国　际　电　信　联　盟

ITU-T

国际电信联盟
电信标准化部门

X.1257

(03/2016)

X系列：数据网、开放系统通信和安全性

网络空间安全 – 身份管理

身份和接入管理分类

ITU-T X.1257 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
PITV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	**X.1250–X.1279**
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
PKI相关建议书	X.1340–X.1349
网络安全信息交换	
网络安全综述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息要求	X.1560–X.1569
标示和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全综述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳实践和指导原则	X.1640–X.1659
云计算安全实现	X.1660–X.1679
其他云计算安全	X.1680–X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1257 建议书

身份和接入管理分类

摘要

ITU-T X.1257建议书制定的规范旨在为IAM的职能与许可赋予必要的业务含义，且在IAM程序整个生命周期中此业务含义具有可追踪性和可引用性，从而能够将许可高效地指派给用户，且职责分离（SoD）控制在不同应用间能得以成功应用，接入复审和协商进程能够高效实施。

沿革

版本	建议书	批准日期	研究组	识别码*
1.0	ITU-T X.1257	2016-03-23	17	11.1002/1000/12608

关键词

接入管理、IAM生命周期、身份和接入管理、角色、许可、业务含义、业务分类、业务任务。

* 访问建议书，请在您的Web浏览器地址栏中输入网址http://handle.itu.int/ ，其次建议书的识别码，例如http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）在电信，信息和通讯技术领域是国际电信联盟的常设机构。国际电信联盟电信标准化部门负责研究技术，操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

世界电信标准化大会（WTSA），每四年举行一次，确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第一号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性和适应性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提醒注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适应性不表示意见。

至本建议书截止之日起，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新消息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1257建议书

身份和接入管理分类

1 范围

本建议书说明了通过[ITU-T X.1252]、[ITU-T X.1254]和[b-ITU-T X.1255]建议书为IAM角色和用户权限赋予业务含义的具体要求，并将要求做如下扩展：

- IAM分类，从语义上确定和组织IAM的阶段和程序，代表了整个IAM生命周期。
- IAM本体模型，从语义上确定IAM的角色和权限类型、权限句法和对应类型关系。

2 参考

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均会得到修订；因此本建议书的使用者应查证是否有可能使用下列建议书和其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

[ITU-T X.1252] ITU-T X.1252（2010）建议书，*身份管理基准术语和定义*

[ITU-T X.1254] ITU-T X.1254（2012）建议书，*实体认证保证框架*。

3 定义

3.1 其他文件中的术语定义

3.1.1 接入控制：[ITU-T X.1252]：用来确定实体是否应按照预先确定的规则和请求方的具体权利或相关授权被授予获得资源、设施、服务或信息的程序。

3.1.2 属性[ITU-T X.1252]：针对实体并说明该实体特性的信息。

3.1.3 上下文[ITU-T X.1252]：由边界条件确定的实体存在和互动的环境。

3.1.4 凭证[ITU-T X.1252]：作为被声称的身份和/或权利的证明的一组数据。

3.1.5 实体[ITU-T X.1252]：单独和独立存在的任何事物，可在上下文中识别。

3.1.6 标识符[ITU-T X.1254]：用来在上下中识别实体的一个或多个属性。

3.1.7 身份[b-ISO/IEC 24760-1]：与实体相关的一系列属性。

注 – 在具体情境中，一个身份可能具有使实体在该情境中得到唯一识别的一个或多个标识符。

3.1.8 角色[ITU-T X.1252]：描述实体能力和性能的特征和属性集合。

注 – 每个实体拥有/发挥多个角色。能力可为固有能力或指定能力。

3.1.9 用户[ITU-T X.1252]：使用资源的任何实体，如系统、设备、终端、程序、应用或企业网络。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 **接入指定：**向用户指定接入权利的程序。

