International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1257

(03/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Identity and access management taxonomy

Recommendation ITU-T X.1257

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	**X.1250–X.1279**
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1257

Identity and access management taxonomy

Summary

Recommendation ITU-T X.1257 develops a specification to ensure that the necessary business meaning is assigned to identity and access management (IAM) roles and permissions, and that this business meaning is traceable and referenceable throughout the IAM process lifecycle. This means that that permissions can be efficiently assigned to users, separation of duties (SoD) controls can be successfully implemented across applications, and access review and reconciliation processes can be carried out efficiently.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1257	2016-03-23	17	11.1002/1000/12608

Keywords

Access management, IAM lifecycle, identity and access management, role, permission, business meaning, business taxonomy, business task.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1257

Identity and access management taxonomy

1 Scope

This Recommendation specifies requirements for assigning business meaning to identity and access management (IAM) roles and user permissions by leveraging [ITU-T X.1252], [ITU-T X.1254] and [b-ITU-T X.1255], and extending them to propose the following:

- An IAM taxonomy to semantically identify and organize IAM phases and processes to represent a comprehensive IAM process lifecycle.
- An IAM ontology model to semantically identify IAM role and permission types, their syntax and corresponding type relationships.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework.*

3 Definitions

3.1 Terms defined elsewhere

3.1.1 access control [ITU-T X.1252]: A procedure used to determine if an entity should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party.

3.1.2 attribute [ITU-T X.1252]: Information bound to an entity that specifies a characteristic of the entity.

3.1.3 context [ITU-T X.1252]: Environment with defined boundary conditions in which entities exist and interact.

3.1.4 credential [ITU-T X.1252]: Set of data presented as evidence of a claimed identity and/or entitlements.

3.1.5 entity [ITU-T X.1252]: Something that has separate and distinct existence and that can be identified in a context.

3.1.6 identifier [ITU-T X.1254]: One or more attributes that uniquely characterize an entity in a specific context.

3.1.7 identity [b-ISO/IEC 24760-1]: Set of attributes related to an entity.

NOTE – Within a particular context, an identity may have one or more identifiers to allow an entity to be uniquely recognized within that context.

3.1.8 role [ITU-T X.1252]: A set of properties or attributes that describe the capabilities or the functions performed by an entity.

NOTE – Each entity can have/play many roles. Capabilities may be inherent or assigned.

3.1.9 user [ITU-T X.1252]: Any entity that makes use of a resource, e.g., system, equipment, terminal, process, application, or corporate network.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 access assignment: A process of assigning access rights to user(s).

3.2.2 access change request management: A process for managing access change requests.

3.2.3 access constraints: A set of access constraints based on user location, temporary restricted tasks and temporary restricted resources.

3.2.4 access engineering: A process of creating and maintaining access rights.

3.2.5 access operation: A process of evaluating user access rights for the purpose of executing certain business tasks.

3.2.6 access policy: An access control constraining mechanism (i.e., what business permissions a user can execute during run-time).

3.2.7 access reconciliation: A process of changing user access rights according to stated access rights requirements to avoid over (or under) privileged user access.

3.2.8 access review: A process of reviewing user access rights for the purpose of subsequent access reconciliation and certification.

3.2.9 assign policy: A permissions assignment constraining mechanism (i.e., what tasks can be assigned to a user).

3.2.10 authorization logic engineering: A process of developing and maintaining authorization logic across related applications.

3.2.11 browser: An application running on a device used by users to interact with a service provider.

3.2.12 business role: A collection of tasks (with or without permissions) that a user can be entitled to perform.

3.2.13 business task access logging: A process of logging successfully completed task execution or user not authorized to perform certain task(s).

3.2.14 business task execution authorization: A process for authorizing a user to perform a specific business task on a specific resource.

3.2.15 business task execution: A process of executing specific business task(s).

3.2.16 business taxonomy engineering: A process of creating and maintaining a business process and business product taxonomy.

3.2.17 business process taxonomy: A taxonomy that semantically identifies and organizes business processes and sub-processes into a hierarchical structure.

3.2.18 channel: A communication method a user chooses to interact with a service provider.

3.2.19 device: A mechanism a user uses to enable the interaction with a service provider.

3.2.20 entitlement: A set of tasks and permissions assigned to a user.

3.2.21 IAM process lifecycle: A life cycle of identity and access management (IAM) processes and sub processes.

3.2.22 IAM role engineering: A process of creating and maintaining IAM roles and permissions.

3.2.23 intent: The user reason or purpose for initiating the interaction with a service provider.

3.2.24 permission: A set of task(s) accessing business resources constrained by corresponding access control policies.

3.2.25 resource: A leaf node of a business product taxonomy also known as business product.

3.2.26 session: A container of runtime authentication and authorization attributes.

3.2.27 task: A leaf node of a business process taxonomy also known as business task.

3.2.28 team: A human resource container of business roles each team member has in common.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APQC	American Productivity and Quality Center
CPC	Central Product Classification
eTOM	enhanced Telecom Operations Map
HTTP	Hypertext Transfer Protocol
IAM	Identity and Access Management
IP	Internet Protocol
IT	Information Technology
JSON	JavaScript Object Notation
JSON-LD	JSON-based serialization for Linked Data
MAC	Media Access Control
PCF	Process Classification Framework
RBAC	Role Based Access Control
REST	Representational State Transfer
SCIM	System for Cross-domain Identity Management
SDLC	Software Development Life Cycle
SKOS	Simple Knowledge Organization System
SOAP	Simple Object Access Protocol
SoD	Separation of Duties
URL	Uniform Resource Locator
XACML	extensible Access Control Markup Language

5 Conventions

The following conventions are used in this Recommendation:

First letter word capitalization in the middle of the sentence denotes the use of a term that is part of a model (i.e., IAM ontology model or IAM taxonomy model) such as "Business Role" or "IAM Role Engineering" and it can be also be found in corresponding diagrams. The term "business task"

and "task" are used interchangeably for readability purposes. The term "business resource" and "resource" are used interchangeably for readability purposes.

6 Introduction

The lack of business meaning in current identity and access management (IAM) roles and user permissions negatively impacts the entire IAM lifecycle. Even though IAM roles such as "SuperAdmin", "SuperUpdate" and "XYZSystemSpecialAccess" are ambiguous, overly-technical and cryptic they are common in many enterprises. Naturally, instead of reusing such ambiguous roles an IAM role engineer time and time again would create new roles. This however eventually leads to a large amount of hard to manage system specific IAM roles that do not convey the intended business meaning.

Such a large number of roles as well as their poor semantic quality negatively impacts key IAM lifecycle phases such as Access Assignment, Access Authorization, Access Review and Access Reconciliation. During Access Assignment an access management specialist that does not understand the meaning of existent roles could assign wrong privileges to user. To compensate for the lack of business meaning in IAM roles application developers have to hard code authorization logic into their applications. Synchronizing the maintenance of such authorization logic source code across applications is problematic and error prone. Furthermore, it is difficult (if not impossible) to implement separation of duties (SoD) controls across many applications. During Access Review due to the same lack of business meaning in IAM roles as well as the pressure to meet compliance deadlines access reviewers erroneously certify (or revoke) user access rights. The high rate of such access review errors and error prone authorization logic implementation increases the risk of reputational harm and financial loss, poses regulatory concerns, negatively impacts the productivity of the IAM operations team, and hinders the ability to deliver large scale enterprise solutions such as process, application and role rationalization.

Since current standard access control specifications do not define the semantics for IAM roles and permissions a complementary set of access management requirements needs to be specified. Such requirements would ensure that necessary business meaning is assigned to IAM roles and permissions and that this business meaning is traceable and referenceable throughout the IAM process lifecycle so that permissions can be efficiently assigned to users, SoD controls successfully implemented across applications and access review and reconciliation processes can be carried out efficiently.

7 Approach overview

Given that the scope of this Recommendation is to develop a set of requirements for assigning business meaning to IAM roles, the following approach is described in detail below. As it was noted in clause 6, an IAM role engineering team needs to assign a required business meaning to new IAM roles. But where would such business meaning originate and who can produce it? Today business architects are given a business strategy and are tasked to develop a business process and business product taxonomy.

A business process taxonomy semantically identifies and organizes business processes and sub-processes into a hierarchical (for process inventory browsing purposes) structure that starts with Industry as its root and decomposes into Business Area, Business Process, Business Action and Business Tasks (see Appendix VI – Business process taxonomy standards for more details). A business taxonomy would also include a hierarchy of business products and is usually maintained by business product architects in a large spread sheet or a document file.

