عبر الميادين (SCIM) هذه المصطلحات مفتوحة للتفسير والتعريف في عملية التنفيذ:

"الاستحقاقات

قائمة من الاستحقاقات للمستعمل الذي يقدم شيئاً يملكه. أي إن الاستحقاق هو حق إضافي في شيء أو كائن أو خدمة. وليس هناك مفردات أو قواعد تركيب محددة ومن المتوقع أن يقوم مقدمو الخدمة والمستهلكين بصياغة معلومات كافية من حيث القيمة بحيث يحددون بدقة وبدون لبس ما الذي سينفذ إليه المستعملُ. وهذه القيمة **ليس** لها أنواع متعارف عليها بالرغم من أن النوع قد يكون مفيداً كوسيلة لتحديد نطاق الاستحقاقات.

الأدوار

قائمة من الأدوار للمستعمل تقدم مجتمعة من هو المستعمل، أي "طالب"، "كلية". وما من مفردات أو قواعد تركيب محددة رغم أنه من المتوقع أن قيمة الدور هي سلسلة أو وسم يمثل مجموعة من الاستحقاقات. و**ليس** لهذه القيمة أنواع متعارف عليها." نقلاً عن https://tools.ietf.org/html/draft-ietf-scim-core-schema-22



الشكل 1.II – توسيع خصائص نظام إدارة الهوية عبر الميادين

يوضح المثال إلى اليمين باللون البرتقالي يبين كيف يمكن لمستعمل ما أن يحظى بدور "صراف" يتكون من مهمتين: "إنشاء حساب" و"تفعيل البطاقة". المهمة الأخرى – "التسجيل في خدمة خاصة" هي استحقاق إضافي مباشر لا يحتاج إلى استحداث دور له.

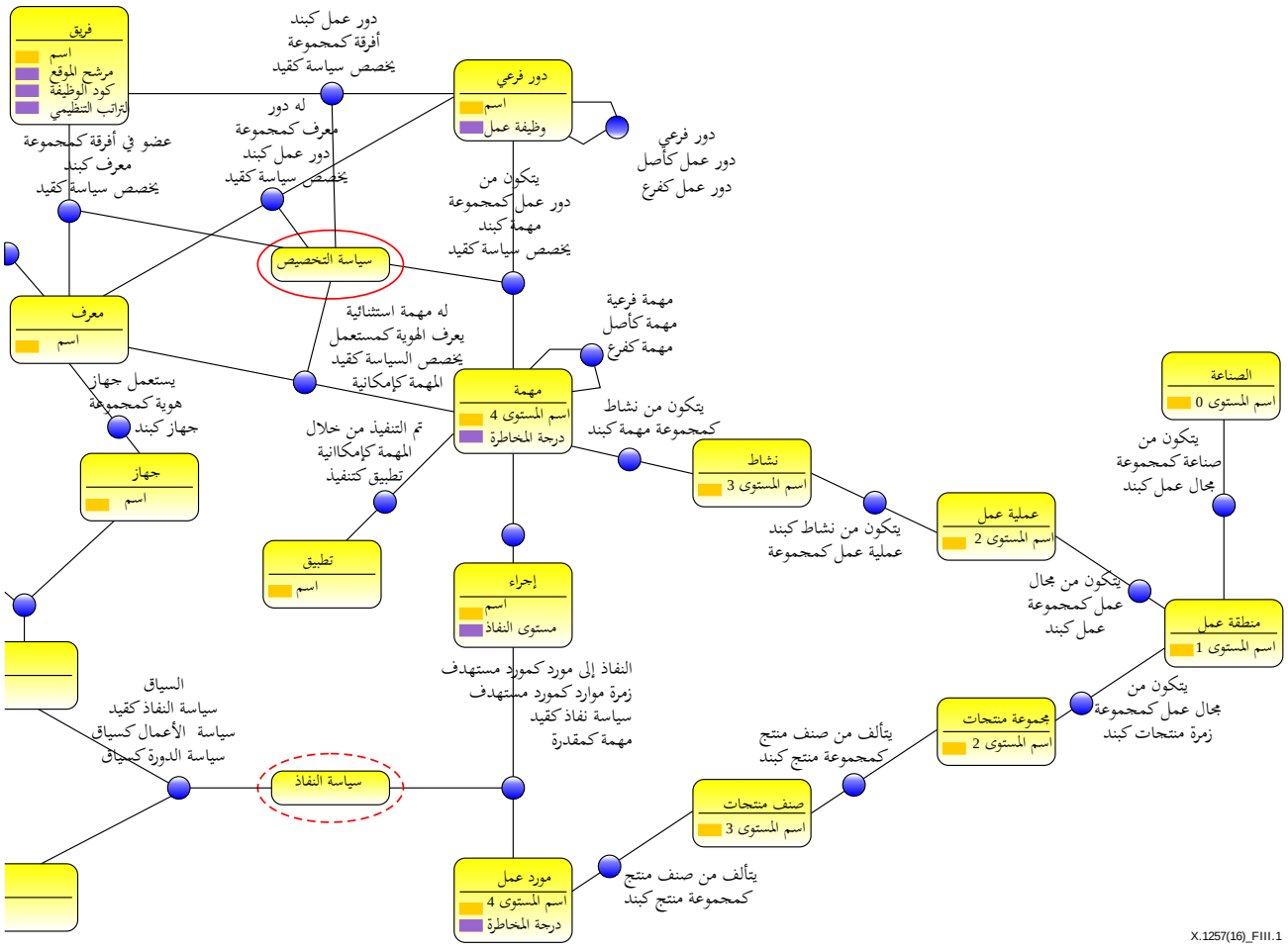
التذييل III

توسيع مقترح لخصائص لغة ترميز التحكم في النفاذ القابلة للتوسيع [XACML 3.0]

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

بغية تحقيق أهداف جودة بيانات إدارة الهوية والنفاذ المحددة في بند العمل هذا، تُقترح خصائص التوسيع التالية:

يهدف المقترح لتقديم نوع جديد من سياسة الإصدار الثالث للغة ترميز التحكم في النفاذ القابلة للتوسيع (XACML 3.0) [b-OASIS XACML 3.0]، سياسة التخصيص (رسمت حولها دائرة حمراء بخط غير متقطع)، وهي سياسة جرى تقييمها خلال وقت طلب النفاذ. ومثال على ذلك سياسة النفاذ لإنفاذ قوانين الفصل بين الواجبات (SoD) خلال وقت تخصيص النفاذ. ومن ناحية أخرى، فإن سياسة النفاذ (رسمت حولها دائرة حمراء بخط متقطع) هي سياسة يجري تقييمها خلال وقت التشغيل وهي عادة أكثر تعقيداً (مليئة بتفاصيل دقيقة). ويُظهر الشكل 1.III أجزاء مخطط إدارة الهوية والنفاذ المؤكدة لسياسة التخصيص المقترحة.