3.2.2 **接入变更请求管理：**管理接入变更请求的程序。

3.2.3 **接入限制：**基于用户地点、临时限制任务和临时限制资源的接入限制集合。

3.2.4 **接入工程设计：**创建、维护接入权限的程序。

3.2.5 **接入操作：**用户接入权限的评估程序，用于执行特定的业务

3.2.6 **接入策略：**即接入控制限制机制（即用户在运行期间能够执行哪些业务权限）。

3.2.7 **接入调整：**根据说明的接入权限要求变更用户接入权限，避免过度（或过低）特权用户接入。

3.2.8 **接入校验**：用户接入权限校验，用于后续接入的调整及认证。

3.2.9 **指定政策：**权限分配限制机制（即哪些任务可以指定给用户）。

3.2.10 **授权逻辑工程：**在相关应用之间制定和保持逻辑授权的程序。

3.2.11 **浏览器：**设备上运行的应用，使用户可以与服务提供商互动。

3.2.12 **业务角色：**用户有权执行的任务（有或没有权限均可）集合。

3.2.13 **业务任务接入日志：**记录成功完成的任务执行或未授权用户执行部分任务的程序。

3.2.14 **业务任务执行授权：**授权用户在具体资源上执行具体业务任务的程序。

3.2.15 **业务任务执行：**执行具体业务任务的程序。

3.2.16 **业务分类工程：**创建并维护业务程序和业务产品分类的程序。

3.2.17 **业务程序分类：**指在分级结构中，在语义上明确、组织业务程序和子程序。

3.2.18 **渠道：**用户选择与服务提供商互动的通信方法。

3.2.19 **设备：**用户用于和服务提供商互动的机制。

3.2.20 **权利：**向用户分配的任务和权限集合。

3.2.21 **IAM 程序生命周期：**身份和接入管理程序和子程序的生命周期。

3.2.22 **IAM 角色工程：**创建并维护 IAM 角色和权限的程序。

3.2.23 **意图：** 与服务提供商发起互动的用户方原因或目的。

3.2.24 **许可：**接入相应接入控制策略限制下的业务资源的任务集合。

3.2.25 **资源：**业务产品分类的叶节点，也称为业务产品。

3.2.26 **会话：**运行时间验证和授权属性的容器。

3.2.27 **任务：**业务产品分类的叶节点，也称为业务任务。

3.2.28 **团队：**每个团队成员都拥有的人力资源容器。

4 缩写词和首字母缩略词

本建议书中使用了下列缩写词和首字母缩略语:

APQC 美国生产力与质量中心

CPC 中央产品分类目录

eTOM 增强的电信运营图

HTTP 超文本传输协议

IAM 身份和接入管理

IP 互联网协议

IT 信息技术

JSON JavaScript 对象表示法

JSON-LD 基于JSON的链接数据序列化

MAC 媒体接入控制

PCF 流程分类框架

RBAC 基于角色的接入控制

REST 表述性状态转移

SCIM 跨域身份管理系统

SDLC 软件开发生命周期

SKOS 简单知识组织系统

SOAP 简单对象接入协议

SoD 职责分离

URL 统一资源定位符

XACML 可扩展接入控制标记语言

5 约定

以下约定用于本建议书。

句子中首字母大写词表示使用模型（即IAM本体模型或IAM分类模型）中的词汇，如“业务角色”或“IAM角色工程”，也能在对应的图中找到。“业务任务”和“任务”、“业务资源”和“资源”互换使用的目的是增强可读性。

6 前言

当前缺少身份和接入管理（IAM）和用户权限的业务含义对整个IAM生命周期产生了负面影响。尽管“超级管理员”、“超级升级”和“XYZ系统特殊接入”等IAM角色的含义模糊、过于技术、难以理解，但却在很多企业中广泛使用。IAM角色工程师常常创建新的角色，而不是使用这些含义模糊的角色。但是，这种做法导致了大量难以管理，针对具体系统的IAM角色。这些IAM角色无法传递特定含义。

