Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1257

(03/2016)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberespace – Gestion des identités

Taxonomie de la gestion d'identité et d'accès

Recommandation UIT-T X.1257

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	**X.1250–X.1279**
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
Recommandations relatives aux infrastructures de clé publique	X.1340–X.1349
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1257

Taxonomie de la gestion d'identité et d'accès

Résumé

La Recommandation UIT-T X.1257 présente des spécifications qui visent à faire en sorte que la signification opérationnelle nécessaire soit assignée aux rôles et aux permissions de gestion d'identité et d'accès (IAM) et que cette signification opérationnelle puisse être tracée et référencée tout au long du cycle de vie des processus IAM, autrement dit que des permissions puissent être assignées efficacement aux utilisateurs, que des contrôles liés à la séparation des fonctions (SoD) puissent être mis en oeuvre avec succès dans différentes applications, et que des processus d'examen et d'actualisation d'accès puissent être effectués d'une manière efficace.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T X.1257	2016-03-23	17	11.1002/1000/12608

Mots clés

Gestion d'accès, cycle de vie IAM, gestion d'identité et d'accès, rôle, permission, signification opérationnelle, taxonomie opérationnelle, tâche opérationnelle.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1257

Taxonomie de la gestion d'identité et d'accès

1 Domaine d'application

La présente Recommandation décrit les exigences relatives à l'assignation d'une signification opérationnelle aux rôles et aux permissions utilisateur de gestion d'identité et d'accès (IAM). Elle se base sur les Recommandations [UIT-T X.1252], [UIT-T X.1254] et [b-UIT-T X.1255], et en étend la portée, pour proposer:

- une taxonomie IAM qui vise à identifier et à organiser sur le plan sémantique les phases et les processus IAM, afin de représenter un cycle de vie complet des processus IAM;
- un modèle ontologique IAM qui vise à identifier sur le plan sémantique les types de rôle et de permission IAM, leur syntaxe ainsi que les relations de type correspondantes.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T X.1252] Recommandation UIT-T X.1252 (2010), Termes et définitions de base relatifs à la gestion d'identité.

[UIT-T X.1254] Recommandation UIT-T X.1254 (2012), Cadre de garantie d'authentification des entités.

3 Définitions

3.1 Termes définis dans d'autres documents

3.1.1 contrôle d'accès (*access control*) [UIT-T X.1252]: Procédure utilisée pour déterminer si l'accès à des ressources, fonctionnalités, services ou informations devrait être accordé à une entité, compte tenu des règles préétablies et des droits spécifiques ou de l'autorité associés à l'entité requérante.

3.1.2 attribut (*attribute*) [UIT-T X.1252]: Information liée à une entité qui en spécifie une caractéristique.

3.1.3 contexte (*context*) [UIT-T X.1252]: Environnement avec des frontières définies dans lequel des entités existent et interagissent.

3.1.4 justificatif (*credential*) [UIT-T X.1252]: Ensemble de données présentées comme preuve d'une identité déclarée et/ou de crédits.

3.1.5 entité (*entity*) [UIT-T X.1252]: Elément qui a une existence séparée et distincte et peut être identifié dans un contexte.

3.1.6 identifiant (*identifier*) [UIT-T X.1254]: Un ou plusieurs attributs utilisés pour identifier une entité dans un contexte particulier.

3.1.7 identité (*identity*) [b-ISO/IEC 24760-1]: Ensemble d'attributs se rapportant à une entité.

NOTE – Dans un contexte particulier, une identité peut avoir un ou plusieurs identifiants, pour permettre à une entité d'être reconnue de façon unique dans ce contexte.

3.1.8 rôle (*role*) [UIT-T X.1252]: Ensemble de propriétés ou d'attributs qui décrivent les capacités ou les fonctions d'une entité.

NOTE – Chaque entité peut avoir/jouer de nombreux rôles. Ses capacités peuvent lui être propres ou lui être attribuées.

3.1.9 utilisateur (*user*) [UIT-T X.1252]: Toute entité qui utilise une ressource, par exemple un système, un équipement, un terminal, un processus, une application ou un réseau d'entreprise.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 assignation d'accès (*access assignment*): Processus consistant à assigner des droits d'accès à un ou plusieurs utilisateurs.

3.2.2 gestion des demandes de modification de l'accès (*access change request management*): Processus destiné à gérer les demandes de modification de l'accès.

3.2.3 contraintes d'accès (*access constraints*): Ensemble de contraintes d'accès basé sur la position de l'utilisateur et sur les tâches et les ressources qui font l'objet d'une restriction temporaire.

3.2.4 ingénierie d'accès (*access engineering*): Processus de création et de maintenance des droits d'accès.

3.2.5 opération d'accès (*access operation*): Processus consistant à évaluer les droits d'accès d'un utilisateur en vue de l'exécution de certaines tâches opérationnelles.

3.2.6 politique d'accès (*access policy*): Mécanisme de restriction lié au contrôle d'accès (c'est-à-dire: quelles permissions opérationnelles un utilisateur peut exercer lors de l'exécution).

3.2.7 actualisation d'accès (*access reconciliation*): Processus consistant à modifier les droits d'accès d'un utilisateur en fonction des exigences formulées en matière de droits d'accès, afin d'éviter que cet utilisateur ait trop (ou trop peu) de privilèges en termes d'accès.

3.2.8 examen d'accès (*access review*): Processus consistant à examiner les droits d'accès des utilisateurs, dans l'optique d'une actualisation et d'une certification ultérieures de l'accès.

3.2.9 politique d'assignation (*assign policy*): Mécanisme de restriction de l'attribution des permissions (c'est-à-dire: quelles tâches peuvent être assignées à un utilisateur).

3.2.10 ingénierie de logique d'autorisation (*authorization logic engineering*): Processus d'élaboration et de maintenance d'une logique d'autorisation dans différentes applications connexes.

3.2.11 navigateur (*browser*): Application exécutée sur un dispositif et utilisée par les utilisateurs pour interagir avec un fournisseur de services.

3.2.12 rôle opérationnel (*business role*): Ensemble de tâches (avec ou sans permissions) qu'un utilisateur peut être habilité à exécuter.

3.2.13 enregistrement d'accès à des tâches opérationnelles (*business task access logging*): Processus d'enregistrement de l'exécution réussie d'une tâche ou du refus fait à un utilisateur d'effectuer une certaine tâche.

3.2.14 autorisation d'exécution de tâche opérationnelle (*business task execution authorization*): Processus consistant à autoriser un utilisateur à effectuer une tâche opérationnelle particulière sur une ressource particulière.

3.2.15 exécution de tâche opérationnelle (*business task execution*): Processus d'exécution d'une tâche opérationnelle particulière.

3.2.16 ingénierie de taxonomie opérationnelle (*business taxonomy engineering*): Processus de création et de maintenance d'une taxonomie de processus opérationnels et de produits opérationnels.

3.2.17 taxonomie de processus opérationnels (*business process taxonomy*): Taxonomie qui a pour objet d'identifier les processus et sous-processus opérationnels sur le plan sémantique et à les organiser dans une structure hiérarchique.

3.2.18 canal (*channel*): Méthode de communication choisie par un utilisateur pour interagir avec un fournisseur de services.

3.2.19 dispositif (*device*): Mécanisme utilisé par un utilisateur pour assurer l'interaction avec un fournisseur de services.

3.2.20 crédit (*entitlement*): Ensemble de tâches et de permissions assignées à un utilisateur.

3.2.21 cycle de vie des processus IAM (*IAM process lifecycle*): Cycle de vie des processus et des sous-processus de gestion d'identité et d'accès (IAM).

3.2.22 ingénierie de rôles IAM (*IAM role engineering*): Processus de création et de maintenance des rôles et des permissions IAM.

3.2.23 finalité (*intent*): Raison ou but qui conduit un utilisateur à engager l'interaction avec un fournisseur de services.

3.2.24 permission (*permission*): Ensemble de tâches qui accèdent à des ressources opérationnelles, sous réserve des politiques de contrôle d'accès correspondantes.

3.2.25 ressource (*resource*): Noeud feuille d'une taxonomie de produits opérationnels, également appelé produit opérationnel.

3.2.26 session (*session*): Ensemble comprenant une authentification d'exécution et des attributs d'autorisation.

3.2.27 tâche (*task*): Noeud feuille d'une taxonomie de processus opérationnels, également appelé tâche opérationnelle.

3.2.28 équipe (*team*): Ensemble lié aux ressources humaines qui comprend les rôles opérationnels que chaque membre de l'équipe a en commun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

APQC American Productivity and Quality Center

CPC classification centrale de produits (*central product classification*)

eTOM plan amélioré d'exploitation des télécommunications (*enhanced telecom operations map*)

HTTP protocole de transfert hypertexte (*hypertext transfer protocol*)

IAM gestion d'identité et d'accès (*identity and access management*)

IP protocole Internet (*Internet protocol*)

IT technologies de l'information (*information technology*)

JSON notation des objets du langage Java (*JavaScript object notation*)

JSON-LD sérialisation JSON pour les données liées (*JSON-based serialization for linked data*)

MAC commande d'accès au support (*media access control*)

PCF cadre de classification des processus (*process classification framework*)

RBAC contrôle d'accès basé sur les rôles (*role-based access control*)

REST transfert d'état représentationnel (*representational state transfer*)

SCIM système de gestion d'identité interdomaine (*system for cross-domain identity management*)

SDLC cycle de développement d'un logiciel (*software development life cycle*)

SKOS système simple d'organisation des connaissances (*simple knowledge organization system*)

SOAP protocole simple d'accès aux objets (*simple object access protocol*)

SoD Séparation des fonctions (*separation of duties*)

URL localisateur uniforme de ressources (*uniform resource locator*)

XACML langage de balisage extensible de contrôle d'accès (*extensible access control markup language*)

5 Conventions

Les conventions suivantes sont utilisées dans la présente Recommandation:

Des mots dont la première lettre est en majuscule à l'intérieur d'une phrase, par exemple "Rôle Opérationnel" ou "Ingénierie de Rôles IAM", indiquent l'emploi d'un terme qui fait partie d'un modèle (c'est-à-dire modèle ontologique IAM ou modèle taxonomique IAM). Cet usage des majuscules est aussi valable dans les diagrammes correspondants. Par ailleurs, dans un souci de lisibilité, les termes "tâche opérationnelle" et "tâche" sont utilisés de manière interchangeable, de même que les termes "ressource opérationnelle" et "ressource".