الشكل 1.III – أجزاء مخطط إدارة الهوية والنفاذ المؤكدة لسياسة التخصيص

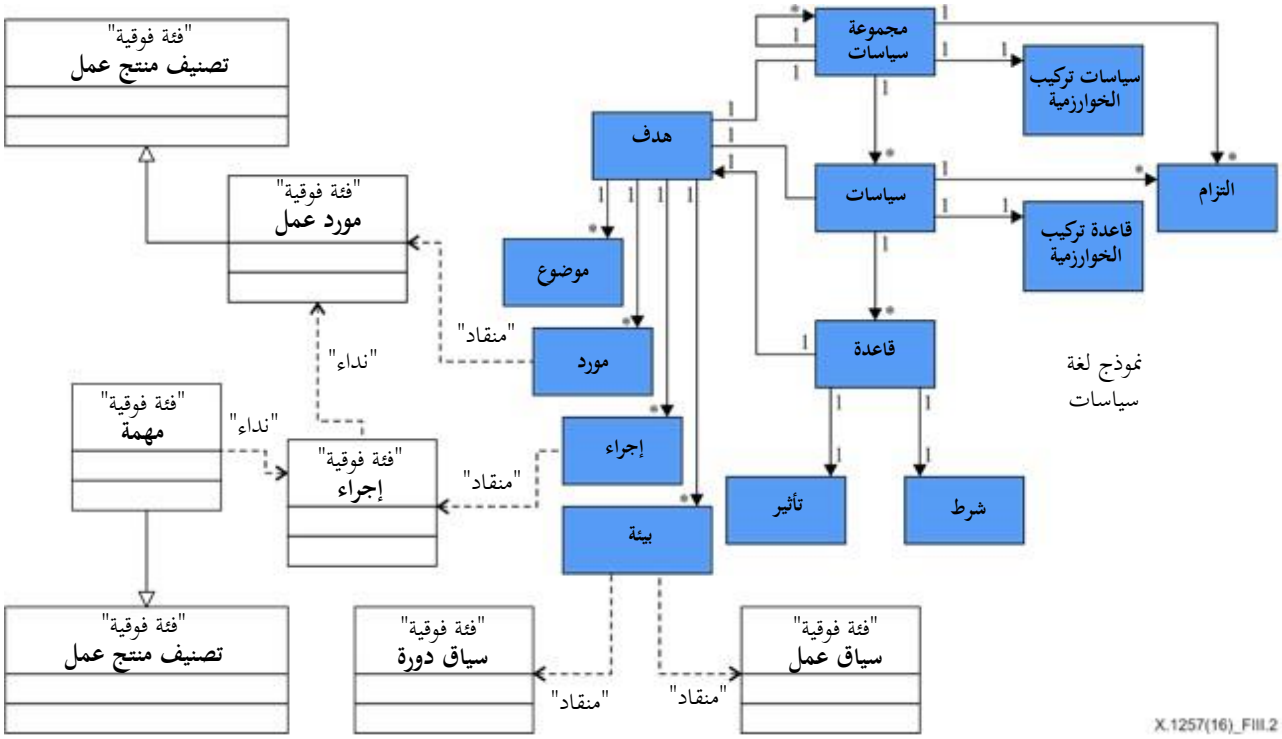
تمكين دلالات العمل لنموذج لغة ترميز التحكم في النفاذ القابلة للتوسيع (XACML):

أ) نعوت المورد المرجعي من خلال هوية مفهوم مورد العمل. ومورد العمل هو العقدة الورقية لتصنيف منتج العمل.

ب) نعوت الإجراء المرجعي من خلال هوية مفهوم الإجراء والمهمة. والمهمة هي العقدة الورقية لتصنيف عملية العمل. والإجراء هو العملية التي قامت بها المهمة في مورد العمل.

ج) نعوت البيئة المرجعية من خلال هوية مفهوم سياق الدورة وسياق العمل. بوسع سياق العمل تقديم نعوت عمل مفصلة بدقة مثل مرشاح رقم الحساب. وبوسع سياق الدورة الواعي بحالة استيقان (أوراق الاعتماد والبيانات الشرحية للجهاز) أن يقدم معلومات مثل عنوان بروتوكول إنترنت (IP) وعنوان جهاز للتحكم في النفاذ إلى الوسائط (MAC) للترخيص التقني الدقيق.

ويُظهر الشكل 2.III التوسيع الدلالي المقترح لنموذج لغة ترميز التحكم في النفاذ القابلة للتوسيع.



الشكل 2.III – توسيع دلالي مقترح لنموذج لغة ترميز التحكم في النفاذ القابلة للتوسيع

التذييل IV

حالات استعمال إدارة النفاذ القائمة على المهمة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

توضح حالات الاستعمال التالية ذات الصلة فائدة هذه التوصية:

1 سياسة النفاذ:

أ) المستعمل ألف لديه الحق في أداء مهمات العمل ألف وباء وجيم من خلال دور العمل ألف.

ب) المستعمل ألف لديه الحق الإضافي في أداء مهمة العمل دال من خلال استحقاقات مباشرة.

ج) السياسة ألف تحدد أن المهمة باء والمهمة دال تستبعد كل منهما الأخرى لرقم الحساب ذاته.

د) تقييم سياسة ألف واتخاذ قرار بالرفض للسيناريو المذكور أعلاه.

2 الإبلاغ عن (استحقاقات) النفاذ:

أ) الاستفادة من مفاهيم المهمة لتحسين وضوح النص ومعنى الجهد الحالي لوصف استحقاقات لغة العمل.

ب) الاستفادة من مفاهيم موارد العمل لتحسين وضوح النص ومعنى الجهد الحالي لوصف استحقاقات لغة العمل.

3 استعمال مهمة عمل:

أ) الاستفادة من تطبيق ويب مرجعي قائم و:

'1' تهيئة قالب تسجيل تطبيق من أجل استعمال معرفات هوية مهمة عمل.

'2' توليد ملفات تسجيل خلال وقت تشغيل التطبيق.

ب) استنفاد ملفات تسجيل التطبيق مع أداة تحليلية من أجل:

'1' الاستفادة من مفاهيم موارد العمل لتحسين وضوح النص ومعنى الجهد الحالي لوصف استحقاقات لغة العمل.