如此大量的角色和较差的语义质量对接入指定、接入授权、接入校验和接入调整等关键IAM生命周期阶段产生了负面的影响。在接入指定阶段，若接入管理专业人员无法理解当前角色的含义，会向用户分配错误的特权。为了弥补IAM角色业务含义的缺失，应用开发者不得不在应用中硬性编码授权逻辑。在应用之间对此类逻辑源代码进行同步存在很多问题，容易产生误差。此外，也很难(如果可能的话)在多个应用之间实施控制职责分离（SoD）。在IAM业务含义缺失和合规期限的双重影响下，接入校验员会错误验证（或取消）用户接入权利。接入校验的高错误率和容易出错的授权逻辑实施增加了名誉受损和财务损失的风险，带来了监管问题、对IAM操作团队的生产力造成了不利影响，同时阻碍了提供大规模企业级解决方案的能力，如程序、应用和角色合理化。

由于当前标准接入控制规格没有定义IAM角色的语义和权限，需要规定补充性的接入管理要求。补充性要求能确保为IAM角色指定必要的业务含义和权限，且在IAM程序的整个生命周期中此含义具有可追踪性和可引用性，从而能高效的向用户分配权限，在不同应用间成功实施职责分离（SoD）控制，有效执行接入校验和调整程序。

7 方法概述

鉴于本建议书旨在说明为IAM角色指定业务含义的要求，下文将详细说明方法。如引言所述 — IAM角色工程团队需要为新的IAM角色指定要求业务含义。但是这些业务含义来自于哪里？又由谁规定呢？如今，业务架构师在业务策略指导下需要开发业务程序和业务产品分类。

业务程序分类从语义上明确、组织融入分层结构（便于浏览程序目录）的业务程序和子程序，这种分层结构随行业发展生根，分解为业务领域、业务程序、业务行动和业务任务（见附录VI – 业务程序分类标准详情）。业务分类还包括业务产品分层结构，一般由义务产品架构师通过大型数据表或文档文件维护。

在软件开发生命周期（SDLC）中，该分层内容的碎片由业务分析师复制和粘贴，制作提交LAM角色工程团队和应用开发团队的业务需求文件，供进一步实施。由于角色工程师无法使用标识符参考具体的业务任务，因此不论是否存在定义，工程师常根据自己对用户能够执行的业务任务的过时解读创建LAM角色。最终导致IAM角色的业务含义丢失，或被应用开发者误读。如何解决这一问题呢？

为解决这一问题，在IAM整个生命周期内IAM角色的业务意义应可参考及追踪至对应的业务任务。这是能够大幅改善整个的IAM程序生命周期的关键基础特征。如何实施这一质量特征呢？为业务分类实施应用程序接口存在多个语义表述表征。（见附录V — 实施业务分类接口的可能机制）。

但是，在IAM整个生命周期内使业务含义具有可参考性和可追踪性还不够，还需要明确IAM角色的语义句法。

目前，IAM角色的句法由广泛使用的标准接入控制机制 – 基于角色的接入控制（RBAC）说明，如图1所示。

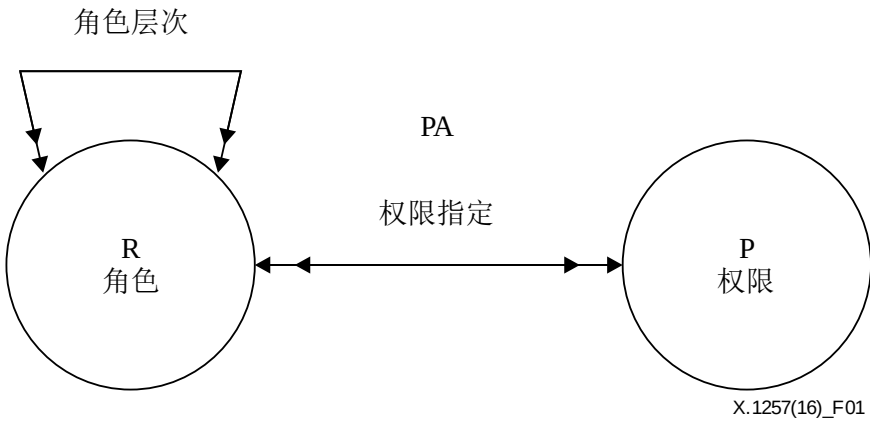


图1 – 传统RBAC模式

我们可以观察到以下角色句法：

- 角色可包含其他角色 — 即组成角色层次。
- 角色由权限构成。

但是，传统RBAC机制存在已知的局限 – 没有说明权限的语义（即“权限的本质”）。该机制的规格说明权限的语义可自由解释 –“权限可用读、写等原语操作定义，或贷项或借项等抽象操作定义。”[b-NIST-RBAC 2000]。但是，在引言介绍的实际操纵中，没有参考对应业务任务时会产生模糊的IAM角色。