During software development life cycle (SDLC) fragments of such hierarchy content are copied and pasted by business analysts to create business requirements documents that are handed to the IAM role engineering team and to the application development team for further implementation. Since a

role engineer cannot reference specific business tasks by its identifier he usually creates IAM roles with or without a definition according to his dated interpretation of the business tasks a user can perform. In the end the business meaning of the IAM role gets lost or misinterpreted by the application developer. How can this problem be solved?

To solve this problem the business meaning in IAM roles should be referenceable and traceable to the corresponding current business tasks throughout the IAM process lifecycle. This is the key foundational quality characteristic that can improve the quality of the entire IAM process lifecycle. How can this quality characteristic be implemented? A number of semantic representation approaches exist for implementing an application programming interface for a business taxonomy (see Appendix V – Possible mechanisms for implementation of business taxonomy interface).

However it is not enough to have the business meaning referenceable and traceable throughout the IAM process lifecycle. It is also required to specify a semantic syntax for IAM roles.

Currently the syntax for IAM roles syntax is specified by a widely used standard access control mechanism called role based access control (RBAC) and this is illustrated in Figure 1.

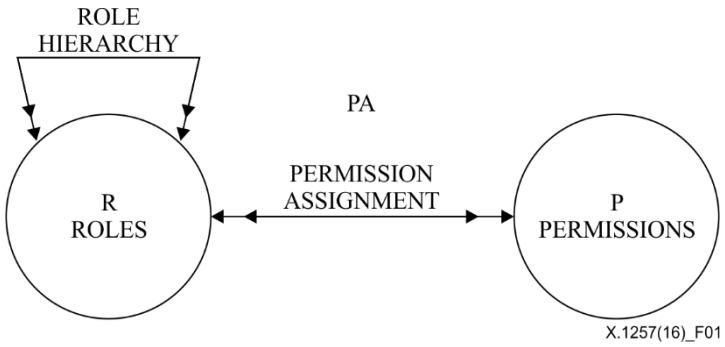

Figure 1 – Traditional RBAC model

The following role syntax can be observed:

- Roles can contain other roles, i.e., forming a role hierarchy.
- Roles are made of permissions.

However such a traditional RBAC mechanism has a known limitation, it does not specify the semantics of the permissions (i.e., the "nature of permissions"). Instead, the specification says that permission semantics is left open for interpretation, "permissions can be defined in terms of primitive operations such as read and write, or abstract operations, such as credit and debit" [b-NIST-RBAC 2000]. However in practice as shown in clause 6, ambiguous IAM roles are created without a reference to the corresponding business tasks.

In order to assign business meaning to IAM roles it is required to specify a semantic syntax for IAM roles. The meaning would have to come from the most granular business taxonomy leaf nodes, tasks and resources. Figure 2 depicts the semantic syntax of the IAM role.

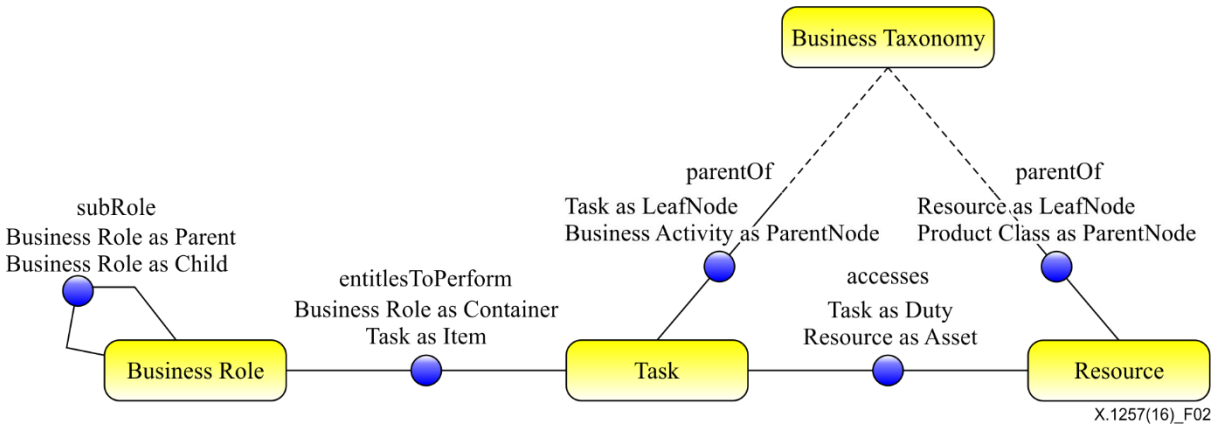

Figure 2 – Task based access management, conceptual diagram

The following can be observed:

- Roles can (still) contain other roles via "subRole" relationship, i.e., forming a role hierarchy.
- IAM roles key semantic syntax:
  - A business role entitles a user to perform business task(s) via an "entitlesToPerform" relationship. This enables any IAM role to implicitly inherit its business meaning from corresponding business tasks.
  - A business task (not the user or the role) accesses a specific resource (i.e., "Business Product"). The "accesses" relationship is an optional one and needed for situations where a more granular access control is required.
  - Task and resource as leaf nodes of the business taxonomy serve as perquisite building blocks during IAM role engineering and are referenced throughout the IAM process lifecycle.

For reasons of simplicity, the parent types of task and resource product in Figure 2 are not shown.

Table 1 shows a few entitlement examples of the above syntax that will help illustrate these points:

Table 1 – Entitlement examples

Business role	Task	Resource
Teller	Set up account	Advanced checking account
Doctor	Review patient history	Patient history
System administrator	Update system environment	System environment

The above semantic syntax for IAM roles will achieve the main goal of assigning business meaning to IAM roles. The following clause will express the proposed approach in a requirements format.

8 IAM role semantic and syntax requirements

The following recommendations are set forth for IAM roles to have the necessary business meaning:

1) Business taxonomy serves as a pre-requisite input into IAM process lifecycle to provide for business meaning in IAM roles and user permissions throughout entire lifecycle.

2) Business meaning in IAM roles is reference-able and traceable to the corresponding business tasks of the business taxonomy throughout IAM process lifecycle.

3) IAM roles to have the following semantic syntax:

3.1) IAM role is composed of business tasks a user is entitled to perform.

3.2) IAM role is composed of business tasks optionally accessing specific business resources if there is a need for a more granular access control.

4) Successful execution of business tasks as well as unauthorized business task execution requests are to be logged by referencing corresponding business tasks identifiers.

Annex A

(This annex forms an integral part of this Recommendation.)

This annex is left blank and is intended for providing possible future implementation scenarios of IAM task based access management.

Appendix I

IAM taxonomy process lifecycle

(This appendix does not form an integral part of this Recommendation.)

Figure I.1 emphasizes the fact that the entire IAM process lifecycle is primarily influenced by changes originated in business taxonomy. These business taxonomy changes would be subscribed by and consumed by IAM role engineering and authorization logic engineering teams. Changes would contain Business Task identifiers in corresponding artefacts such as IAM roles, Authorization Logic source code, and Business Task execution and authorization log files.