'2' تحديث تصنيف الأعمال بفضل المعلومات الإحصائية الواردة أعلاه.

4) استعمال الاستحقاقات:

أ) الاستفادة من تطبيق ويب مرجعي قائم و:

'1' تهيئة قالب تسجيل تطبيق من أجل استعمال معرفات هوية مهمة عمل.

'2' توليد ملفات تسجيل خلال وقت تشغيل التطبيق.

ب) استنفاد ملفات تسجيل التطبيق مع أداة تحليلية من أجل:

'1' ربط أحداث تنفيذ مهمات العمل القائمة على معرف هوية المهمة.

'2' ربط أحداث رفض التراخيص القائمة على معرف هوية المهمة.

'3' إنتاج تقارير تحليلية تشير إلى السيناريوهات المتضاربة الخاصة بالفصل بين الواجبات التي تعود لفترة زمنية سابقة.

التذييل V

آليات ممكنة لتنفيذ واجهة تصنيف عمل

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

تستطيع الحلول القائمة على المعايير مثل آلية المفردات المضبوطة أو آلية تسجيل البيانات الشرحية الخاصة بالنظام البسيط لتنظيم المعرفة[3] (SKOS) [b-Antonie] أن تقدم تسجيل وتحديد هوية مفهوم تصنيف العمل. ونظام المعرفة (SKOS) مفيد بوجه خاص في تمثيل علاقات تراتبية.

وثمة حل آخر يتمثل في تسلسل البيانات المرتبطة القائم على ترميز الأغراض (JSON) باستخدام جافاسكريبت [b-W3C JSON-LD] (JSON-LD) أو ما يعرف باسم JSON-Linked Data. وبينما يسمح النظام (JSON-LD) بخلط مفردات مضبوطة متنوعة وله القدرة على تمثيل علاقات بيانية معقدة؛ فإنه ليس ثمة معيار لواجهة تصنيف. ولا يوجد حتى وقتنا هذا عمليات تنفيذ للنقل التمثيلي للحالة (REST) أو حتى لبروتوكول النفاذ البسيط إلى الأشياء (SOAP).

3 يوفر نظام المعرفة (SKOS) علاقة تراتبية أساسية من قبيل أوسع وأضيق إلا أنه لا يسمح بمزيد من العلاقات الأنطولوجية المحددة التي قد تلزم للإعراب عن معنى وقواعد تركيب عنصر بيانات إدارة الهوية والنفاذ.

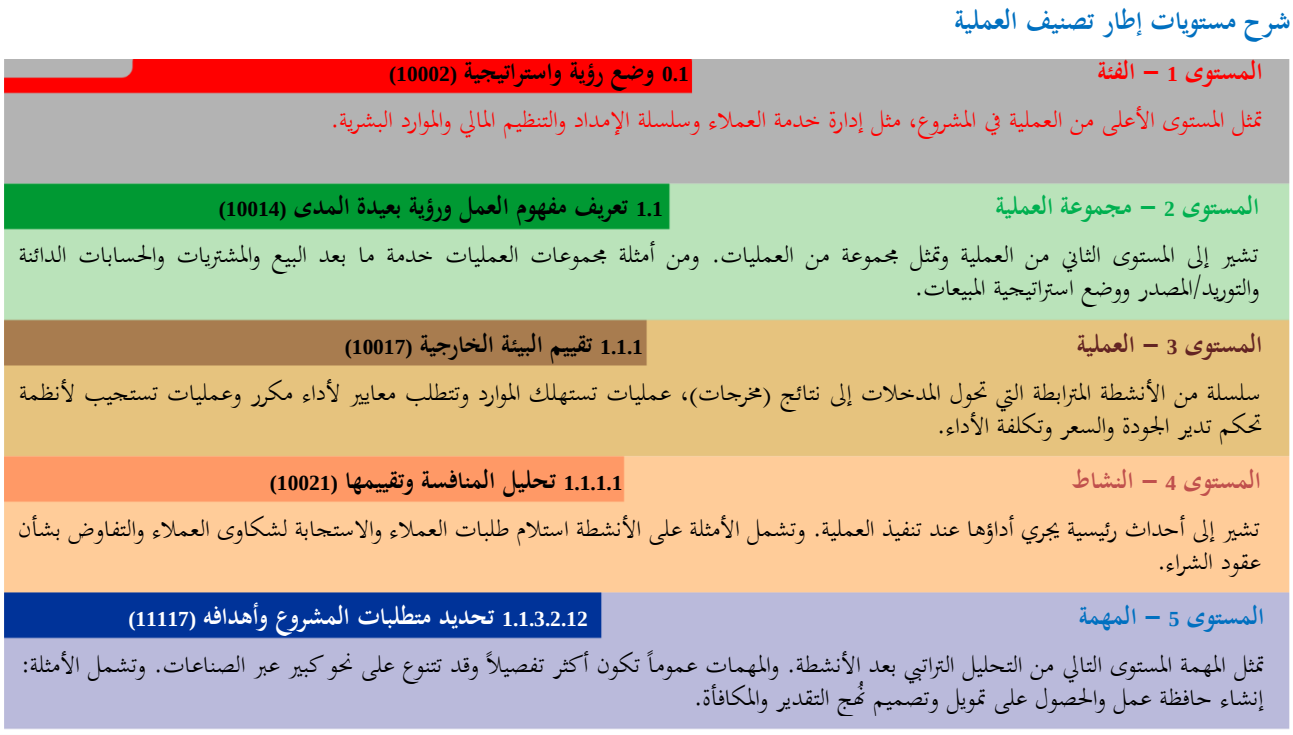
التذييل VI

معايير تصنيف عملية العمل

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

أشارت هذه التوصية على الأقل إلى نوعين من أنواع تصنيف عمل: تصنيف عملية العمل، وتصنيف منتج العمل. وقد وضعت هذين المصطلحين هيئات معنية بمعايير إدارة عملية العمل مثل خريطة عمليات الاتصالات المعززة التابعة لمنتدى إدارة الاتصالات (eTOM) والتصنيف المركزي للمنتجات ([b-CPC] (CPC)).

ويوضح المثال التالي في الشكل 1.VI إطار تصنيف عملية (PCF) من المركز الأمريكي للجودة والإنتاجية [b-APQC-PCF] (APQC) ويوضح كيف يمكن تصنيف العمليات.