为了向IAM角色指定业务含义，需要明确IAM角色的语义句法。含义将来自最精细的业务分类叶节点 – 任务和资源。图2描述了IAM角色的语义句法。

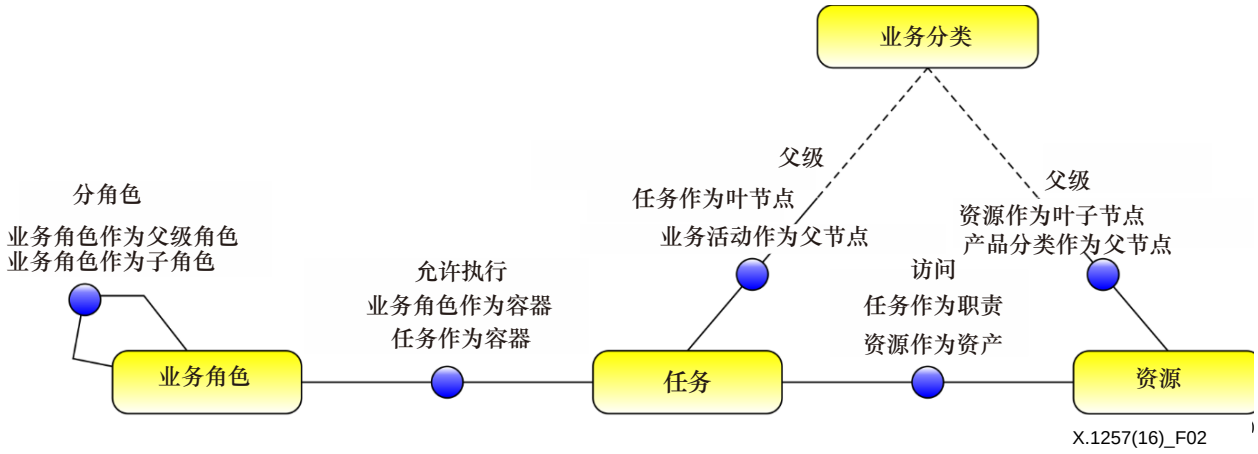


图2 – 基于任务的接入管理，概念图

我们可观察到以下内容：

- 角色（还）能通过分角色关系包含其他角色□— 即组成角色分级。
- IAM角色关键语义句法：
  - 业务角色使用户通过“允许执行”关系执行业务任务。这使任何IAM角色能从对应的业务任务继承其业务含义。

– 业务任务（非用户或角色）接入具体资源（即“业务产品”）。“接入”关系为可选关系，需要更精细的范围控制环境。
– 任务和资源作为业务分类的叶节点，是IAM角色工程中的先决构建模块，且在整个IAM生命周期内具有可参考性。

为简单起见，图2中未显示任务和资源产品的父类型。

Table 1以上句法的一些权利有助于表述上述观点：

表1 – 权利示例

业务角色	任务	资源
讲述人	建立账户	进一步检查账户
医生	核对病史	病史
系统管理员	升级系统环境	系统环境

以上IAM角色的语义句法能够实现我们的目标 — 为IAM角色指定业务含义。以下条款将以要求的格式表述建议的方法。

8 IAM角色语义和句法要求

以下是为IAM角色指定必要业务含义的建议：

1) 业务分类作为IAM程序生命周期中的先决输入内容，在整个生命周期内为IAM角色和用户权限提供业务含义。
2) 在IAM整个生命周期内，IAM角色的业务意义应可参考及追踪至对应的业务任务。
3) IAM角色具有以下语义句法：
   3.1) IAM角色由用户有权执行的业务任务构成。
   3.2) IAM角色由选择性接入具体业务资源的业务任务构成，如果需要更加精细的接入控制的话。
4) 通过参考对应的业务任务标识符记录成功执行的业务任务，以及未授权业务任务执行请求。