6 Introduction

Le manque de signification opérationnelle des rôles et des permissions utilisateur de gestion d'identité et d'accès (IAM) actuels a des incidences négatives sur tout le cycle de vie IAM. Bien que des rôles tels que "SuperAdmin", "SuperUpdate" ou "XYZSystemSpecialAccess" soient ambigus, excessivement techniques et peu explicites, ils sont courants dans de nombreuses entreprises. Naturellement, plutôt que de réutiliser des rôles aussi ambigus, un ingénieur de rôles IAM préférera créer sans cesse de nouveaux rôles. Toutefois, cette pratique finit par conduire à l'existence d'un grand nombre de rôles IAM propres au système et difficiles à gérer, qui ne véhiculent pas la signification opérationnelle souhaitée.

L'existence d'un si grand nombre de rôles ainsi que leur qualité médiocre sur le plan sémantique ont des incidences négatives sur des étapes clés du cycle de vie IAM, telles que l'Assignation d'Accès, l'Autorisation d'Accès, l'Examen d'accès et l'Actualisation d'Accès. Lors de l'Assignation d'Accès, un spécialiste de la gestion d'accès qui ne comprendrait pas la signification des rôles existants pourrait attribuer des privilèges erronés à un utilisateur. Pour compenser le manque de signification opérationnelle des rôles IAM, les développeurs d'applications sont contraints de recourir au codage en dur pour incorporer une logique d'autorisation dans leurs applications. La maintenance de ce type de code source de logique d'autorisation d'une manière synchronisée entre différentes applications est difficile et susceptible d'erreurs. En outre, il est difficile (sinon impossible) de mettre en oeuvre des

contrôles de Séparation des Fonctions (SoD) dans un grand nombre d'applications à la fois. Lors de l'Examen d'accès, en raison du même manque de signification opérationnelle des rôles IAM, ainsi que de la pression liée à la nécessité de respecter des délais de conformité, les responsables de l'examen d'accès certifient (ou révoquent) des droits d'accès d'utilisateur d'une manière erronée. Un taux d'erreurs élevé dans l'examen d'accès et la mise en oeuvre d'une logique d'autorisation susceptible d'erreurs augmentent le risque de mauvaise publicité et de pertes financières, soulèvent des préoccupations sur le plan réglementaire, nuisent à la productivité de l'équipe chargée des opérations IAM, et limitent la capacité de fournir des solutions d'entreprise à grande échelle, comme la rationalisation des processus, des applications et des rôles.

Dans la mesure où les spécifications normalisées actuelles en matière de contrôle d'accès ne définissent pas la sémantique des rôles et des permissions IAM, il est nécessaire de spécifier un ensemble complémentaire d'exigences relatives à la gestion d'accès. Ces exigences permettraient de faire en sorte que la signification opérationnelle nécessaire soit assignée aux rôles et aux permissions IAM et que cette signification opérationnelle puisse être tracée et référencée tout au long du cycle de vie des processus IAM, de sorte que des permissions puissent être assignées efficacement aux utilisateurs, que des contrôles liés à la séparation des fonctions (SoD) puissent être mis en oeuvre avec succès dans différentes applications, et que des processus d'examen et d'actualisation d'accès puissent être effectués d'une manière efficace.

7 Présentation de l'approche

En vue de remplir l'objet de la présente Recommandation, qui est d'élaborer un ensemble d'exigences relatives à l'assignation d'une signification opérationnelle aux rôles IAM, l'approche décrite en détail ci-après a été adoptée. Comme indiqué au paragraphe 6, une équipe d'ingénierie de rôles IAM doit assigner la signification opérationnelle nécessaire aux nouveaux rôles IAM. Mais d'où proviendrait cette signification opérationnelle et qui peut la produire? Aujourd'hui, les architectes opérationnels reçoivent une stratégie opérationnelle et sont chargés d'élaborer une taxonomie de processus opérationnels et une taxonomie de produits opérationnels.

Une taxonomie de processus opérationnels identifie les processus et sous-processus opérationnels sur le plan sémantique et les organise dans une structure hiérarchique (aux fins de la navigation dans le répertoire des processus) qui commence par le Secteur, à sa racine, et se décompose en Secteur Opérationnel, Processus Opérationnel, Action Opérationnelle et Tâches Opérationnelles. (Pour de plus amples informations, voir l'Appendice VI – Normes relatives à la taxonomie de processus opérationnels.) Une taxonomie opérationnelle devrait aussi comporter une hiérarchie de produits opérationnels, et sa maintenance est généralement assurée par des architectes de produits opérationnels dans une grande feuille de calcul ou un fichier de document.

Au cours du cycle de développement d'un logiciel (SDLC), des fragments d'une structure hiérarchique de ce type sont copiés et collés par des analystes opérationnels, afin d'élaborer des documents relatifs aux exigences opérationnelles qui sont remis à l'équipe d'ingénierie de rôles IAM ainsi qu'à l'équipe de développement d'applications à des fins de mise en oeuvre. Etant donné qu'un ingénieur de rôles IAM ne peut pas référencer des tâches opérationnelles particulières à l'aide de leur identifiant, il crée généralement des rôles IAM, avec ou sans définition, en fonction de son interprétation des tâches opérationnelles qu'un utilisateur peut effectuer, interprétation qui se base sur des informations non actualisées. Au bout du compte, la signification opérationnelle du rôle IAM est perdue ou mal interprétée par le développeur d'applications. Comment ce problème peut-il être résolu?

Pour résoudre ce problème, il convient de faire en sorte que la signification opérationnelle des rôles IAM puisse être référencée et tracée par rapport aux tâches opérationnelles correspondantes en cours tout au long du cycle de vie des processus IAM. C'est là la caractéristique qualité fondamentale qui peut permettre d'améliorer la qualité de l'ensemble du cycle de vie des processus IAM. Comment

cette caractéristique qualité peut-elle être mise en oeuvre? Il existe un certain nombre d'approches en matière de représentation sémantique pour ce qui est de mettre en oeuvre une interface de programmation d'applications relative à une taxonomie opérationnelle. (Voir l'Appendice V – Mécanismes envisageables pour la mise en oeuvre d'une interface de taxonomie opérationnelle.)

Cependant, il ne suffit pas de pouvoir référencer et tracer la signification opérationnelle tout au long du cycle de vie des processus IAM. Il est de plus nécessaire de spécifier une syntaxe sémantique pour les rôles IAM.

Actuellement, la syntaxe relative aux rôles IAM est spécifiée par un mécanisme de contrôle d'accès normalisé couramment utilisé, appelé Contrôle d'Accès Basé sur les Rôles (RBAC) et représenté dans la Figure 1.

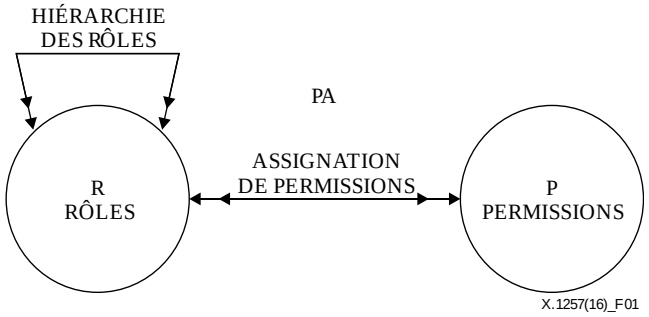

Figure 1 – Modèle classique de contrôle RBAC

On observe la syntaxe de rôles suivante:

- Les rôles peuvent contenir d'autres rôles, c'est-à-dire former une hiérarchie de rôles.
- Les rôles sont constitués de permissions.

Ce mécanisme classique de contrôle RBAC présente toutefois une limite connue: il ne spécifie pas la sémantique des permissions (c'est-à-dire la "nature des permissions"). Au lieu de cela, la spécification indique que la sémantique des permissions est laissée ouverte à l'interprétation: "les permissions peuvent être définies en termes d'opérations primitives telles que lire et écrire, ou d'opérations abstraites, telles que crédit et débit" [b-NIST-RBAC 2000]. Toutefois, dans la pratique, comme cela est expliqué au paragraphe 6, des rôles IAM ambigus sont créés sans qu'il soit fait référence aux tâches opérationnelles correspondantes.

Afin d'assigner une signification opérationnelle aux rôles IAM, il est nécessaire de spécifier une syntaxe sémantique pour les rôles IAM. La signification devrait provenir des noeuds feuilles les plus granulaires de la taxonomie opérationnelle: les tâches et les ressources. La Figure 2 décrit la syntaxe sémantique des rôles IAM.

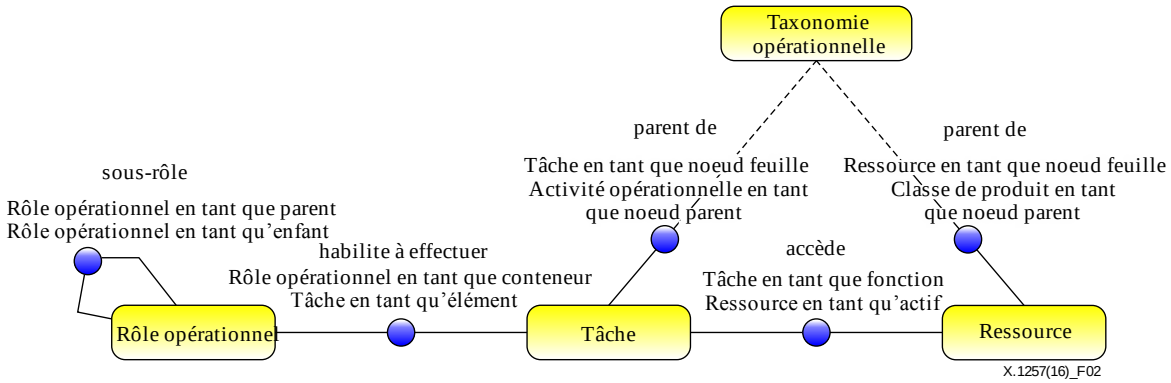

Figure 2 – Gestion d'accès basée sur les tâches: diagramme conceptuel

On observe ce qui suit:

- Les rôles peuvent (encore) contenir d'autres rôles, par l'intermédiaire d'une relation "sous-rôle", c'est-à-dire qu'ils forment une hiérarchie de rôles.
- Syntaxe sémantique fondamentale des rôles IAM:
  - Un rôle opérationnel habilite un utilisateur à effectuer des tâches opérationnelles par l'intermédiaire d'une relation "habilite à effectuer". Tout rôle opérationnel peut ainsi hériter implicitement sa signification opérationnelle des tâches opérationnelles correspondantes.
  - Une tâche opérationnelle (pas l'utilisateur ou le rôle) accède à une ressource particulière (c'est-à-dire un "Produit Opérationnel"). La relation "accède" est optionnelle et nécessaire dans les cas où un contrôle d'accès plus granulaire est requis.
  - Les tâches et les ressources en tant que noeuds feuilles de la taxonomie opérationnelle servent de blocs élémentaires de privilèges pendant l'ingénierie de rôles IAM et sont référencées tout au long du cycle de vie des processus IAM.