X.1257(16)_FVI.1

الشكل 1.VI – تعاريف هيكل تصنيف عملية العمل المتعلقة بإطار تصنيف عملية

التذييل VII

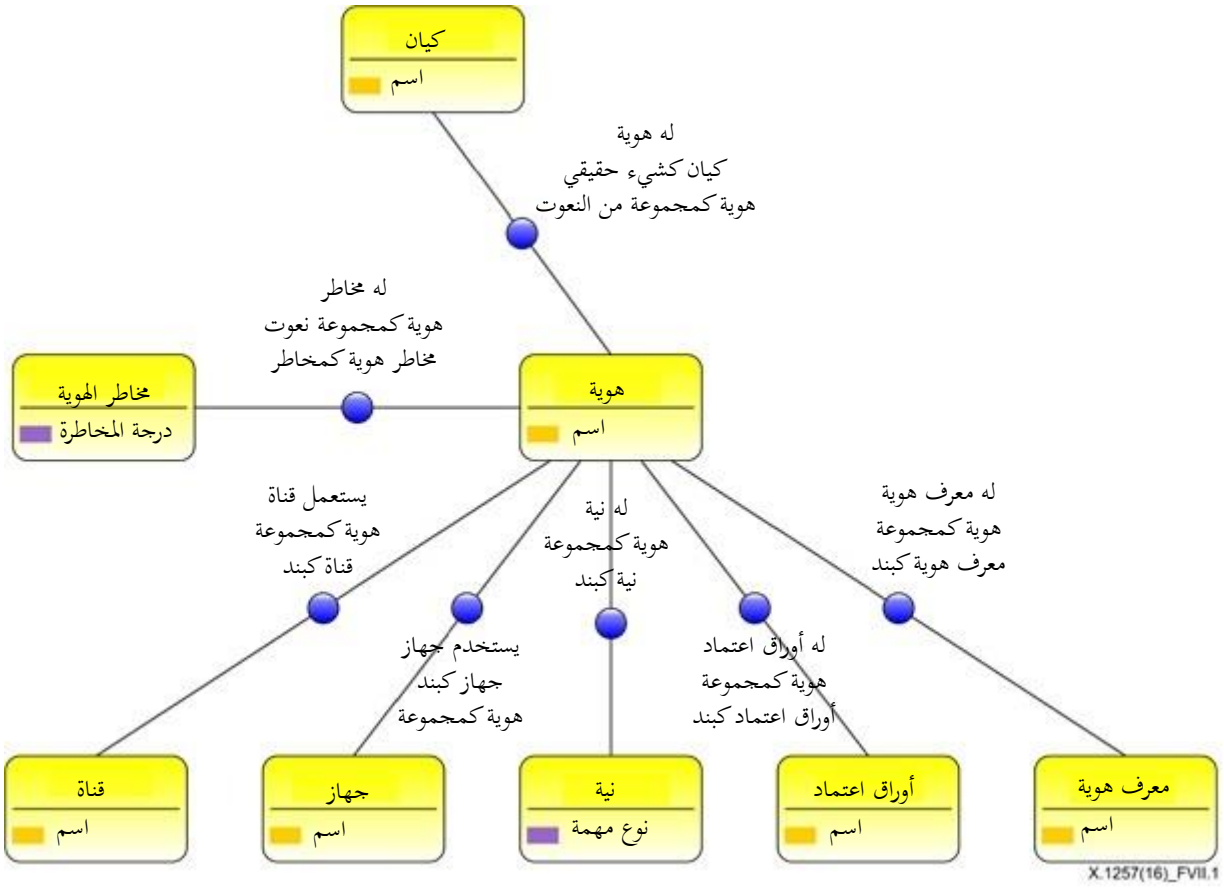
نموذج ميدان أنطولوجيا إدارة الهوية والنفاذ

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يصف الشكل 5.VII نموذج ميدان أنطولوجيا إدارة الهوية والنفاذ بكامله. وتسهيلاً على القارئ في الدخول إلى ميدان إدارة الهوية والنفاذ، قدمت أولاً المواضيع التالية المتعلقة بإدارة الهوية والنفاذ:

- الشكل 1.VII نموذج ميدان إدارة الهوية والنفاذ – موضوع المستعمل
- الشكل 2.VII نموذج ميدان إدارة الهوية والنفاذ – موضوع تخصيص النفاذ
- الشكل 3.VII نموذج ميدان إدارة الهوية والنفاذ – موضوع التحكم في النفاذ
- الشكل 4.VII نموذج ميدان إدارة الهوية والنفاذ – موضوع ميدان العمل.

وأخيراً سوف تُدمج المواضيع الواردة أعلاه في نموذج ميدان إدارة الهوية والنفاذ كله المبيّن في الشكل 5.VII. وهكذا فإن الموضوع الأول يعالج أنواع مفهوم المستعمل. ووفقاً للتوصيتين [ITU-T X.1252] و [ITU-T X.1254]، يمثل المستعمل بكيان من وجهات نظر قليلة مثل كينونة أو وجود الفرد. وللكيان هوية واحدة أو أكثر. وللهوية معرف هوية واحد أو أكثر.