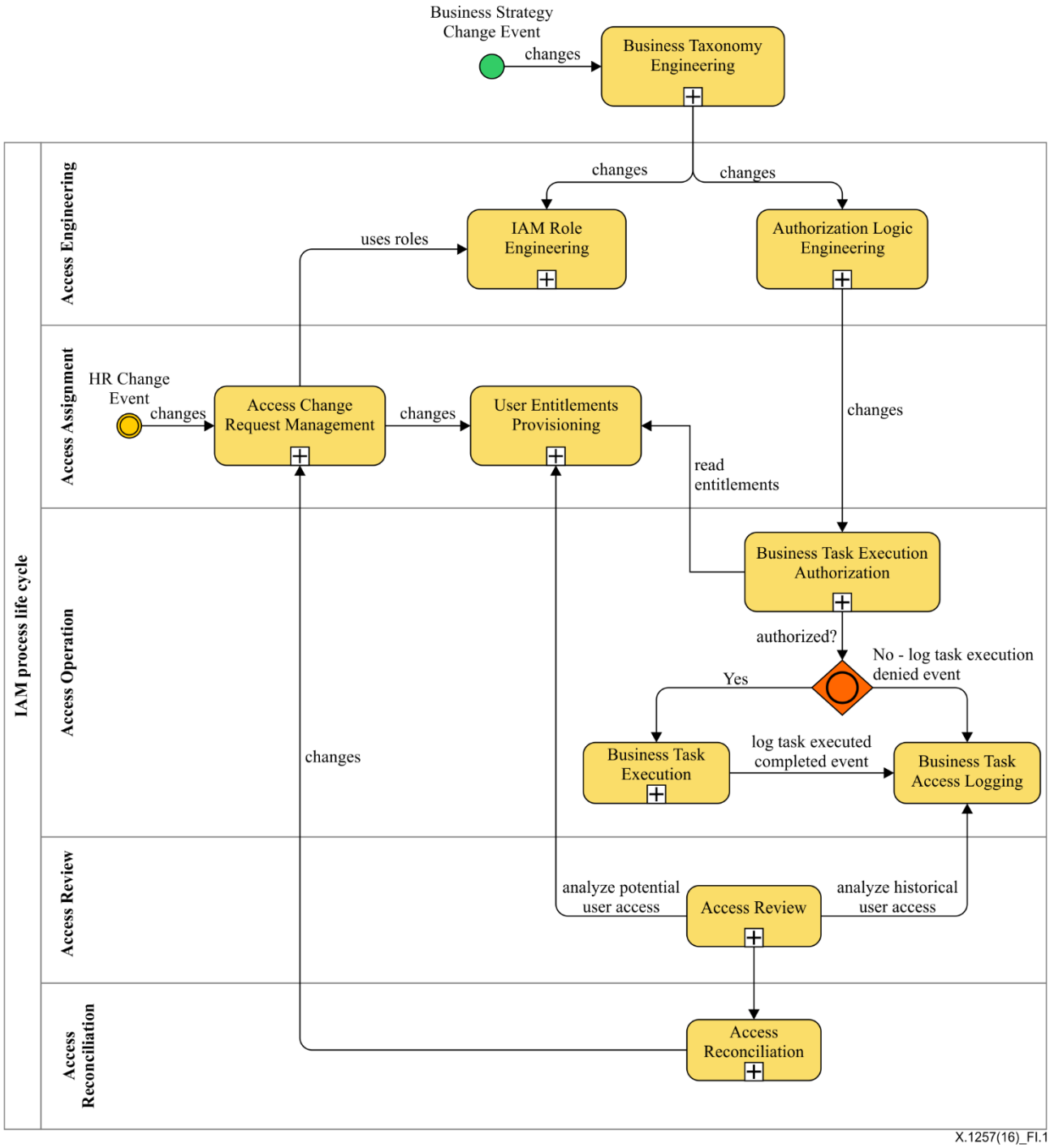

Figure I.1 – IAM process lifecycle dependencies

The second source of changes is human resource events such as hire, on-leave, move and other events of these types. These events are processed by the Access Change Request Management process and corresponding user entitlements would be provisioned to user entitlements directories. Notably, these entitlements would contain identifier references to business tasks that provide a business meaning and they would then be referenced during application runtime authorization. Once the user is authenticated (process not shown for simplicity sake) preventive SoD controls would block execution of conflicting business tasks during runtime authorization. During the Business Task Execution Authorization process a user is either authorized to perform a task and the task gets executed or the user is not authorized to perform a task. In both cases the application would log these events by referencing corresponding business task identifiers. Below is a possible example of such a logging format:

```
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"
```

where:

- **btt** – is a namespace name that resolves to an HTTP URL prefix such as **http://example.com/mylob/businesstaxonomy/task/**
- **btt:TaskID1** – is a business task identifier. When such a business task identifier is appended to a **btt** namespace it can be used to retrieve additional business task information such as task name, task description and task usage statistics.
- **bttes** – is a namespace name that resolves to an HTTP URL prefix such as **http://example.com/mylob/businesstaxonomy/task/execution/state**
- **bttes:200** – is a task execution status code indicating successful task execution.
- **bttes:401** – is a task execution status code indicating task execution not authorized.

Since business tasks are semantically referenced in the log files it would be possible for an access reviewer to analyse historical user access as well as potential user access in terms of business task execution. Once user access is comprehensively analysed and reviewed corresponding reconciliation changes are sent back to Access Change Request Management for correcting any over (or under) privileged user access rights. These reconciliation changes are an important loopback mechanism that characterizes any process as a lifecycle, i.e., IAM process lifecycle. However not all the phases would be required for small or medium size enterprises. For example Application Authorization Logic Engineering is left out or implemented by a user directory component. Figure I.1 contains only the key portions of the entire IAM process lifecycle.

The following hierarchical bulleted list is a textual representation of the IAM process lifecycle. Each taxonomy node is also defined in clause 3.2. For a codified representation please see the simple knowledge organization system (SKOS) schema [b-Antonie].

1. Business Change Management
    - 1.1 Business Taxonomy Engineering
        - 1.1.1 Business Process Change
        - 1.1.2 Business Product Change
2. Access Engineering
    - 2.1 IAM role Engineering
    - 2.2 Authorization Logic Engineering
3. Entity Identity Management
    - 3.1 ITU-T X.1254 "Enrolment Phase" (Entity enrolment)
        - 3.1.1 Application and initiation

3.1.2 Identity proofing
3.1.3 Identity verification
3.1.4 Record-keeping recording
3.1.5 Registration
3.2 X.1254 "Credential Management Phase" (Credential Management)
3.2.1 Credential creation
3.2.2 Credential pre-creation
3.2.3 Credential initialization
3.2.4 Credential binding
3.2.5 Credential issuance
3.2.6 Credential activation
3.2.7 Credential storage
3.2.8 Credential suspension
3.2.9 Credential revocation
3.2.10 Credential destruction
3.2.11 Credential renewal
3.2.12 Credential replacement
3.2.13 Record-keeping
4. Access Assignment
4.1 Access Change Request Management
4.2 User Permission Management
4.3 User Entitlements Provisioning
5. Access Operation
5.1 "Entity authentication phase" ITU-T X.1254 (Authentication)
5.1.1 Record-keeping
5.1.2 Session Authentication
5.2 Authorization
5.2.1 Business Task Execution Authorization
5.3 Business Task Access Logging
6. Access Review
6.1 Analysis
6.1.1 Analyse Potential Access Rights
6.1.2 Analyse Historical user Access
6.2 Access Audit
7. Access Reconciliation

Appendix II

SCIM 2.0 extension profile proposal

(This appendix does not form an integral part of this Recommendation.)

The following extension profile is a suggested system for cross-domain identity management (SCIM) 2.0[1] representational state transfer (REST) web service protocol as a base [b-SCIM REST]. Figure II.1 illustrates the proposed profile extension. The lines and shapes in black represent the core parts of the current SCIM 1.0 specification [b-IETF SCIM 1.0]. The two shapes in blue ("roles" and "entitlements") are the SCIM extension points. The lines and shapes in solid orange represent proposed extensions. Since SCIM specification leaves the semantic nature of "roles" and "entitlements" open for interpretation and definition by implementations[2] it is possible to further specify the extensions points to be become part of the core standard.

To be able to assign business meaning to IAM roles the following recommendations are proposed as an extension profile to the current SCIM specification:

- SCIM "roles" extension point serves a container of business roles and a business role is composed of one or more business tasks.
- SCIM "entitlements" extension point serves as a container of additional business tasks a user can perform (in addition to the business tasks a user can perform via assigned business roles).