Par souci de simplicité, les types parents de tâche et de ressource (produit) n'apparaissent pas dans la Figure 2.

A titre d'illustration en ce qui concerne la syntaxe ci-dessus, le Tableau 1 présente quelques exemples de crédits:

Tableau 1 – Exemples de crédits

Rôle opérationnel	Tâche	Ressource
Caissier	Créer un compte	Compte chèque évolué
Médecin	Examiner les antécédents du patient	Antécédents du patient
Administrateur système	Mettre à jour l'environnement système	Environnement système

Cette syntaxe sémantique relative aux rôles IAM permettra d'atteindre l'objectif principal, qui est d'assigner une signification opérationnelle aux rôles IAM. La section suivante décrit l'approche proposée en termes d'exigences.

8 Exigences relatives à la sémantique et à la syntaxe des rôles IAM

Les recommandations formulées ci-après visent à faire en sorte que les rôles IAM aient la signification opérationnelle nécessaire:

1) La taxonomie opérationnelle sert de prérequis au cycle de vie des processus IAM afin d'assigner une signification opérationnelle aux rôles et aux permissions utilisateur IAM tout au long du cycle de vie.

2) La signification opérationnelle des rôles IAM peut être référencée et tracée par rapport aux tâches opérationnelles correspondantes de la taxonomie opérationnelle tout au long du cycle de vie des processus IAM.

3) Les rôles IAM devraient respecter la syntaxe sémantique suivante:

   3.1) Un rôle IAM est composé des tâches opérationnelles qu'un utilisateur est habilité à effectuer.

   3.2) Un rôle IAM est composé de tâches opérationnelles qui peuvent, à titre optionnel, accéder à des ressources opérationnelles spécifiques, si un contrôle d'accès plus granulaire est nécessaire.

4) L'exécution réussie de tâches opérationnelles ainsi que le refus de demandes d'exécution de tâches opérationnelles doivent être enregistrés en se référant aux identifiants des tâches opérationnelles correspondantes.

Annexe A

(Cette Annexe fait partie intégrante de la présente Recommandation.)

Cette annexe est laissée vide. Elle est destinée à décrire d'éventuels futurs scénarios de mise en oeuvre de la Gestion d'Accès Basée sur les Tâches.

Appendice I

Taxonomie et cycle de vie des processus IAM

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

La Figure I.1 met en évidence le fait que la totalité du cycle de vie des processus IAM est d'abord influencée par des changements provenant de la taxonomie opérationnelle. Ces modifications de la taxonomie opérationnelle seraient prises en compte et reflétées par les équipes d'Ingénierie de Rôles IAM et de Logique d'Autorisation. Elles comporteraient des identifiants de Tâches Opérationnelles dans les artefacts correspondants, tels que les rôles IAM, le code source de Logique d'Autorisation, et les fichiers journaux d'exécution et d'autorisation de Tâches Opérationnelles.

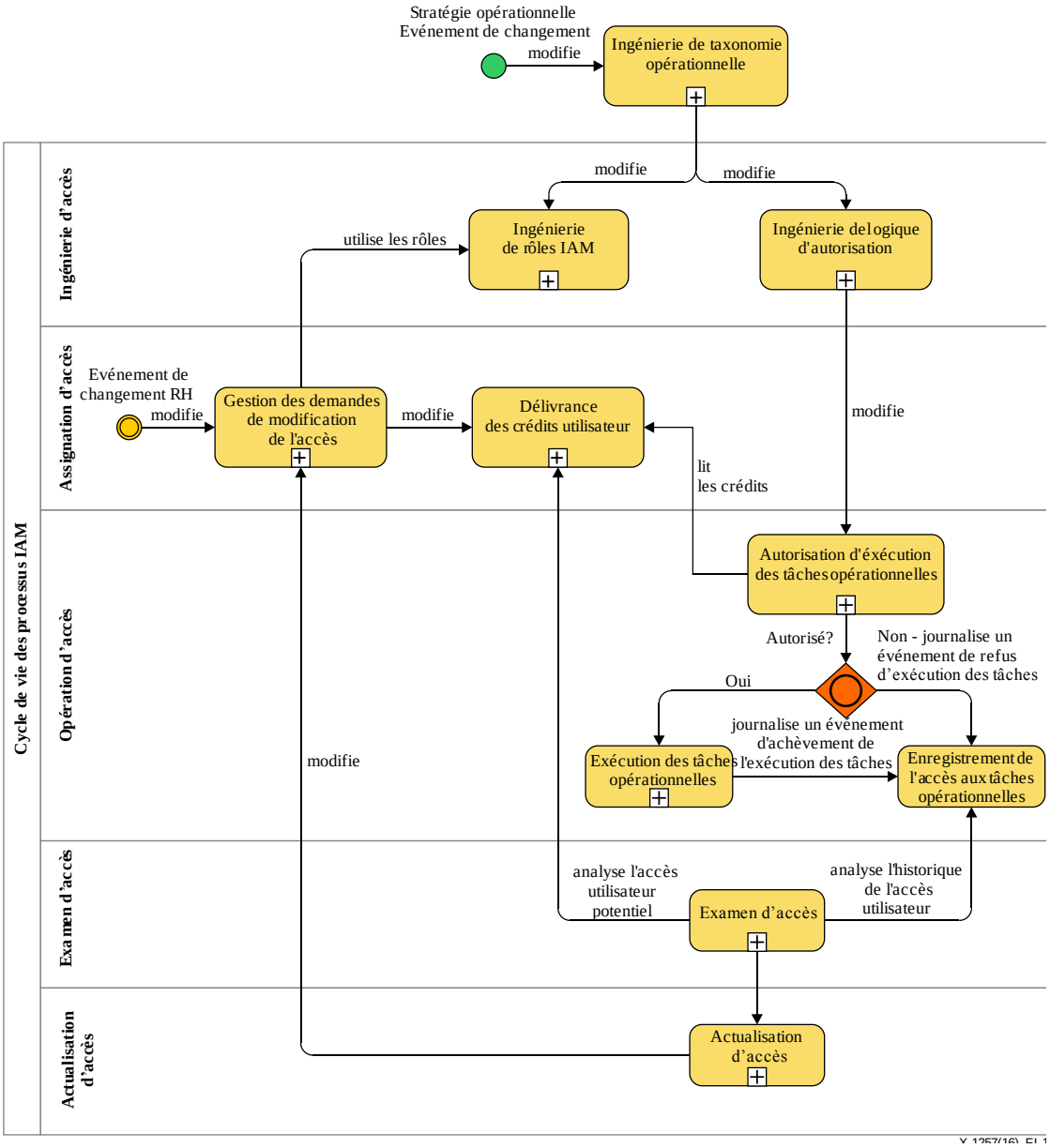

Figure I.1 – Relations de dépendance du cycle de vie des processus IAM

La deuxième source de changements se situe au niveau des événements relatifs aux ressources humaines, tels que: "recrutement", "en congé", "déplacement" et autres événements de ce type. Ces événements sont traités par le processus de Gestion des Demandes de Modification de l'Accès, et les crédits d'utilisateur correspondants seraient inscrits dans les répertoires de crédits utilisateur. Point important, ces crédits contiendraient des références par identifiant aux tâches opérationnelles apportant une signification opérationnelle, et seraient ensuite référencés lors de l'autorisation d'exécution des applications. Une fois l'utilisateur authentifié (processus non présenté par souci de simplicité), des contrôles préventifs de SoD bloqueraient l'exécution de tâches opérationnelles conflictuelles pendant l'autorisation d'exécution. Lors du processus d'Autorisation d'Exécution de Tâche Opérationnelle, un utilisateur est soit autorisé à effectuer une tâche, auquel cas celle-ci est exécutée, soit non autorisé à effectuer une tâche. Dans les deux cas, l'application enregistrerait ces événements en se référant aux identifiants des tâches opérationnelles correspondantes. Voici un exemple possible de format d'enregistrement:

```
2016-02-08 22:20:02,165 ait:AppID1 192.168.0.1 UserID123 btt:TaskID1 btr:456:355 bttes:200 "Task successfully completed."
```

```
2016-02-08 22:24:02,165 ait:AppID1 192.168.0.1 UserID123 btt:TaskID2 bttes:401 "User Not Authorized to execute Task"
```

où:

- **btt** – est un nom d'espace de nommage qui se résout sous la forme d'un préfixe HTTP URL, tel que: **http://example.com/mylob/businesstaxonomy/task/**.
- **btt:TaskID1** – est un identifiant de tâche opérationnelle. Lorsqu'un identifiant de tâche opérationnelle est accolé à un espace de nommage **btt**, il peut être utilisé afin d'obtenir des informations supplémentaires concernant la tâche opérationnelle, telles que le nom de la tâche, la description de la tâche et les statistiques relatives à l'utilisation de la tâche.
- **bttes** – est un nom d'espace de nommage qui se résout sous la forme d'un préfixe HTTP URL, tel que: **http://example.com/mylob/businesstaxonomy/task/execution/state**
- **bttes:200** – est un code d'état d'exécution des tâches qui indique l'exécution réussie d'une tâche.
- **bttes:401** – est un code d'état d'exécution des tâches qui indique le refus de l'exécution d'une tâche.

Dans la mesure où les tâches opérationnelles font l'objet d'un référencement sémantique dans les fichiers journaux, l'examinateur d'accès pourrait analyser l'historique de l'accès utilisateur ainsi que l'accès utilisateur potentiel en termes d'exécution de tâches opérationnelles. Une fois l'accès utilisateur entièrement analysé et examiné, les actualisations correspondantes sont renvoyées à la Gestion des Demandes de Modification de l'Accès, afin qu'il soit procédé, le cas échéant, à la correction de droits d'accès d'utilisateur donnant trop (ou trop peu) de privilèges. Ces actualisations constituent un mécanisme de bouclage important qui caractérise tout processus en tant que cycle de vie – à savoir un cycle de vie de processus IAM. Cependant, toutes les phases ne seraient pas nécessaires pour les petites et moyennes entreprises. Par exemple, l'Ingénierie de Logique d'Autorisation des Applications est laissée de côté ou mise en oeuvre par une composante de répertoire d'utilisateur. La Figure I.1 représente uniquement les parties essentielles de l'ensemble du cycle de vie des processus IAM.