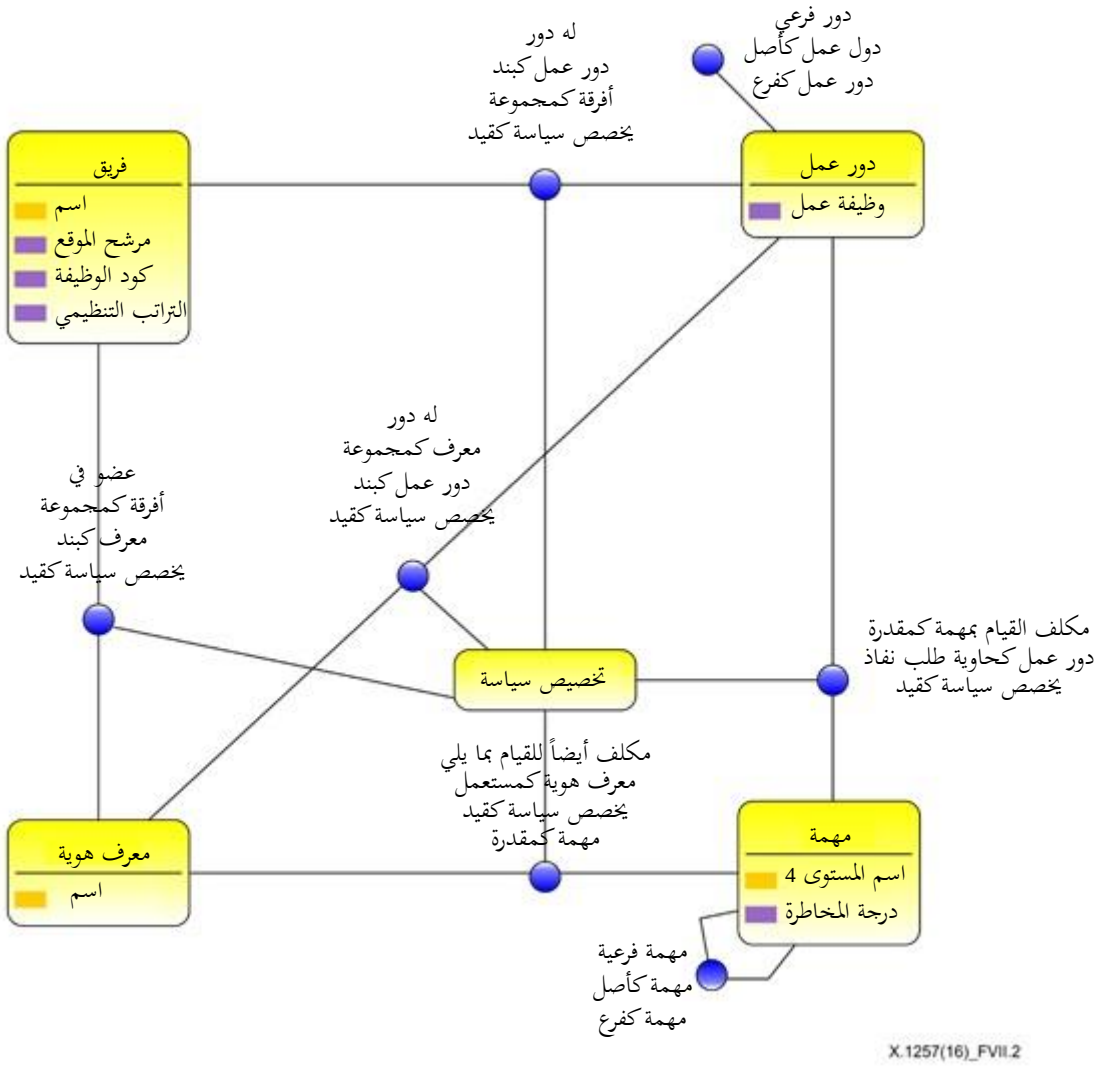


الشكل 1.VII – نموذج ميدان إدارة الهوية والنفاذ – موضوع المستعمل

مثال: للإنسان كيان يتميز بالاسم وتاريخ الولادة وما إلى ذلك. وقد يكون هذا الكائن موظفاً وعميلاً في آن واحد وبالتالي فقد يكون له هويتان على الأقل. وعليه سيكون لهذا الكائن معرّفي هوية هما هوية موظف (Employee ID) وهوية عميل (Customer ID).

ملاحظة – في بعض الحالات يمكن أن يقوم بدور الإنسان جهاز يعمل نيابة عن الإنسان.

في الشكل 2.VII يتم وصف موضوع تخصيص النفاذ. يعالج تخصيص النفاذ مع تخصيص حقوق النفاذ لمستعمل من خلال معرّف (معرّفات) هويته. ويمكن تخصيص حقوق النفاذ للمستعمل من خلال فريق (فرق) يكون هذا المستعمل عضواً فيه (فيها). والفريق في هذا السياق هو حاوية لحقوق نفاذ تديرها موارد بشرية. وبالإضافة إلى حقوق النفاذ الخاصة بعضوية الفريق يستطيع المستعمل أن يحصل على حقوق نفاذ خاصة به من خلال دور تجاري يقوم به. وأخيراً وكاستثناء يستطيع المستعمل أن يؤدي مهام عمل معينة. وفي النهاية فإن حقوق النفاذ هي مجموعة من المهام يستطيع المستعمل تأديتها. ومع ذلك يتم تقييم كل ما يقوم به المستعمل من تخصيص من خلال استحقاقات معينة قابلة للتطبيق تسمى "سياسات التخصيص" وتستبعد التوليفات المؤذية للاستحقاقات فضلاً عن إنفاذ قواعد الفصل بين الواجبات (SoD).