附件A

（本附件为本建议书的组成部分）

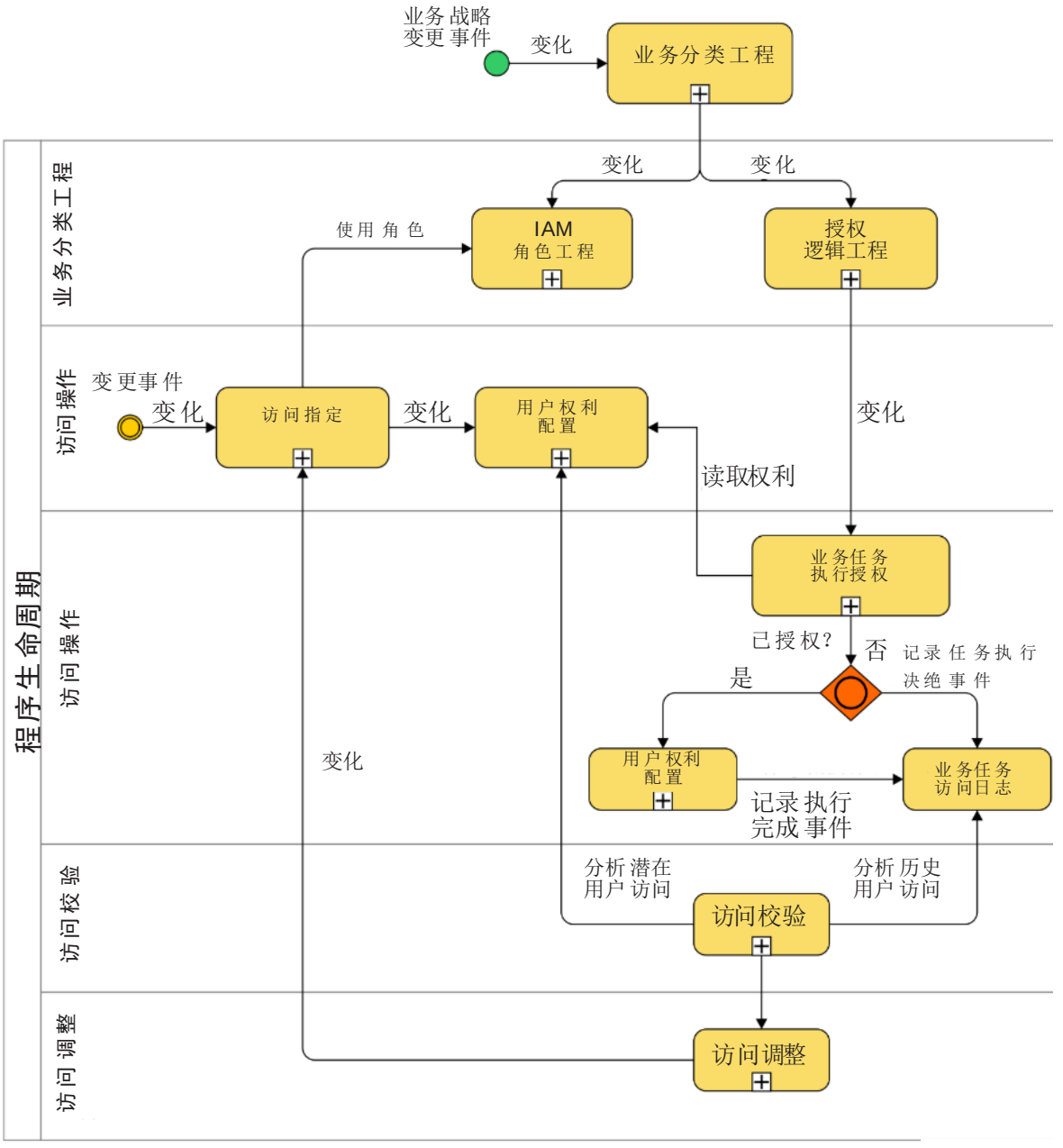
文件本部分空白，用于填写IAM基于任务的接入管理在未来可能的实施场景。

附录I

IAM分类程序生命周期

（本附录不是本建议书的组成部分）

图I.1强调的事实是，整个IAM程序生命周期主要受业务分类的变化影响。这些业务分类变化将由IAM角色工程和授权逻辑工程团队订阅和消耗。变化将包括对应人工制品中的业务任务标识符，如IAM角色、授权逻辑源代码、业务任务执行和授权日志文件。