La liste à puces hiérarchisée suivante est une représentation textuelle du Cycle de vie des Processus IAM. Chaque noeud de taxonomie est également défini au paragraphe 3.2. Pour une représentation codifiée, veuillez vous reporter au schéma du Système Simple d'Organisation des Connaissances (SKOS) [b-Antonie].

1 Gestion des Modifications Opérationnelles
- 1.1 Ingénierie de Taxonomie Opérationnelle
  - 1.1.1 Modification des Processus Opérationnels
  - 1.1.2 Modification des Produits Opérationnels

2 Ingénierie d'Accès
- 2.1 Ingénierie de Rôles IAM
- 2.2 Ingénierie de Logique d'Autorisation

3 Gestion d'Identité des Entités
- 3.1 UIT-T X.1254 "Phase d'Enrôlement" (Enrôlement des Entités)
  - 3.1.1 Demande et lancement
  - 3.1.2 Confirmation de l'identité
  - 3.1.3 Vérification de l'identité
  - 3.1.4 Consignation des données
  - 3.1.5 Inscription
- 3.2 X.1254 "Phase de Gestion des Justificatifs" (Gestion des Justificatifs)
  - 3.2.1 Création des justificatifs
  - 3.2.2 Pré-création des justificatifs
  - 3.2.3 Initialisation des justificatifs
  - 3.2.4 Consolidation des justificatifs
  - 3.2.5 Délivrance des justificatifs
  - 3.2.6 Activation des justificatifs
  - 3.2.7 Stockage des justificatifs
  - 3.2.8 Suspension des justificatifs
  - 3.2.9 Révocation des justificatifs
  - 3.2.10 Destruction des justificatifs
  - 3.2.11 Renouvellement des justificatifs
  - 3.2.12 Remplacement des justificatifs
  - 3.2.13 Consignation des données

4 Assignation d'Accès
- 4.1 Gestion des Demandes de Modification de l'Accès
- 4.2 Gestion des Permissions Utilisateur
- 4.3 Délivrance des Crédits Utilisateur

5 Opération d'Accès
- 5.1 "Phase d'Authentification des Entités" UIT-T X.1254 (Authentification)
  - 5.1.1 Consignation des données
  - 5.1.2 Authentification de Session
- 5.2 Autorisation
  - 5.2.1 Autorisation d'Exécution des Tâches Opérationnelles
- 5.3 Enregistrement de l'Accès aux Tâches Opérationnelles

Appendice II

Proposition de profil d'extension SCIM 2.0

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Le profil d'extension suivant est proposé pour le système de gestion d'identité interdomaine (SCIM), version 2.0[1], sur la base du protocole de service web de transfert d'état de représentation (REST) [b-SCIM REST]. La Figure II.1 représente l'extension de profil proposée. Les lignes et les formes de couleur noire représentent les parties centrales de la spécification SCIM 1.0 existante [b-IETF SCIM 1.0]. Les deux formes bleues ("rôles" et "crédits") sont les points d'extension du SCIM. Les lignes et les formes en trait plein orange représentent les extensions proposées. Etant donné que la spécification SCIM laisse la nature sémantique des "rôles" et des "crédits" ouverte à une interprétation et à une définition par les mises en oeuvre[2], il est possible de spécifier les points d'extension pour les intégrer dans la partie centrale de la norme.

Afin de pouvoir assigner une signification opérationnelle aux rôles IAM, les recommandations suivantes sont proposées comme profil d'extension à la spécification SCIM actuelle:

- Le point d'extension "rôles" du SCIM sert d'ensemble de rôles opérationnels, et un rôle opérationnel est composé d'une ou plusieurs tâches opérationnelles.
- Le point d'extension "crédits" du SCIM sert d'ensemble de tâches opérationnelles supplémentaires qu'un utilisateur peut effectuer (outre les tâches opérationnelles qu'un utilisateur peut effectuer en vertu des rôles opérationnels assignés).

---

1 "La spécification du système de gestion d'identité interdomaine (SCIM) est destinée à faciliter la gestion des identités utilisateur dans les applications et les services dans le nuage." (Source: http://www.simplecloud.info/)

2 La spécification SCIM laisse les éléments suivants ouverts à une interprétation et à une définition par les mises en oeuvre:

"crédits

Une liste de crédits pour l'utilisateur qui représentent une chose dont dispose l'utilisateur. Autrement dit, un crédit est un droit supplémentaire à une chose, à un objet ou à un service. Aucun vocabulaire ni aucune syntaxe ne sont spécifiés, et les fournisseurs de services et les consommateurs sont censés encoder suffisamment d'informations dans la valeur pour déterminer avec exactitude et sans ambiguïté ce à quoi l'utilisateur a accès. Cette valeur n'a PAS de type canonique, bien qu'un type puisse être utile pour délimiter la portée des crédits.

Rôles

Une liste de rôles pour l'utilisateur qui, ensemble, représentent qui est l'utilisateur; c'est-à-dire "Etudiant", "Faculté". Aucun vocabulaire ni aucune syntaxe ne sont spécifiés, même si l'on suppose qu'une valeur rôle est une chaîne ou une désignation qui représente un ensemble de crédits. Cette valeur n'a PAS de type canonique." (Source: https://tools.ietf.org/html/draft-ietf-scim-core-schema-22)

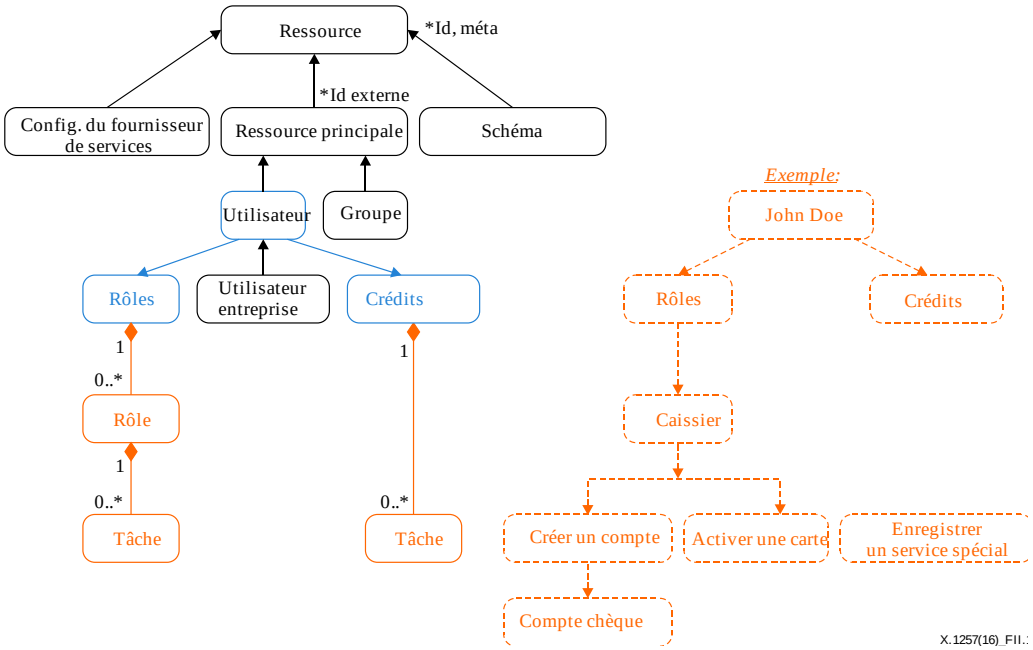

Figure II.1 – Extension de profil SCIM

L'exemple en orange à droite de la Figure montre comment un utilisateur peut avoir un rôle "Caissier" qui est composé de deux tâches: "Créer un compte" et "Activer une carte". L'autre tâche – "Enregistrer un service spécial" est un crédit supplémentaire direct pour lequel il n'est pas encore nécessaire de créer un rôle.

Appendice III

Proposition d'extension de profil XACML 3.0

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Le profil d'extension suivant est proposé afin d'atteindre les objectifs de qualité de données IAM décrits dans cet élément de travail.

La proposition consiste à introduire un nouveau type de politique XACML 3.0 [b-OASIS XACML 3.0], à savoir la Politique d'Assignation (entourée par un trait plein rouge), politique évaluée pendant la Demande d'Accès. On peut citer en exemple une politique d'accès destinée à appliquer les règles de Séparation des Fonctions (SoD) pendant l'assignation d'accès. Par ailleurs, la Politique d'Accès (entourée par un trait pointillé rouge) est une politique évaluée pendant l'exécution, qui est généralement plus complexe (à grain fin). La Figure III.1 montre un fragment de schéma IAM illustrant la Politique d'Assignation proposée.