---

1 "System for Cross-domain Identity Management (SCIM) specification is designed to make managing user identities in cloud-based applications and services easier." From http://www.simplecloud.info/

2 SCIM leaves the following open for interpretation and definition by implementations:

"entitlements

A list of entitlements for the user that represent a thing the user has. That is, an entitlement is an additional right to a thing, object or service. No vocabulary or syntax is specified and service providers/consumers are expected to encode sufficient information in the value so as to accurately and without ambiguity determine what the user has access to. This value has NO canonical types though type may be useful as a means to scope entitlements.

roles

A list of roles for the user that collectively represent who the user is; e.g., 'Student', 'Faculty'. No vocabulary or syntax is specified though it is expected that a role value is a string or label representing a collection of entitlements. This value has NO canonical types."
From https://tools.ietf.org/html/draft-ietf-scim-core-schema-22

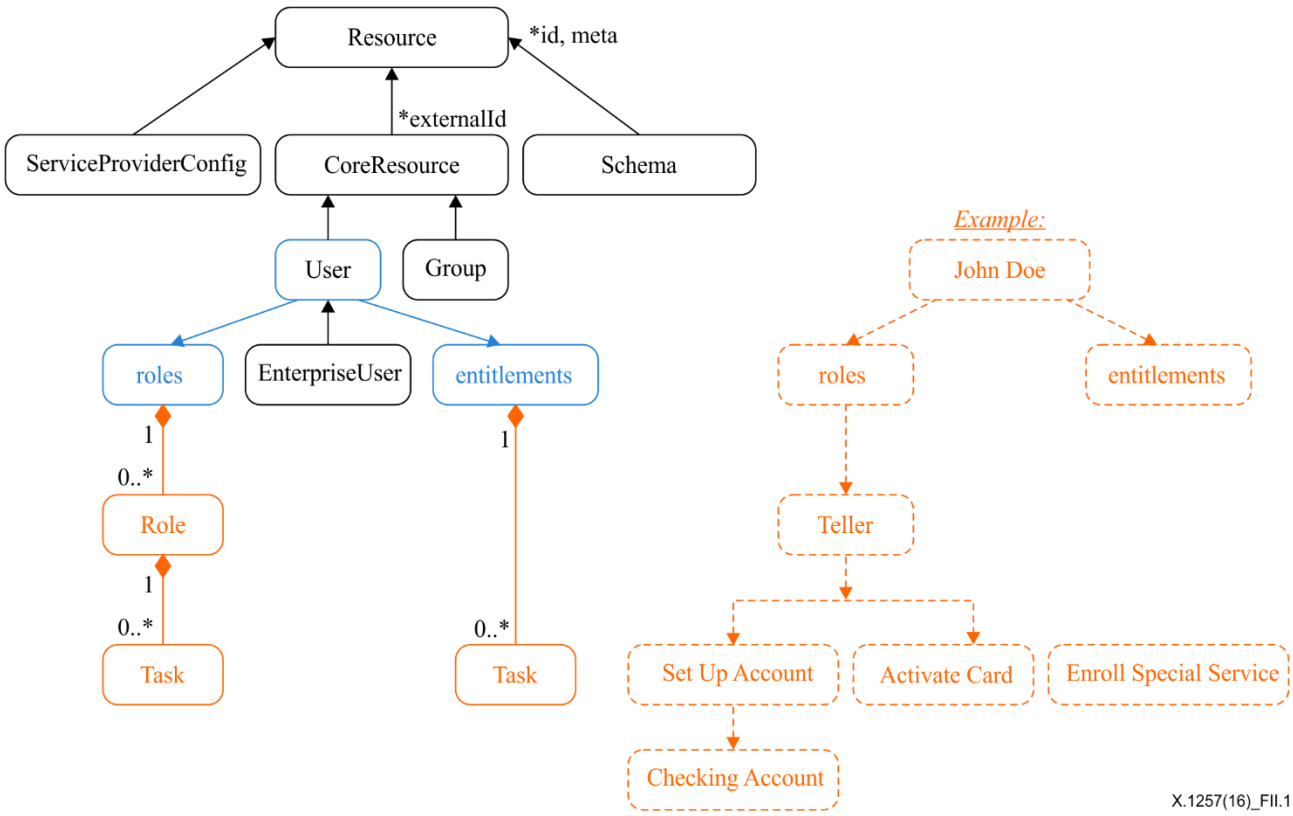

Figure II.1 – SCIM profile extension

The example on the right in orange colour illustrates how a user can have a business role "Teller" that consists of two tasks: "Set up Account" and "Activate Card". The other task – "Enrol Special Service" is a direct additional entitlement for which a role does not need to be created yet.

Appendix III

Suggested extension to XACML 3.0 profile

(This appendix does not form an integral part of this Recommendation.)

In order to achieve IAM data quality objectives outlined in this work item the following extension profile is proposed:

The proposal is to introduce a new XACML 3.0 [b-OASIS XACML 3.0] policy type, Assign Policy (circled in with a red solid line), a policy evaluated during Access Request time. An example is an access policy to enforce separation of duties (SoD) rules during access assign time. On the other hand the Access Policy (circled with a red dashed line) is a policy evaluated during run time and it is usually more complex (fine grained). Figure III.1 shows an IAM schema fragment emphasizing the proposed Assign Policy.

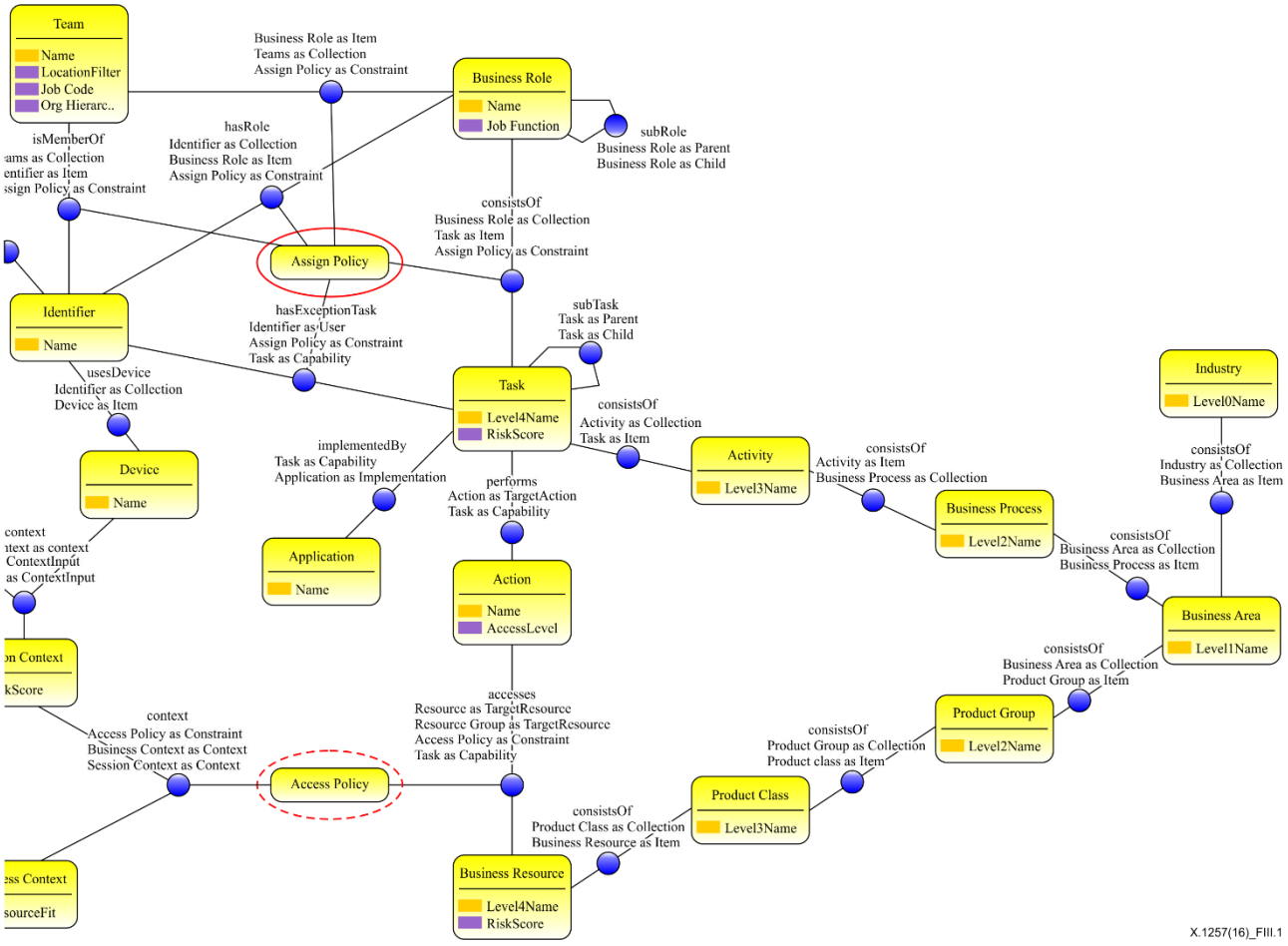

Figure III.1 – IAM schema fragment emphasizing Assign Policy

Enable business semantics for the extensible access control markup language (XACML) model:

a) Reference resource attributes via a business resource concept id. Business resource is the leaf node of the business product taxonomy.

b) Reference action attributes via a Task and Action concept id. Task is the leaf node of the business process taxonomy. Action is the operation performed by task on the business resource.

c) Reference Environment attributes via a Business Context and Session Context concept id. Business Context could provide fine grain business attributes such as an account number filter. Session Context that is aware of an Authentication state (credentials and device meta-data) could provide information such as an Internet protocol (IP) address and a media access control (MAC) device address for technical fine grain authorization.