X.1257(16)_FI.1

图I.1 – IAM程序生命周期依赖关系

变化的第二个来源是人力资源事件，如雇佣、休假、流动等事件。这些事件由接入变化请求管理程序处理，对应用户权利将向权利目录提供。值得注意的是，这些权利中包括指向提供业务含义的业务任务的标识符参考，应用程序运行授权时会参考这些标识符。一旦用户获得认证后，（为简单起见不予显示）预防性SoD控制将在运行授权时限制执行冲突业务任务。在业务任务执行授权程序中，或者授权用户执行任务以及任务得到执行，或者未授权用户执行任务。在两种情况下，应用将通过参考对应业务任务标识符记录这些事件。以下为可能的日志模板：

```
2016-02-08 22:20:02,165 ait:AppID1 192.168.0.1 UserID123 btt:TaskID1 btr:456:355 bttes:200 "任务成功完成。"
2016-02-08 22:24:02,165 ait:AppID1 192.168.0.1 UserID123 btt:TaskID2 bttes:401 "未授权用户执行此任务。"
```

其中：

- btt – 为命名空间名称，用于分解为HTTP URL的前缀，如http://example.com/mylob/businesstaxonomy/task/
- btt:TaskID1 – 为业务任务标识符。当该业务任务标识符被附加了btt命名空间名称，可用于检索其他业务任务信息，如任务名称、任务描述和任务使用统计。
- bttes – 为命名空间名称，用于分解为HTTP URL的前缀，如http://example.com/mylob/businesstaxonomy/task/execution/state
- bttes:200 – 为任务执行状态代码，表示成功执行任务。
- bttes:401 – 为任务执行状态代码，表示任务执行未授权。

由于业务任务在日志文件中以语义的方式进行引用，接入校验员能够在业务任务执行方面分析历史用户接入和潜在用户接入。一旦完成用户接入的全面分析和校验，对应调整变化将发回接入变更请求管理，用于修订过度（不足）的特权用户接入权利。这些调整变化是重要的环回机制，体现了生命周期程序的特点 — 即IAM程序生命周期。但是，中小企业并不需要所有阶段。例如，不考虑应用授权逻辑工程，或由用户目录组件实施。图I.1仅包括IAM程序整个生命周期的关键部分。

以下分层项目列表是IAM程序生命周期的文本表述。第“3.2本建议书定义的术语”中也定义了每个分类节点。编码表述见单知识组织系统（SKOS）模式。

1 业务变化管理
  1.1 业务分类工程
    1.1.1 业务程序变化
    1.1.2 业务产品变化
2 接入工程
  2.1 IAM角色工程
  2.2 授权逻辑工程
3 实体身份管理
  3.1 ITU-T X.1254“注册阶段”（实体注册）
    3.1.1 应用和启动
    3.1.2 身份证明
    3.1.3 身份验证

附录II

SCIM 2.0扩展文件建议

（本附录不是本建议书的组成部分）

本附件建议将扩展文件作为跨域身份管理（SCIM）2.0 [1]— 表述性状态转移(REST) web服务协议[b-SCIM REST]的基础。图II.1展示了建议的扩展文件。黑色部分的图线和图块代表当前SCIM1.0 [b-IETF SCIM 1.0]的核心部分。蓝色部分（“角色”和“权利”）的图块表示SCIM的扩展点。橙色部分的图线和图块代表建议的扩展。由于SCIM的规格使“角色”和“权利”的语义实质可通过实施进行解读和定义，[2] 可以进一步明确扩展点，使其成为核心标准的一部分。