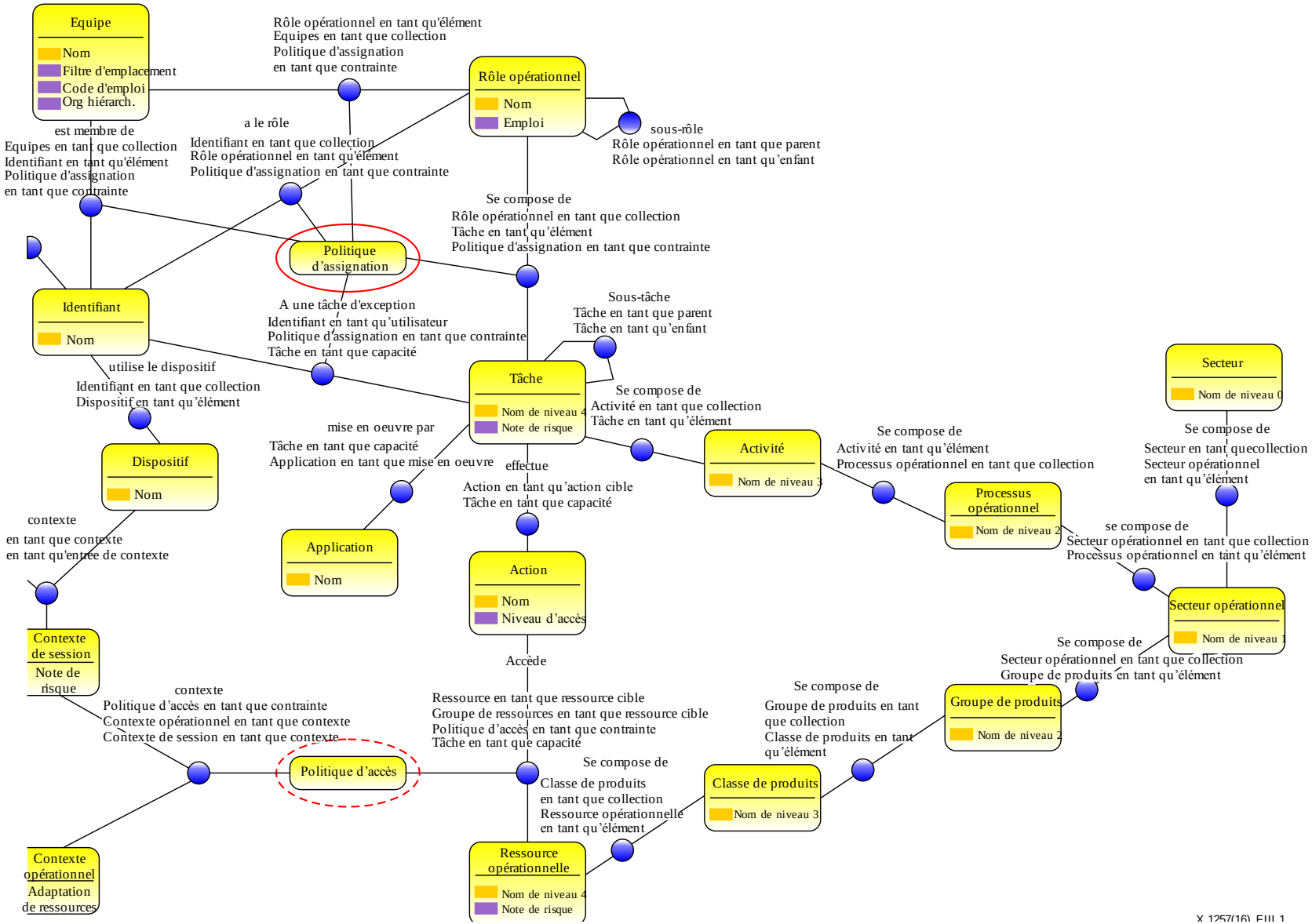

Figure III.1 – Fragment de schéma IAM illustrant la Politique d'Assignation

Créer une sémantique opérationnelle pour le modèle XACML (langage de balisage extensible de contrôle d'accès):

a) Référencer les attributs de ressource par l'intermédiaire d'un identifiant de concept de ressource opérationnelle. Ressource Opérationnelle est le noeud feuille de la taxonomie de produits opérationnels.

b) Référencer les attributs d'action par l'intermédiaire d'un identifiant de concept de Tâche et d'Action. Tâche est le noeud feuille de la taxonomie de processus opérationnels. Action est l'opération effectuée par la tâche sur la ressource opérationnelle.

c) Référencer les attributs d'environnement par l'intermédiaire d'un identifiant de concept de Contexte Opérationnel et de Contexte de Session. Le Contexte Opérationnel pourrait fournir des attributs opérationnels à grain fin, par exemple un filtre de numéro de compte. Un Contexte de Session ayant connaissance d'un état d'Authentification (crédits et métadonnées de dispositif) pourrait fournir des informations telles qu'une adresse de Protocole Internet (IP) et une adresse de dispositif de commande d'accès au support (MAC) pour une autorisation technique à grain fin.

La Figure III.2 montre l'extension sémantique proposée pour le modèle XACML.

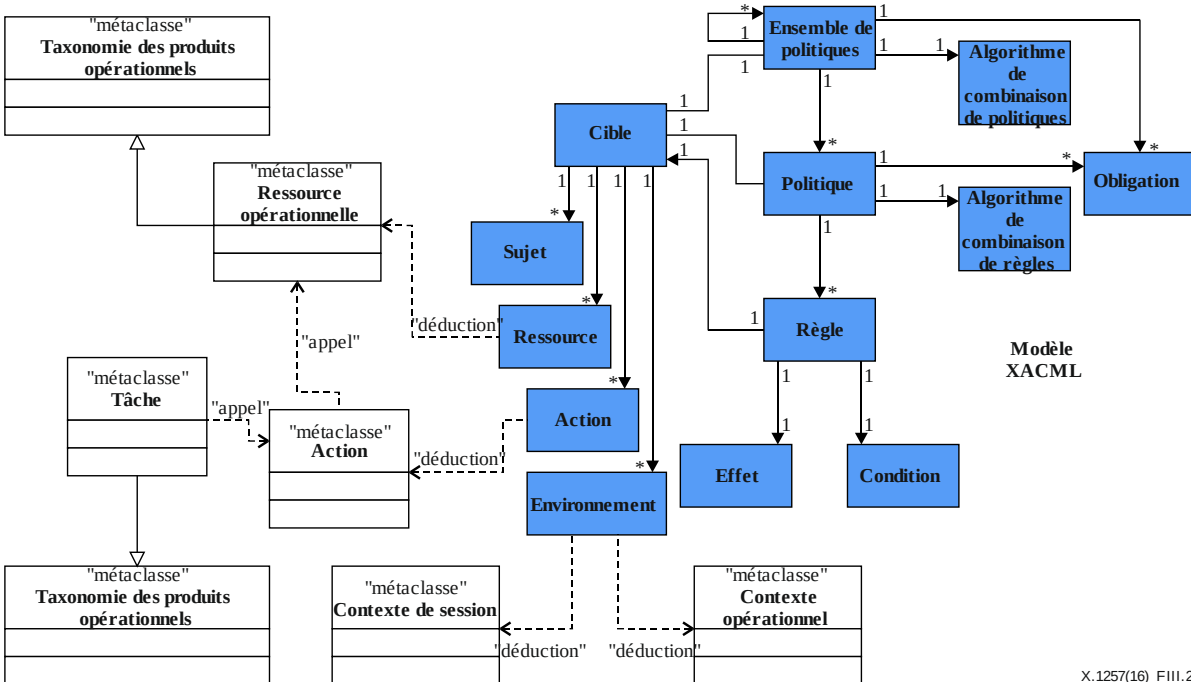

Figure III.2 – Extension sémantique proposée pour le modèle XACML

Appendice IV

Cas d'utilisation de la gestion de l'accès basée sur les tâches

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Les cas d'utilisation pertinents suivants illustrent l'utilité de la présente Recommandation:

1) Politique d'Accès
   a) L'utilisateur A est habilité à effectuer les tâches opérationnelles A, B et C par l'intermédiaire du rôle opérationnel A.
   b) L'utilisateur A est en outre habilité à effectuer la tâche opérationnelle D par l'intermédiaire de crédits directs.
   c) La politique A spécifie que la tâche B et la tâche D sont mutuellement exclusives pour un même numéro de compte.
   d) Evaluer la politique A et générer une décision de refus pour le scénario précédent.
2) Rapport d'accès (crédits)
   a) Mettre à profit les concepts de tâche afin d'améliorer la lisibilité et la signification des efforts en cours concernant la description des crédits en termes de langage opérationnel.
   b) Mettre à profit les concepts de ressource opérationnelle afin d'améliorer la lisibilité et la signification des efforts en cours concernant la description des crédits en termes de langage opérationnel.
3) Utilisation des tâches opérationnelles
   a) Tirer parti d'une application web de référence existante et:
      i) configurer un modèle d'enregistrement d'applications pour utiliser des identifiants de tâche;
      ii) générer des fichiers journaux pendant l'exécution d'applications.
   b) Utiliser des fichiers journaux d'applications à l'aide d'un outil analytique pour:
      i) rendre compte des tâches opérationnelles utilisées pendant l'exécution de la production;
      ii) mettre à jour la taxonomie opérationnelle sur la base des informations statistiques précédentes.
4) Utilisation des crédits
   a) Tirer parti d'une application web de référence existante et:
      i) configurer un modèle d'enregistrement d'applications pour utiliser des identifiants de tâche;
      ii) générer des fichiers journaux pendant l'exécution d'applications.
   b) Utiliser des fichiers journaux d'applications à l'aide d'un outil analytique pour:
      i) corréler les événements d'exécution de tâches opérationnelles sur la base de l'identifiant des tâches;
      ii) corréler les événements de refus d'autorisation sur la base de l'identifiant des tâches;
      iii) produire des rapports analytiques indiquant des scénarios antérieurs conflictuels sur le plan de la SoD.

Appendice V

Mécanismes envisageables pour la mise en oeuvre d'une interface de taxonomie opérationnelle

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Des solutions basées sur les normes, par exemple un vocabulaire contrôlé basé sur le système SKOS[3] [b-Antonie] ou un mécanisme d'enregistrement de métadonnées, peuvent permettre d'assurer l'identification et l'enregistrement des concepts de taxonomie opérationnelle. Le système SKOS est particulièrement utile pour représenter des relations hiérarchiques.

Une autre solution possible consiste à utiliser la sérialisation basée sur la notation des objets du langage Java (JSON) pour les données liées (JSON-LD) [b-W3C JSON-LD], également appelée, en anglais, JSON-Linked Data. Si la sérialisation JSON-LD permet de combiner différents vocabulaires contrôlés et de représenter des relations de graphe complexes, il n'existe pas de norme relative à une interface de taxonomie. Il n'existe pas, à ce jour, de mise en oeuvre d'un transfert d'état représentationnel (REST) ou d'un protocole simple d'accès aux objets (SOAP).

[3] Le système SKOS fournit des relations hiérarchiques de base, telles que *broader* et *narrower*, mais ne permet pas de décrire des relations ontologiques plus précises, qui peuvent être nécessaires pour exprimer la syntaxe et la signification des éléments de données IAM.

Appendice VI

Normes relatives à la taxonomie de processus opérationnels

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Dans la présente Recommandation, il a été fait référence à au moins deux types de taxonomies opérationnelles: les taxonomies de processus opérationnels et les taxonomies de produits opérationnels. Ces termes sont créés par des organismes de normalisation de la gestion des processus opérationnels, tels que le Plan amélioré d'exploitation des télécommunications du TeleManagement Forum (eTOM) et la classification centrale des produits (CPC) [b-CPC].

L'exemple présenté dans la Figure VI.1 ci-après décrit un cadre de classification des processus (PCF) de l'American Productivity and Quality Center (APQC) [b-APQC-PCF] et montre comment les produits peuvent être classifiés.