Figure III.2 shows the proposed semantic extension to the XACML model.

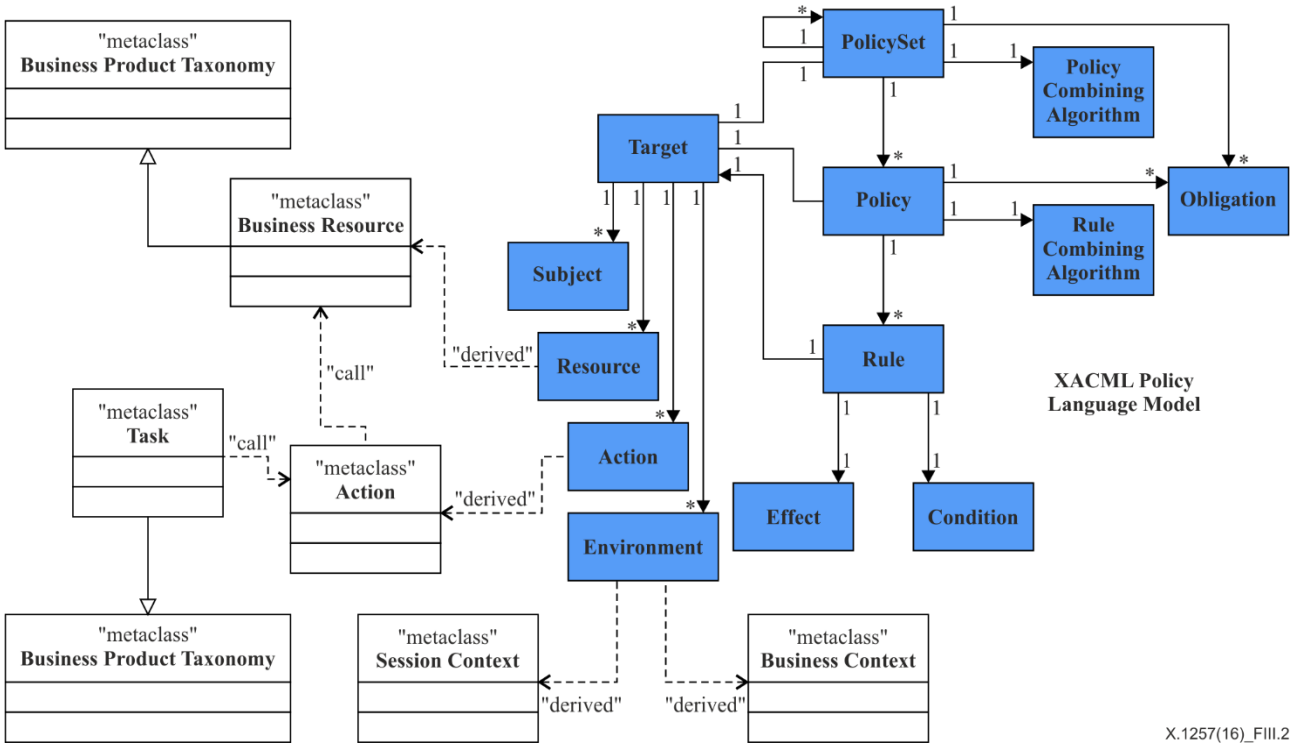

Figure III.2 – Proposed semantic extension to XACML model

Appendix IV

Task based access management use cases

(This appendix does not form an integral part of this Recommendation.)

The following relevant use cases illustrate the usefulness of this Recommendation:

1) Access policy:
   a) User A is entitled to perform business tasks A, B and C via business role A.
   b) User A is additionally entitled to perform business task D via direct entitlements.
   c) Policy A specifies that task B and task D are mutually exclusive for the same account number.
   d) Evaluate policy A and yield a deny decision for the above given scenario.
2) Access (Entitlements) reporting:
   a) Leverage task concepts to improve readability and meaning of the current business language entitlements description effort.
   b) Leverage business resource concepts to improve readability and meaning of the current business language entitlements description effort.
3) Business task usage
   a) Leverage an existent reference web application and:
      i) Configure application logging template to use business task ids.
      ii) Generate log files during application runtime.
   b) Consume app log files with an analytical tool to:
      i) Report on the business tasks being used during production runtime.
      ii) Update business taxonomy with the above statistical information.
4) Entitlements usage
   a) Leverage an existent reference web application and:
      i) Configure application logging template to use business task ids.
      ii) Generate log files during application runtime.
   b) Consume app log files with an analytical tool to:
      i) Correlate business task execution events based on task identifier.
      ii) Correlate authorizations deny events based on task identifier.
      iii) Produce analytical reports indicating SoD conflicting scenarios going back in time.

Appendix V

Possible mechanisms for implementation of business taxonomy interface

(This appendix does not form an integral part of this Recommendation.)

Standard based solutions such as a SKOS[3] [b-Antonie] controlled vocabulary or a metadata registry mechanism can provide business taxonomy concept identification and registration. SKOS is particularly useful for representing hierarchical relationships.

Another possible solution is to use JavaScript object notation (JSON)-based serialization for linked data (JSON-LD) [b-W3C JSON-LD] otherwise known as JSON-Linked Data. While JSON-LD allows various controlled vocabularies to be mixed and is able to represent complex graph relationships there is no standard for a taxonomy interface. There are neither REST nor simple object access protocol (SOAP) implementations at this point in time.

[3] SKOS provides basic hierarchical relationships such as broader and narrower however it does not allow more specific ontological relationships that may be required to express IAM data element syntax and meaning.

Appendix VI

Business process taxonomy standards

(This appendix does not form an integral part of this Recommendation.)

This Recommendation referenced at least two types of business taxonomies: Business process taxonomy and business product taxonomies. These terms are coined by business process management standard bodies such as TeleManagement Forum enhanced Telecom Operations Map (eTOM) and central product classification (CPC) [b-CPC].

The next example in Figure VI.1 shows a process classification framework (PCF) from American Productivity and Quality Center (APQC) [b-APQC-PCF] and it illustrates how processes can be classified.