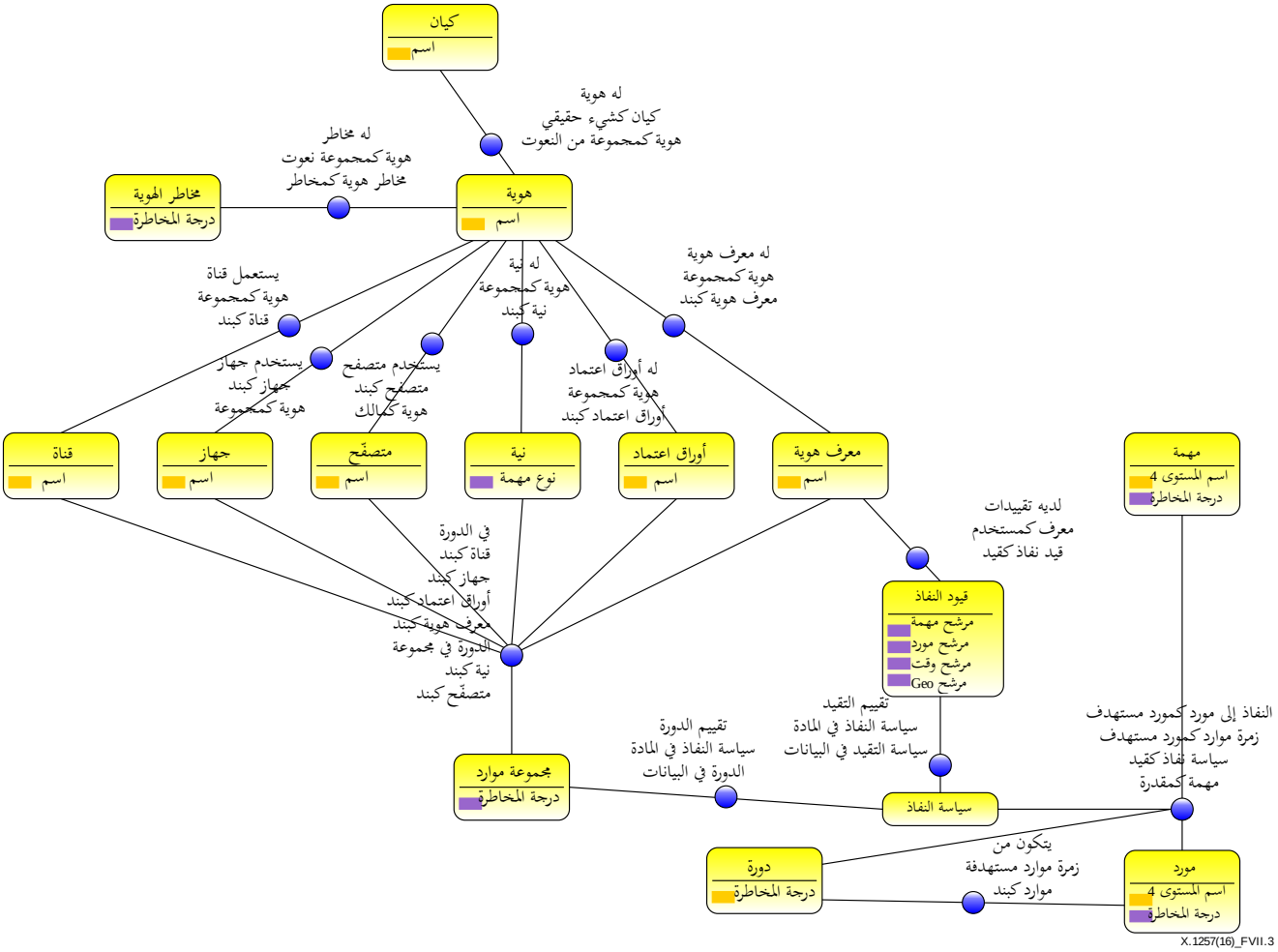


الشكل 2.VII – نموذج ميدان إدارة الهوية والنفاذ – موضوع تخصيص النفاذ

مثال: المستعمل ألف هو عضو في الفريق سين. ولكل عضو في الفريق سين موجود في الموقع الرئيسي (وأي منطقة = رئيسي، ومكتب= رئيسي) خمسة أدوار عمل ويمنح كل واحد فيها المستعمل الحق في أداء عشر مهام. وهكذا فإن كل عضو من أعضاء الفريق سين بوسعه بطبيعة الحال أن يؤدي 50 مهمة. فضلاً عن ذلك خُصصت للمستعمل ألف ثلاثة أدوار عمل إضافية تمنحه الحق في أداء خمسة مهام إضافية. كما يحق للمستعمل ألف أداء مهمة أخرى بشكل مباشر على سبيل الاستثناء. وفي المحصلة يحق

للمستعمل ألف أداء 66 مهمة منفصلة. إلا أن أعضاء الفريق غير الموجودين في المقر الرئيسي ليس لهم إلا ثلاثة أدوار عمل – أي أقل بثلاثين مهمة عمل.

الموضوع التالي – التحكم في النفاذ – تنفيذ الترخيص القائم على المهمة والسياسة استناداً إلى استحقاقات المستعمل وسياق الدورة. وتمنح مهمة معنية حق النفاذ إلى موارد بعينها إذا كانت سياسة النفاذ المناظرة تسمح بحدوث هذا النفاذ. وستقيِّم سياسة النفاذ قواعدها التي لها سياق الدورة وتقييدات نفاذ المستعمل المناظرة. وسوف يحصل سياق الدورة على البيانات الشرحية الخاصة باستيقان المستعمل مثل القناة والجهاز والقصد (النية) وأوراق الاعتماد ومعرف الهوية.

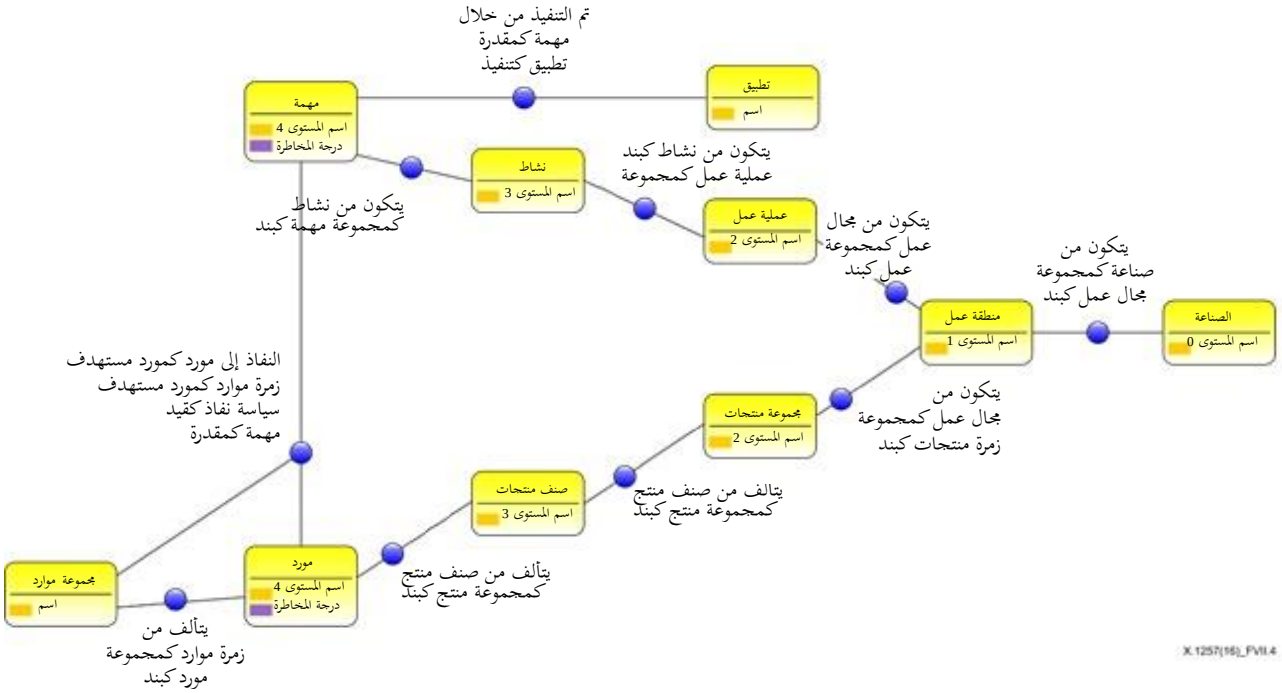


الشكل 3.VII – نموذج ميدان إدارة الهوية والنفاذ – موضوع التحكم في النفاذ

مثال: ينوي المستعمل ألف أداء مهمة "إنشاء حساب". وهذه المهمة سوف تحقق النفاذ (أي إنشاء) إلى مورد عمل "ميزة حساب جاري". ويحدث هذا النفاذ إذا كانت سياسة النفاذ المناظرة تقيّم الأمر بأنه صحيح. وستضمن سياسة النفاذ أن يستخدم مستعمل معين القناة المناسبة لهذه العملية المصرفية وأن يكون عنوان بروتوكول الإنترنت ضمن مدى صالح من عناوين بروتوكول الإنترنت. وقد تلجأ السياسة لاستشارة مخزن مؤقت للمهام غير المسموح بها في ذلك الوقت لأنه يقع بعد أوقات العمل.