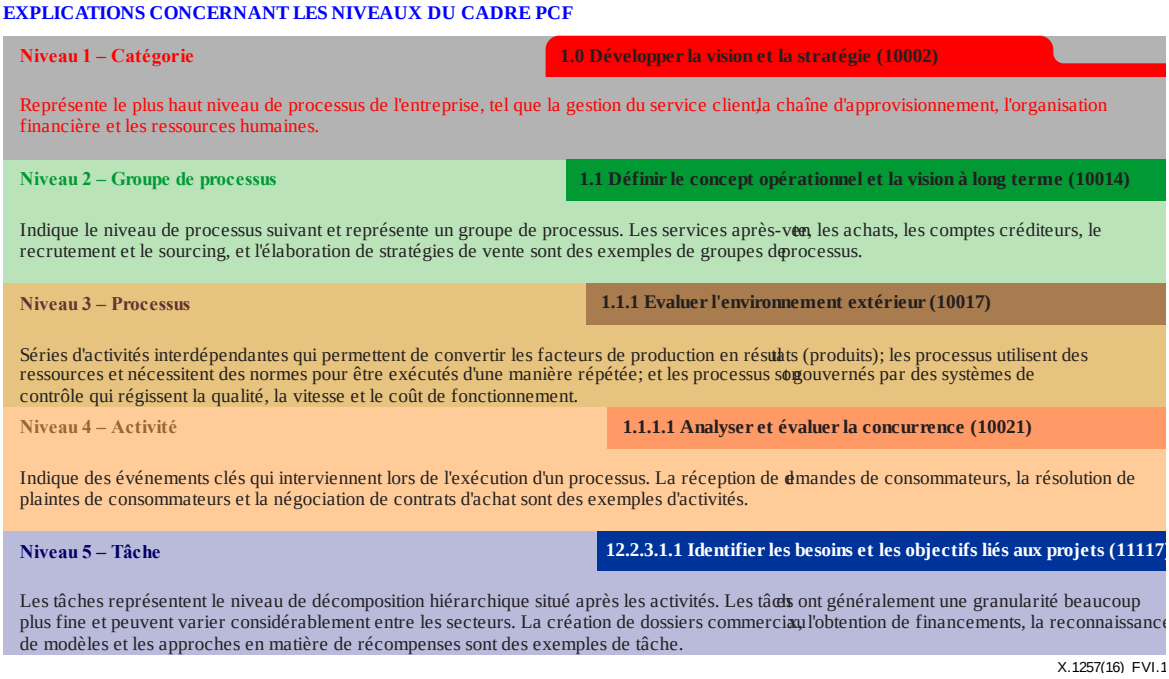

Figure VI.1 – Définitions relatives à la structure de la taxonomie de processus opérationnels du cadre PCF

Appendice VII

Modèle de domaine d'ontologie IAM

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

L'intégralité du modèle ontologique de domaine IAM est décrite dans la Figure VII.5. Pour permettre au lecteur d'aborder plus facilement le domaine IAM, cet Appendice commence par la présentation des volets suivants de la gestion IAM:

- Figure VII.1, Modèle de domaine IAM – Volet Utilisateur
- Figure VII.2, Modèle de domaine IAM – Volet Assignation d'accès
- Figure VII.3, Modèle de domaine IAM – Volet Contrôle d'accès
- Figure VII.4, Modèle de domaine IAM – Volet Domaine opérationnel.

Les volets précédents seront finalement fusionnés pour constituer le modèle de domaine IAM complet de la Figure VII.5. Le premier volet concerne les types de concept d'utilisateur. Conformément aux Recommandations [UIT-T X.1252] et [UIT-T X.1254], l'utilisateur est représenté par une Entité selon différentes perspectives, telles que la composante existentielle ou l'existence d'un sujet. Une Entité a une ou plusieurs Identités. Une Identité a un ou plusieurs Identifiants.

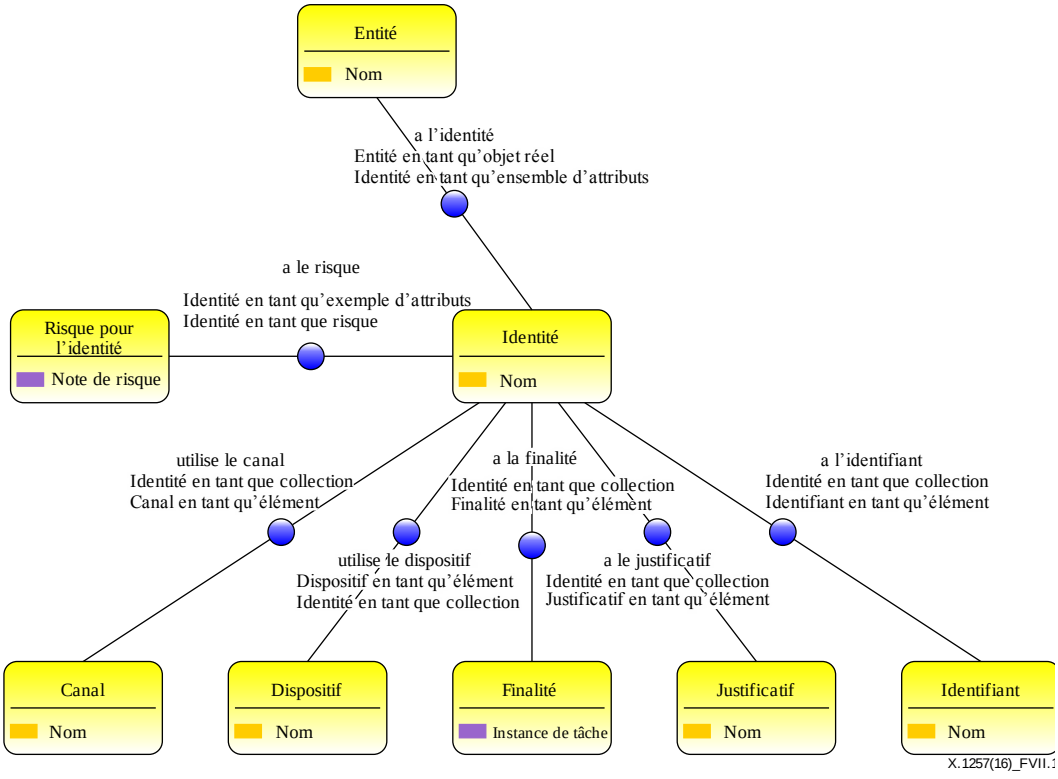

Figure VII.1 – Modèle de domaine IAM – Volet Utilisateur

Exemple: Un être humain vivant a une Entité caractérisée par son nom, sa date de naissance, etc. Cet être humain peut être simultanément employé et client, et peut donc avoir au moins deux identités. L'employé et le client auront respectivement pour identifiants un IDemployé et un IDclient.

NOTE – Dans certains cas, le rôle de l'être humain peut être joué par un dispositif qui accomplit des actions pour le compte de l'être humain.

Le volet représenté dans la Figure VII.2 est l'Assignation d'Accès. L'Assignation d'Accès consiste à assigner des droits d'accès à un utilisateur par l'intermédiaire de son (ses) identifiant(s). Les droits d'accès peuvent être assignés à l'utilisateur du fait de son appartenance à une ou plusieurs Equipes. Dans ce contexte, une Equipe est un ensemble de droits d'accès basé sur les ressources humaines. L'utilisateur peut obtenir ses droits d'accès par l'intermédiaire d'un rôle opérationnel qu'il pourrait avoir en plus des droits d'accès liés à son appartenance à une ou plusieurs équipes. Enfin, l'utilisateur peut être habilité à effectuer certaines tâches opérationnelles à titre d'exception. En définitive, les droits d'accès sont un ensemble de tâches opérationnelles que l'utilisateur peut effectuer. Toutefois, toute assignation de tâche à un utilisateur est évaluée en fonction de certaines "Politiques d'Assignation" applicables en matière de crédits, qui écartent les combinaisons de crédits toxiques et assurent l'application des règles de Séparation des Fonctions.

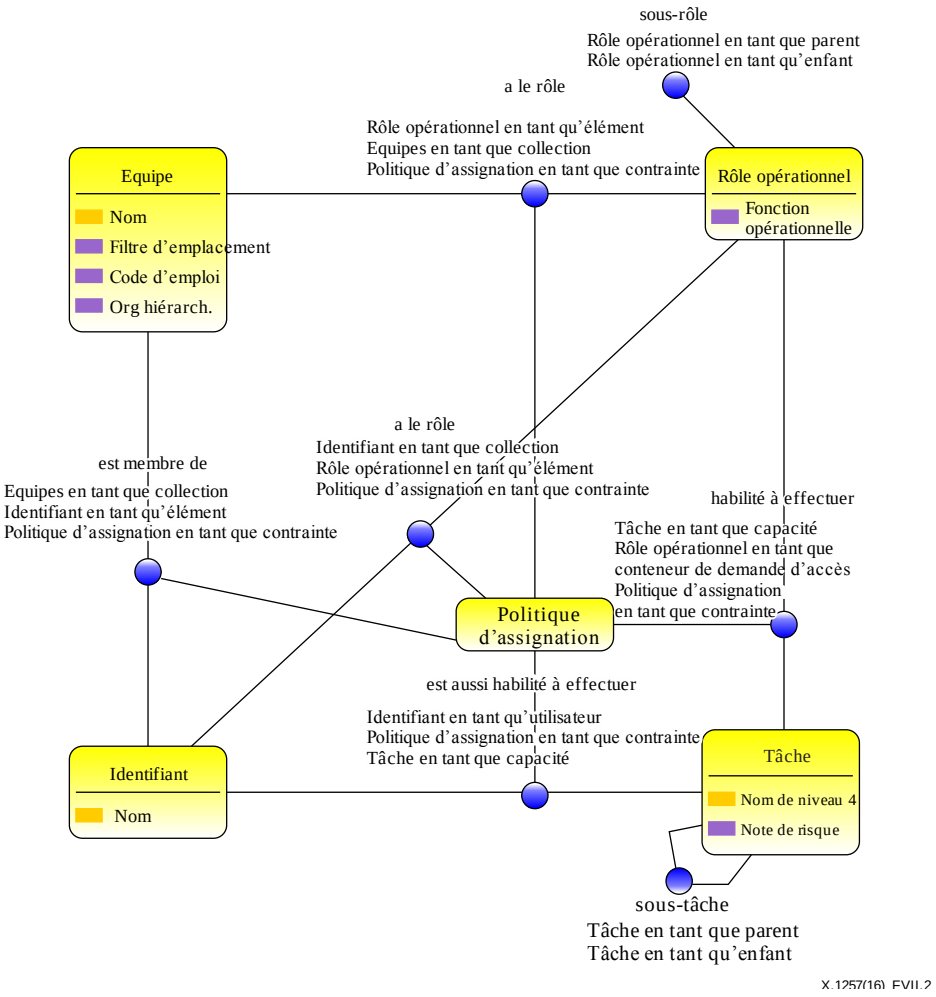

Figure VII.2 – Modèle de domaine IAM – Volet Assignation d'accès

Exemple: Un utilisateur A est membre de l'équipe X. Chaque membre de l'équipe X qui se trouve au siège (c'est-à-dire: Région = principal, Bureau = principal) a cinq rôles opérationnels, et chaque rôle opérationnel habilite un utilisateur à effectuer dix tâches. Par défaut, tout membre de l'équipe X peut donc effectuer 50 tâches. En outre, trois rôles opérationnels supplémentaires sont assignés à l'utilisateur A, chacun de ces rôles habilitant l'utilisateur à effectuer cinq tâches supplémentaires. L'utilisateur A est aussi habilité à effectuer une tâche supplémentaire directement à titre d'exception.