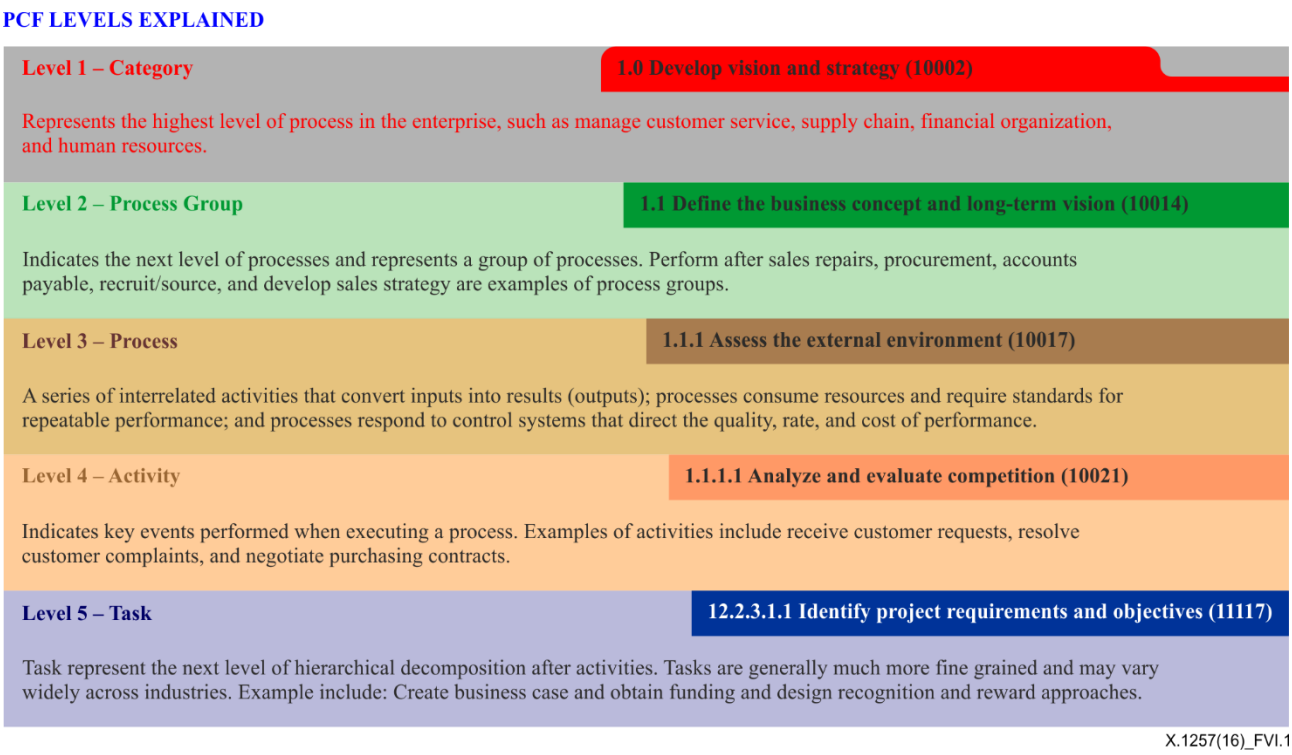

Figure VI.1 – PCF business process taxonomy structure definitions

Appendix VII

IAM ontology domain model

(This appendix does not form an integral part of this Recommendation.)

The entire IAM ontology domain model is depicted by Figure VII.5. To ease the reader into the IAM domain the following IAM subject areas are introduced first:

- Figure VII.1, IAM domain model – User subject area
- Figure VII.2, IAM domain model – Access assignment subject area
- Figure VII.3, IAM domain model – Access control subject area
- Figure VII.4, IAM domain model – Business domain subject area.

Finally, the above subject areas will be merged into the entire IAM domain model in Figure VII.5. The first subject area deals with user concept types. As per [ITU-T X.1252] and [ITU-T X.1254] the user is represented by an Entity from a few perspectives such as being or existence of a subject. An Entity has one or more Identities. An Identity has one or more Identifiers.

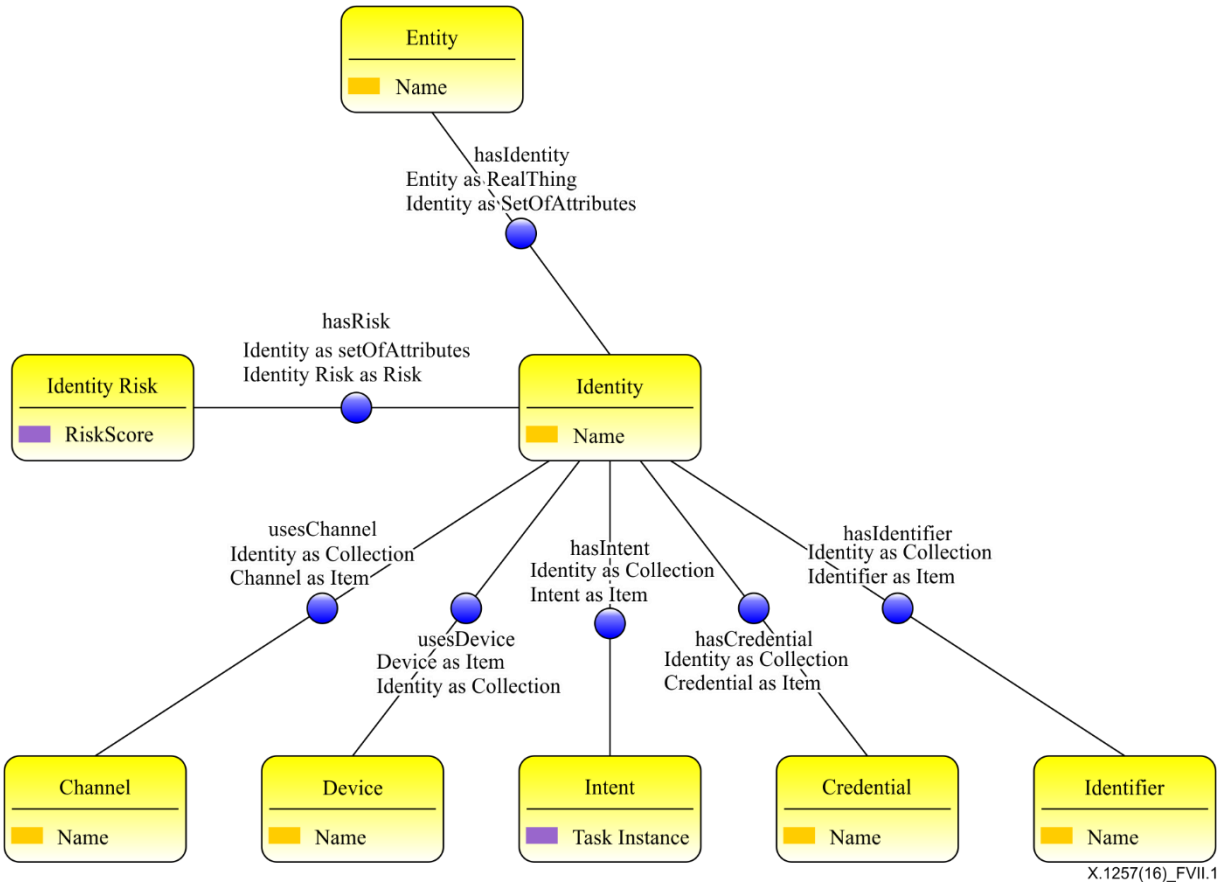

Figure VII.1 – IAM domain model – User subject area

Example: A living human being has an Entity characterized by name, date of birth, etc. This human being can be both an employee and a customer at the same time and therefore can have at least two identities. Subsequently the employee will have an EmployeeID and a customer will have a CustomerID as identifiers.

NOTE – In some cases the role of the human being can be played by a device that acts on behalf of the human being.

In Figure VII.2 the illustrated subject area is Access Assignment. Access Assignment deals with assigning access rights to a user via its identifier(s). Access rights can be assigned to user via Team(s) he or she is a member of. Team in this context is a container of human resource driven access rights. The user can get its access rights via a business role he or she could have in addition to team member access rights. Finally as an exception the user can be entitled to perform certain business tasks. In the end the access rights are a collection of tasks the user can perform. However all user to task assignment is evaluated through certain applicable entitlements called "Assign Policies" that both rule out toxic entitlement combinations as well as enforce separation of duties (SoD) rules.