ويوضح آخر موضوع، وهو موضوع تصنيف العمل، كيف أن ميدان إدارة الهوية والنفاذ وميدان العمل يترابطان. ويتألف تصنيف العمل من عمليات عمل ومنتجات. ويلاحَظ (من اليمين إلى اليسار) أن مجالات الصناعة والعمل هما أول مستويين من هذا التصنيف. ويظهر على يسار مجال العمل هيكلان تراتبيان مترابطان هما تصنيف عملية العمل وتصنيف منتج العمل. وعادةً ما تكون

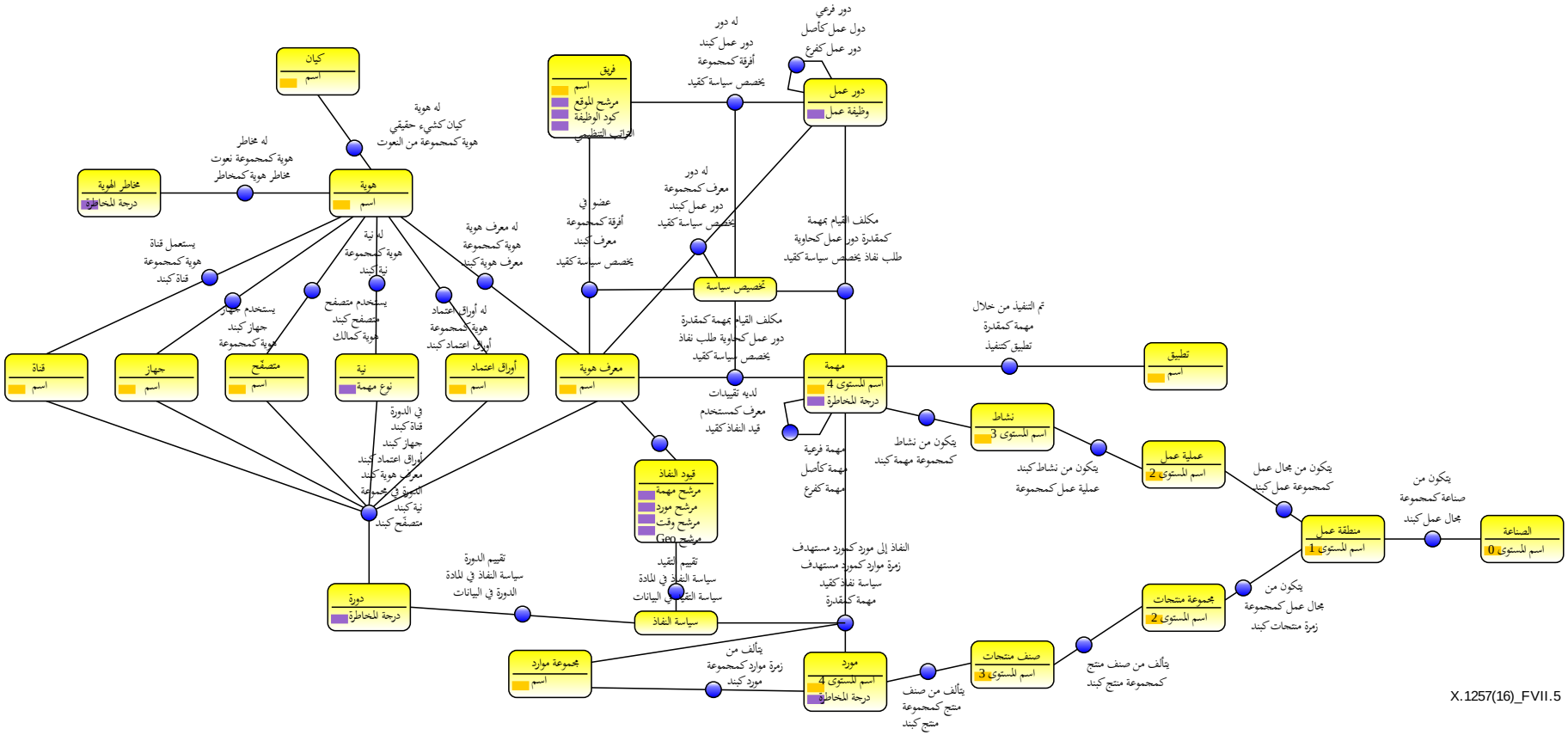
المهمة عقدة ورقية في تصنيف عملية العمل، ومورد العمل عقدة ورقية في تصنيف منتج العمل. ويقوم التطبيق بتنفيذ المهام المناظرة ويؤدي النفاذ إلى الموارد نيابة عن المستعمل.



الشكل 4.VII – نموذج ميدان إدارة الهوية والنفاذ – موضوع ميدان العمل

مثال: صناعة هي مجال مالي. ومجال العمل هو خدمة العملاء. وعملية العمل هي الإنشاء. والنشاط هو نشاط الحساب. والمهمة هي "إنشاء حساب". ومن منظور تصنيف منتج العمل فإن مجموعة العمل هي الحساب وصنف فئة المنتج هي حساب جاري، ومورد العمل هو "ميزة حساب جاري".

أخيراً فإن مجمل نموذج ميدان إدارة الهوية والنفاذ يمثله الشكل 5.VII أدناه الذي يُدمج المواضيع الأربعة المذكورة أعلاه.



الشكل 5.VII – نموذج ميدان إدارة الهوية والنفاذ

يقدم الميدان المعروض في الشكل 5.VII نموذجاً للعلاقة بين المفاهيم طبقاً للمتطلبات المنصوص عليها في القسم المناظر. ويعرض الشكل المبادئ الرئيسية التالية:

- يتمثل المستعمل بكيانه وهوياته ومعرّفات هويته، وسمات أخرى كذلك. وخلال عملية تخصيص الاستحقاقات قد يحق للمستعمل أداء مهام محددة من خلال الفريق والدور (عادةً ما تكون الحالة كذلك في 80% من الوقت) أو قد تسند له مباشرة مهام محددة (كاستثناء في 20% من الوقت).
- الفريق هو حاوية أدوار لموارد بشرية. والهدف الرئيسي للفريق وأنواع دور العمل هو الإسراع بعملية تخصيص الاستحقاقات وقبولها وتبسيطها.
- وينبغي أن تحوز أدوار العمل معنى العمل من مهمات العمل المناظرة.