En définitive, l'utilisateur A est habilité à effectuer 66 tâches distinctes. En revanche, les membres de l'équipe qui ne se trouvent pas au siège n'auraient que trois rôles opérationnels – soit trente tâches opérationnelles de moins.

Le volet suivant, Contrôle d'accès, procède à une autorisation basée sur les politiques et sur les tâches, compte tenu des crédits utilisateur et du contexte de session. Une tâche particulière accède à certaines ressources si une Politique d'Accès associée autorise cet accès. La Politique d'Accès évaluera ses règles sur la base du Contexte de Session et des Contraintes d'Accès correspondantes de l'utilisateur. Le contexte de session comprendra les métadonnées d'authentification de l'utilisateur, tels que: Canal, Dispositif, Finalité, Justificatif et Identifiant.

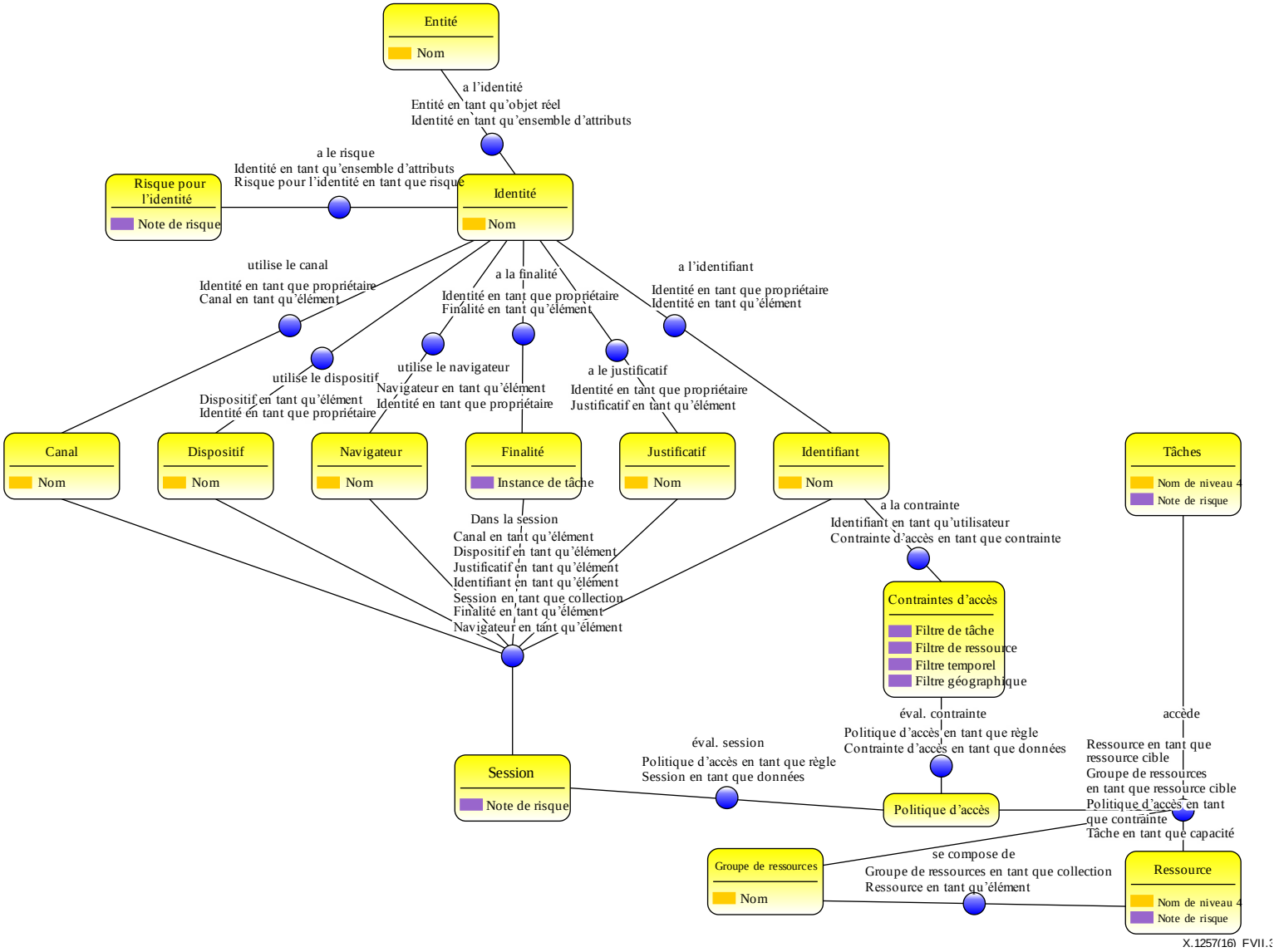

Figure VII.3 – Modèle de domaine IAM – Volet Contrôle d'accès

Exemple: Un utilisateur A souhaite effectuer une tâche "Créer un compte". Cette tâche accèdera à (c'est-à-dire: créera) une ressource opérationnelle "Compte chèque évolué". Cet accès se produira si l'évaluation de la Politique d'Accès correspondante renvoie la valeur "true". La Politique d'Accès permettra de faire en sorte qu'un certain utilisateur soit obligé d'utiliser un Canal approprié pour cette transaction et que les adresses IP se situent dans une plage valide d'adresses IP. Une politique peut aussi consulter un répertoire temporaire de tâches non autorisées valable en dehors des heures de bureau.

Le dernier volet, Taxonomie opérationnelle, illustre l'interconnexion entre le domaine IAM et le domaine opérationnel. Une taxonomie opérationnelle est composée de processus et de produits opérationnels. On peut voir (de droite à gauche) que le Secteur et le Secteur Opérationnel sont les deux premiers niveaux de cette taxonomie. A gauche du Secteur Opérationnel sont présentées deux structures hiérarchiques associées: la taxonomie de processus opérationnels et la taxonomie de produits opérationnels. En général, une tâche est un noeud feuille d'une taxonomie de processus opérationnels, alors qu'une ressource opérationnelle est un noeud feuille d'une taxonomie de produits opérationnels. Une application met en oeuvre les tâches correspondantes et assure l'accès aux ressources pour le compte de l'utilisateur.

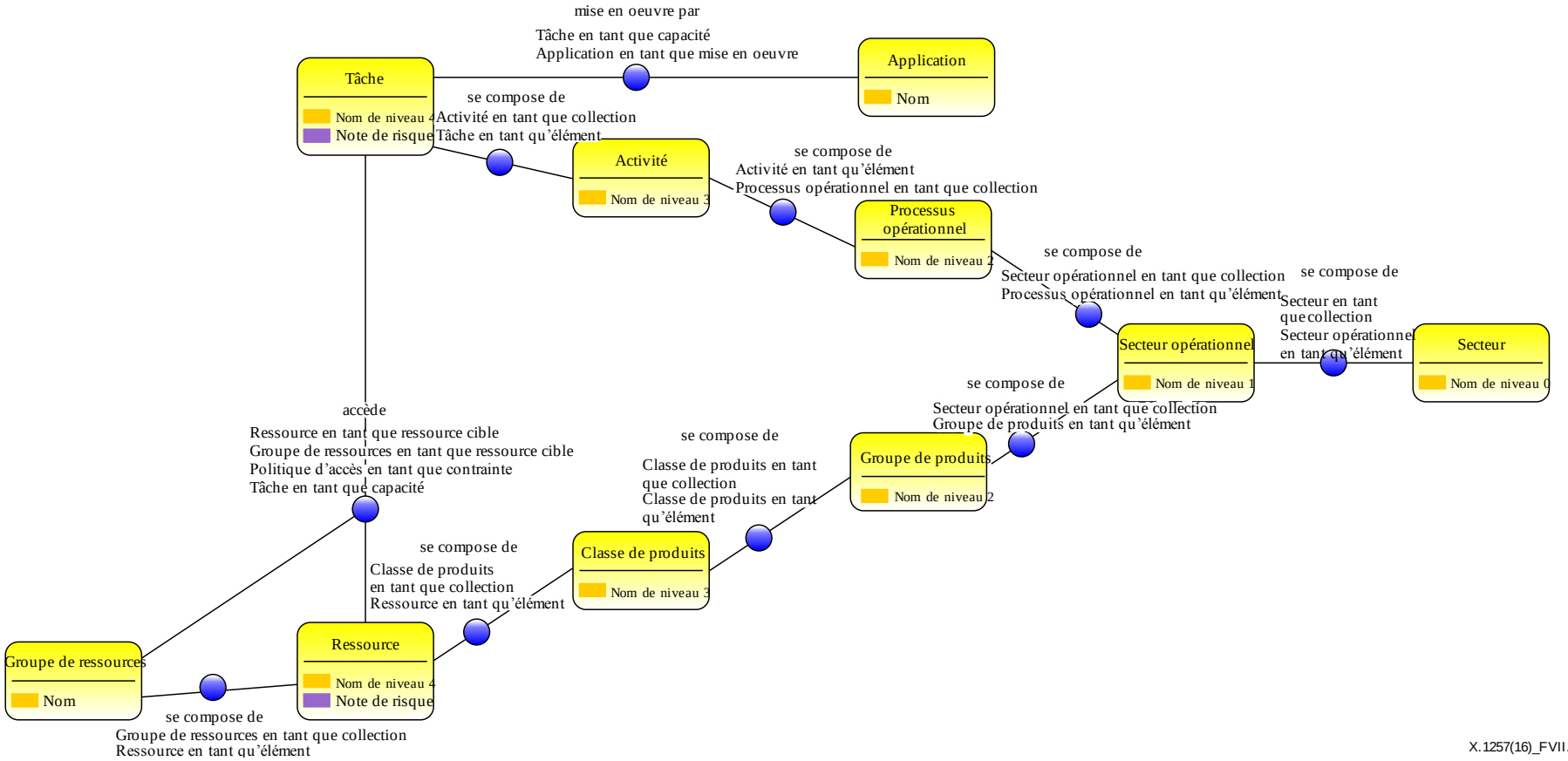

Figure VII.4 – Modèle de domaine IAM – Volet Domaine opérationnel

Exemple: La branche est "Finance". Le secteur opérationnel est "Service à la clientèle". Le processus opérationnel est "Origination". L'activité est "Activité de compte". La tâche est "Créer un compte". Du point de vue de la taxonomie de produits opérationnels, le groupe de produits est "Compte", la classe de produits est "Compte Chèque" et la ressource opérationnelle est "Compte Chèque Evolué".