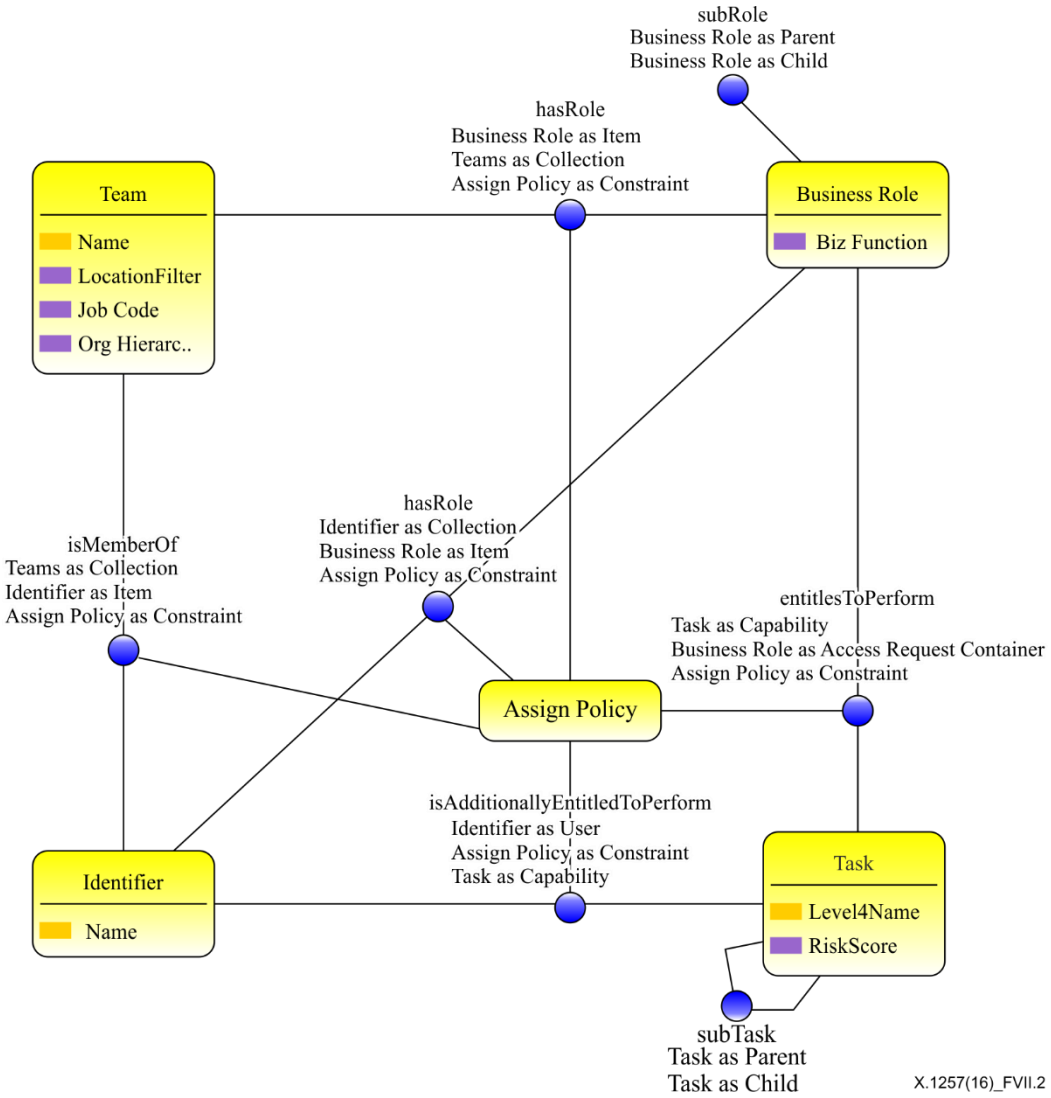

Figure VII.2 – IAM domain model – Access assignment subject area

Example: User A is member of team X. Each member of team X who is located at the headquarters location (i.e., Region=main, Desk=main) has five business roles and each business role entitles the user to perform ten tasks. So by default any team X member can perform 50 tasks. Additionally user A is assigned three more business roles that entitle the user to perform 5 more tasks. User A is also entitled to perform one more task directly as an exception. In the end user A is entitled to perform 66 distinct tasks. However team members that are not located in the headquarters would have only three business roles, i.e., 30 business tasks less.

The next subject area, Access control, carries out policy and task based authorization based on user entitlements and session context. A particular task accesses certain resource(s) if a corresponding Access Policy allows this access to happen. The Access Policy will evaluate its rules having Session context and corresponding user Access Constraints. Session context will have user authentication metadata such as Channel, Device, Intent, Credential and Identifier.

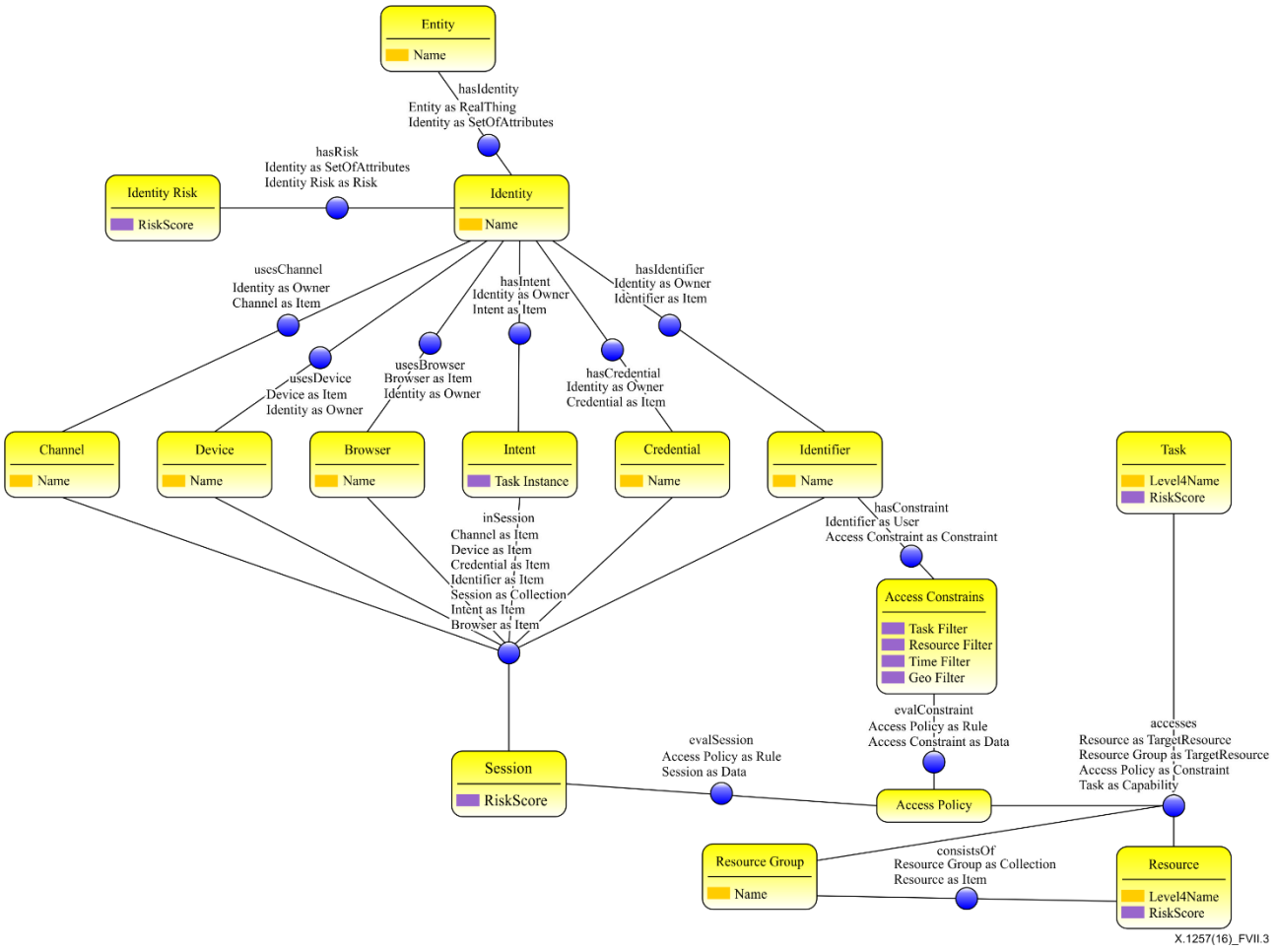

Figure VII.3 – IAM domain model – Access control subject area

Example: User A intends to perform a "Set up Account" task. This task will access (i.e., create) an "Advantage Checking Account" business resource. This access will occur if corresponding access policy evaluates to true. Access Policy will ensure that a certain user must use a proper Channel for this transaction and that the IP addresses are within a valid range of IP addresses. A policy may also consult a transient store of non-permitted tasks at this point in time since it is past business hours.

The last subject area, business taxonomy, illustrates how the IAM domain and the business domain interconnect. A business taxonomy is composed of business processes and products. It can be seen (from right to left) that Industry and Business Areas are the first two levels of this taxonomy. To the left of Business Area two related hierarchical structures, business process taxonomy and business product taxonomy are presented. Usually Task is a leaf node in a business process taxonomy and business resource is a leaf node in a business product taxonomy. Application is implementing corresponding tasks and performs resource access on behalf of the user.