ملاحظة – تقوم تكنولوجيا المعلومات الآن بإنشاء أدوار إدارة الهوية والنفاذ والحفاظ عليها، ولذلك لا تحظى بمعنى عمل مباشر قابل للتتبع. وفي حالات كثيرة فإن الاعتماد على اسم دور بمفرده لنقل معنى العمل ليس كافياً لاستعراض حقوق النفاذ على نحو ناجح.

- المهمات هي العقد الورقية لتصنيف عملية العمل ويقوم بإنشائها والحفاظ عليها مهندسو العمل وواضعو نماذج العمل.
- تكون المهمات عادة أكثر تفصيلا من التطبيقات التي تقوم بتنفيذها.
- تنفذ المهمات بواسطة التطبيق (التطبيقات) المناظر (المناظرة).
- المهمات تمثل الواجبات كما هو الحال في حالات استعمال الفصل بين الواجبات (SoD).

ملاحظة – من المستحيل تنفيذ الفصل بين الواجبات دون تحديد مهمات العمل.

- ليس لدى المستعمل نفاذ مباشر إلى موارد العمل. بل يكون للمستعمل الحق في أداء مهمة العمل وتنفُذُ مهمة العمل إلى موارد (موارد) العمل نيابة عن المستعمل.
- مهمة العملية – النشاط – المهمة هو هيكل منطقي وجزء من تصنيف عملية العمل لتحديد وتنظيم عمليات العمل بطريقة معيارية [b-APQC PCF 5.0.1] وعادةً يقوم بصيانتها مهندسو العمل وواضعو نماذج عملية العمل.
- مجموعة المنتج – صنف المنتج – مورد العمل هو هيكل منطقي وجزء من تصنيف منتج العمل لتحديد وتنظيم منتجات العمل بطريقة معيارية [b-CPC Ver 2] وعادة يقوم بصيانتها مهندسو العمل وواضعو نماذج عملية العمل.
- سياسة التخصيص هي آلية لتقييد تخصيص الاستحقاقات تستخدم خلال مرحلة تخصيص الاستحقاقات لمنع الغش والتوليفات المؤذية خلال وقت التشغيل.
- سياسة النفاذ هي آلية لتقييد عمليات النفاذ تستخدم خلال وقت تشغيل مرحلة النفاذ لمنع الغش والتوليفات المؤذية خلال وقت التشغيل.
- موارد العمل هي مفاهيم مثل سجلات المرضى وحساب القروض والحسابات الجارية. وهي تسمح بتخصيص استحقاقات ذي مستوى موارد دقيقة التفاصيل والتحكم في النفاذ.
- استحقاقات العمل هي مهمة (مهمات) يحق للمستعمل في أدائها (مثل استحقاقات العمل غير المفصلة).
- تصاريح العمل هي مهمة (مهمات) تنفذ إلى موارد عمل محددة وتقيدها سياسة.
- خلال توفير استحقاقات المستعمل يمكن وضع تقابل بين استحقاقات العمل وتصاريح نظام مناظر إذا لزم الأمر.
- تتعامل تصاريح النظام مع موارد النظام مثل قواعد البيانات أو الجداول أو الأعمدة أو الملفات أو مجموعة بيانات الحاسوب المركزي.

بيبليوغرافيا

[b-ITU-T X.1255] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information.*

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2011, *Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts.*

[b-Antonie] Antoine Isaac, E. S. (2009, August 18). *SKOS simple knowledge organization system primer*. http://www.w3.org/TR/skos-primer/ (Retrieved May 18, 2016)

[b-APQC-PCF] Tesmer, John (2014, March), *Process Classification Framework 6.1.1*. http://www.apqc.org/process-classification-framework (Retrieved May 18, 2016)

[b-APQC PCF 5.0.1] APQC PCF. (2011, June), *Banking Process Classification Framework*. http://www.apqc.org/knowledge-base/download/33193/ PCF_Banking_Ver_5.0.1_2011.pdf (Retrieved May 18, 2016)

[b-CPC] http://en.wikipedia.org/wiki/Central_Product_Classification.

[b-CPC Ver 2] CPC Workgroup. (2008, December 31), *Central Product Classification, Ver.2, Detailed structure and explanatory notes*. http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=25 (Retrieved May 18, 2016)

[b-example] http://www.apqc.org/knowledge-base/documents/apqc-process-classification-framework-pcf-banking-excel-version-501

[b-IETF SCIM 1.0] C. Mortimore, Ed. (2013, April 15), *System for Cross-Domain Identity Management: Core Schema*. http://tools.ietf.org/html/draft-ietf-scim-core-schema-01 (Retrieved May 18, 2016)

[b-IETF SCIM 2.0] Hunt, e. a. (2015, June 8), *System for Cross-Domain Identity Management: Core Schema*. https://tools.ietf.org/html/draft-ietf-scim-core-schema-22 (Retrieved May 18, 2016)

[b-NIST-RBAC 2000] Sandhu, R., David, F., & Khun, R. (2000), *The NIST Model for Role-Based Access Control: Towards A Unified Standard*.

[b-OASIS XACML 3.0] Erik Rissanen. (2013, January 22), *eXtensible Access Control Markup Language (XACML) Version 3.0*. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html (Retrieved May 18, 2016)

[b-OBAC] Mohammad, A. (2011, March 7). *Ontology-Based Access Control Model for Semantic Web*. http://www.worldacademicunion.com/journal/1746-7659JIC/ jicvol6no3paper03.pdf (Retrieved May 18, 2016)

[b-schema.org 2011] Google, Yahoo, Bing, Yandex. (2011). *schema.org*. http://schema.org (Retrieved May 18, 2016)

[b-SCIM REST] SCIM 2.0 REST web service protocol, C. Mortimore, Ed., 2013; http://www.simplecloud.info/ (Retrieved May 18, 2016)

Role[b-W3C JSON-LD] Manu Sporny. (2013, August 6), *JSON-LD 1.0, A JSON-based Serialization for Linked Data*. http://json-ld.org/spec/latest/json-ld/ (Retrieved May 18, 2016)

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

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

طُبعت في سويسرا
جنيف، 2016