Enfin, le modèle de domaine IAM complet est présenté dans la Figure VII.5 suivante, où sont fusionnés les quatre volets décrits ci-avant.

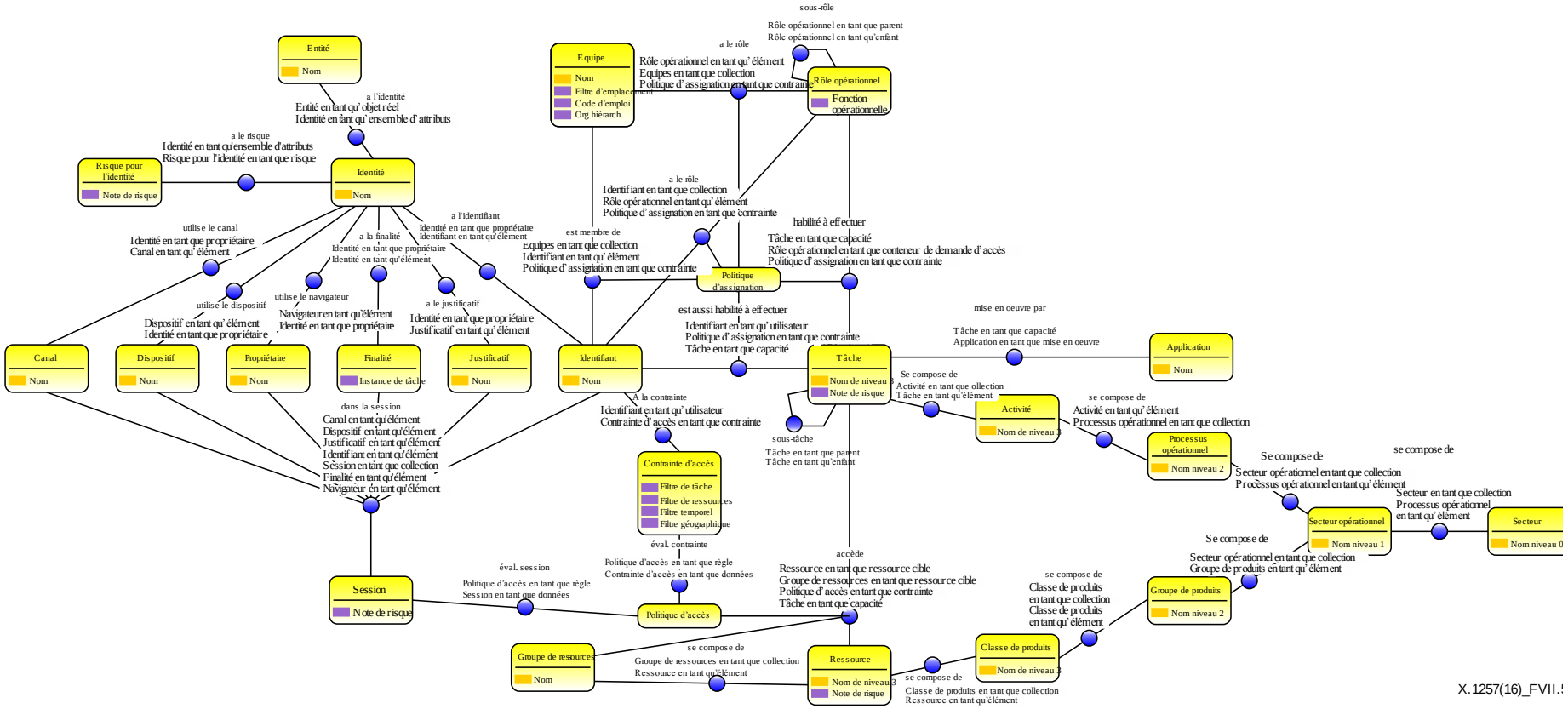

Figure VII.5 – Modèle de domaine IAM

Le modèle de domaine représenté dans la Figure VII.5 modélise les relations existant entre les concepts, conformément aux exigences présentées dans la section correspondante. Ce diagramme exprime les principes clés suivants:

- Un Utilisateur est représenté par son Entité, ses Identités, ses Identifiants, ainsi que par d'autres caractéristiques. Au cours d'un processus d'Assignation des Crédits, un utilisateur peut être habilité à effectuer des tâches particulières par l'intermédiaire des concepts d'Equipe et de Rôle (généralement le cas: 80% du temps) ou peut se voir assigner directement le droit d'effectuer des tâches particulières (à titre d'exception: 20% du temps).
- Une équipe est un ensemble de rôles lié aux ressources humaines. L'objet principal des types Equipe et Rôle Opérationnel est d'accélérer et de simplifier l'Assignation de Crédits et le processus d'Approbation.
- Les rôles opérationnels devraient hériter la signification opérationnelle des tâches opérationnelles correspondantes.

NOTE – Actuellement, les rôles IAM sont créés et maintenus par IT et n'ont donc pas de signification opérationnelle directement traçable. Dans de nombreux cas, le fait de se baser seulement sur un nom de rôle pour transmettre la signification opérationnelle ne suffit pas pour examiner avec succès les droits d'accès.

- Les tâches sont les noeuds feuilles de la taxonomie de processus opérationnels créés et maintenus par des architectes opérationnels et des modélisateurs opérationnels.
  - Les tâches ont généralement une granularité plus fine que les applications qui les mettent en oeuvre.
  - Les tâches sont mises en oeuvre par les applications correspondantes.
  - Les tâches représentent les Fonctions, comme dans les cas d'utilisation de la Séparation des Fonctions (SoD).

NOTE – Il est impossible de mettre en oeuvre la Séparation des Fonctions (SoD) sans tâches opérationnelles sous-jacentes.

- Un utilisateur n'a pas d'accès direct à une Ressource Opérationnelle. Il est habilité à effectuer une Tâche Opérationnelle, et cette Tâche Opérationnelle accède à des Ressources Opérationnelles pour le compte de l'utilisateur.
- Processus-Activité-Tâche est une structure logique qui s'inscrit dans une taxonomie de processus opérationnels et sert à identifier et à organiser les processus opérationnels d'une manière normalisée [b-APQC PCF 5.0.1], et dont la maintenance est généralement assurée par des architectes opérationnels et des modélisateurs de processus opérationnels.
- Groupe de Produits-Classe de Produits-Ressource Opérationnelle est une structure logique qui s'inscrit dans une taxonomie de produits opérationnels et sert à identifier et à organiser les produits opérationnels d'une manière normalisée [b-CPC Ver 2], et dont la maintenance est généralement assurée par des architectes opérationnels et des modélisateurs de processus opérationnels.
- Une Politique d'Assignation est un mécanisme de contrainte d'assignation de crédits, utilisé lors de la phase d'Assignation des Crédits, afin d'empêcher les fraudes et les combinaisons de tâches opérationnelles toxiques statiques.
- Une Politique d'Accès est un mécanisme de Contrainte d'Opération d'Accès, utilisé lors de phase d'Accès d'Exécution, afin d'empêcher les fraudes et les combinaisons toxiques d'exécution dynamiques.
- Les Ressources Opérationnelles sont des concepts tels que: antécédents du patient, compte de prêts et compte de chèques. Elles permettent une assignation de crédits et un contrôle d'accès à grain fin au niveau ressources.
- Les Crédits Opérationnels sont des tâches qu'un utilisateur est habilité à d'effectuer (c'est-à-dire: crédits opérationnels à gros grain).

- Les Permissions Opérationnelles sont des tâches qui accèdent à des ressources opérationnelles particulières et sont restreintes par une politique.
- Lors de l'assignation de crédits à un utilisateur, les crédits opérationnels peuvent être corrélés aux permissions système correspondantes, si nécessaire.
- Les permissions système concernent des ressources système telles que: base de données, tableau, colonne, fichier ou ensemble de données de l'ordinateur central.

Bibliographie

[b-UIT-T X.1255] Recommandation UIT-T X.1255 (2013), Cadre pour la découverte des informations relatives à la gestion d'identité.

[b-ISO/IEC 24760-1] ISO/CEI 24760-1:2011, Technologies de l'information – Techniques de sécurité – Cadre pour la gestion de l'identité – Partie 1: Terminologie et concepts.

[b-Antonie] Antoine Isaac, E. S. (18 août 2009), SKOS simple knowledge organization system primer. http://www.w3.org/TR/skos-primer/ (consulté le 18 mai 2016)

[b-APQC-PCF] Tesmer, John (mars 2014), Process Classification Framework 6.1.1. http://www.apqc.org/process-classification-framework (consulté le 18 mai 2016)

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

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

[b-CPC Ver 2] CPC Workgroup. (31 décembre 2008), Central Product Classification, Ver.2, Detailed structure and explanatory notes. http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=25 (consulté le 18 mai 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. (15 avril 2013), System for Cross-Domain Identity Management: Core Schema. http://tools.ietf.org/html/draft-ietf-scim-core-schema-01 (consulté le 18 mai 2016)

[b-IETF SCIM 2.0] Hunt, e. a. (8 juin 2015), System for Cross-Domain Identity Management: Core Schema. https://tools.ietf.org/html/draft-ietf-scim-core-schema-22 (consulté le 18 mai 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. (22 janvier 2013), 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 (consulté le 18 mai 2016)

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

[b-schema.org 2011] Google, Yahoo, Bing, Yandex. (2011). schema.org. http://schema.org (consulté le 18 mai 2016)

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

[b-W3C JSON-LD] Manu Sporny. (6 août 2013), JSON-LD 1.0, A JSON-based Serialization for Linked Data. http://json-ld.org/spec/latest/json-ld/ (consulté le 18 mai 2016)

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2016