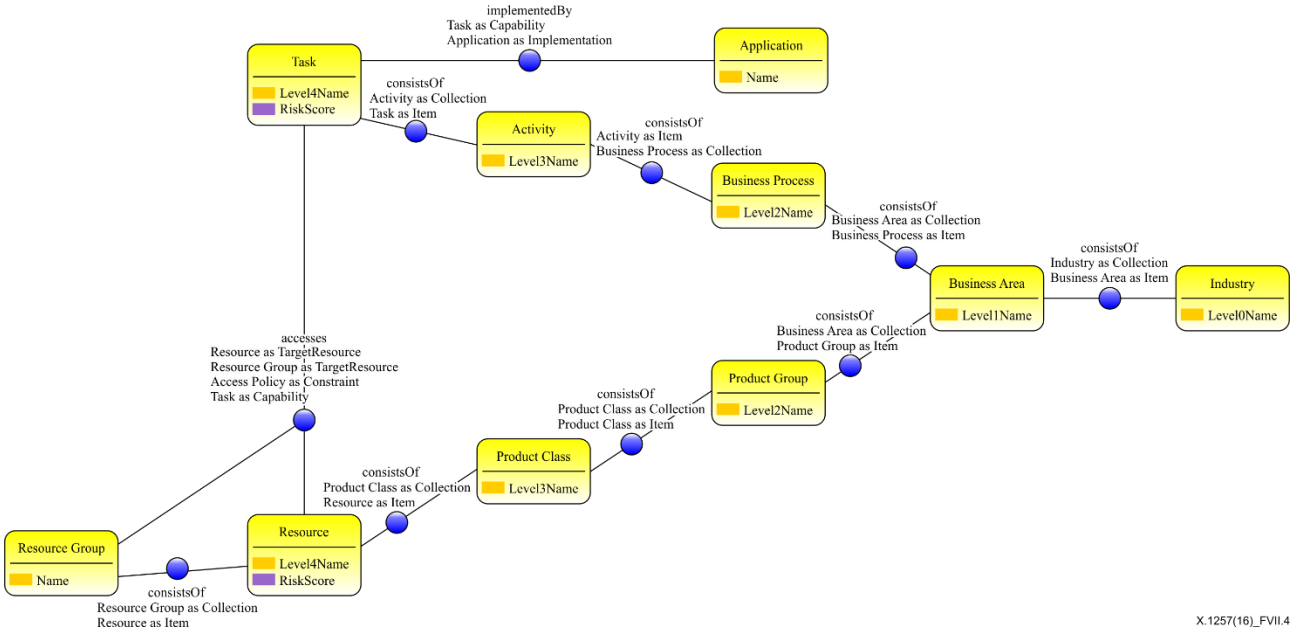

Figure VII.4 – IAM domain model – Business domain subject area

Example: Industry is financial. Business area is customer service. Business Process is Origination. Activity is Account Activity. Task is "Set up Account." From the business product taxonomy perspective, Product Group is Account, Product Class is Checking Account and Business Resource is "Advantage Checking Account."

Finally the entire IAM domain model is represented by Figure VII.5 below which merges the four subject areas mentioned above.

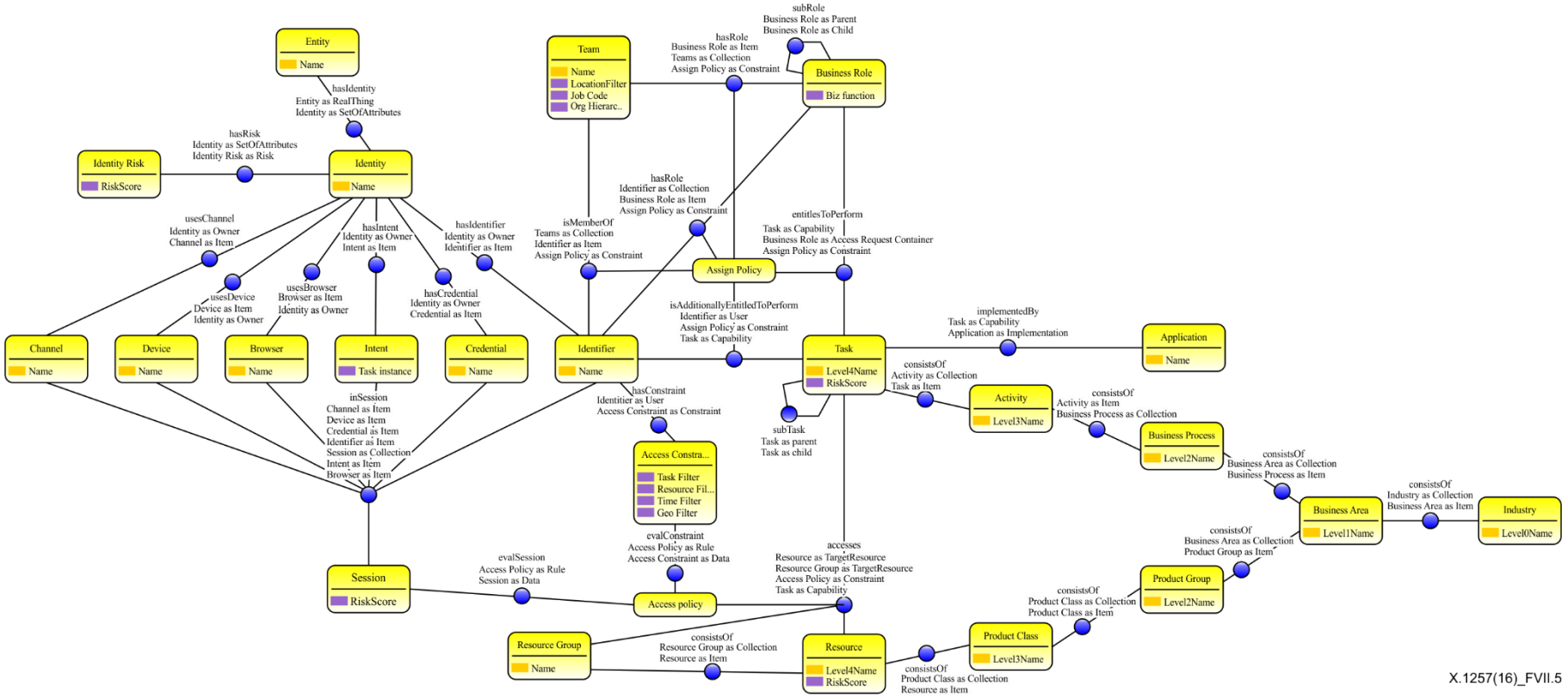

Figure VII.5 – IAM domain model

The domain model displayed in Figure VII.5 is modelling relationships between concepts according to requirements set forth in the corresponding section. The following key principles are communicated by this diagram:

- A user is represented by its Entity, Identities, Identifiers, as well as other characteristics. During an Entitlements Assignment process a user can be entitled to perform specific tasks via Team and role (usually the case in 80% of the time) or can be directly assigned to perform specific tasks (as an exception in 20% of the time).
- A Team is a human resource container of roles. The main purpose of the Team and Business Role types is to speed up and simplify the Entitlement Assignment and Approval process.
- Business roles should inherit the business meaning from corresponding business tasks.

NOTE – Currently IAM roles are created and maintained by IT and therefore do not have a direct traceable business meaning. In many cases relying a on a role name alone to convey the business meaning is not sufficient to successfully review access rights.

- Tasks are the leaf nodes of the business process taxonomy created and maintained by business architects and business modellers.
    - Tasks are usually more granular than the applications that implement them.
    - Tasks are implemented by corresponding application(s).
    - Tasks represent the Duties as in separation of duties (SoD) use cases.

NOTE – It is impossible to implement SoD without underlying business tasks.

- A user does not have a direct access to a Business Resource. Instead the user is entitled to perform a Business Task and the Business Task accesses Business Resource(s) on behalf of the user.
- A Process-Activity-Task is a logical structure and part of a business process taxonomy for identifying and organizing business processes in a standard way [b-APQC PCF 5.0.1] and usually is maintained by business architects and business process modellers.
- Product Group-Product Class-Business Resource is a logical structure and part of a business product taxonomy for identifying and organizing business products in a standard way [b-CPC Ver 2] and usually maintained is by business architects and business process modellers.
- Assign policy is an entitlement assignment constraint mechanism used during the Entitlement Assignment phase for preventing fraud and static toxic business task combinations.
- Access Policy is an Access Operation Constraint mechanism used during Runtime Access phase for preventing fraud and dynamic runtime toxic combinations.
- Business Resources are concepts such as patient records, loan account and checking account. They enable fine-grain resource level entitlement assignment and access control.
- Business entitlements are task(s) a user is entitled to perform (i.e., coarse-grain business entitlements).
- Business permissions are task(s) that access specific business resources and that are constrained by a policy.
- During user entitlements provisioning, business entitlements can be mapped to a corresponding system permissions if necessary.
- System permissions deal with system resources such as database, table, column, file, or mainframe data set.

Bibliography

[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)

[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)

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016