为向IAM角色指定业务含义，建议将以下建议作为当前SCIM规格的扩展文件：

- SCIM“角色”扩展点作为业务角色容器，业务角色由一个或更多业务任务组成。
- SCIM“权利”扩展点作为用户可以执行的（用户可通过指定业务角色执行的业务任务义务的）其他业务任务容器。

---

1 “跨域身份管理（SCIM）规范旨在简化基于云的应用和服务中用户身份管理。”来源 http://www.simplecloud.info/

2 通过实施以下内容，SCIM具有解读和定义空间：

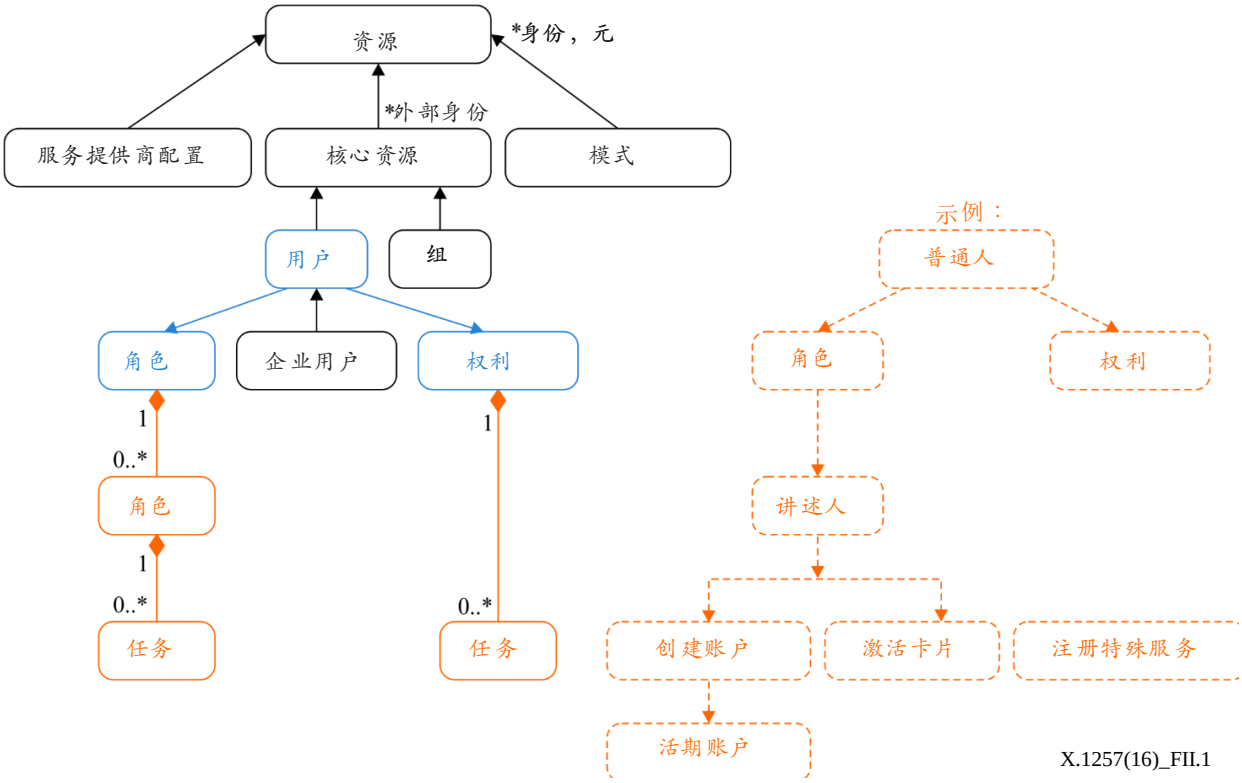
权利

用户的权利清单，代表用户拥有的事物。即，权利是事物、目标或服务的额外权利。由于没有制定具体的词汇或句法，需要服务提供商/消费者在数值中编码足够的信息，明确无误地确定拥有哪些访问权利。数值不具有规范类型，尽管类型有助于划定权利。

角色

用户的角色清单，总体代表用户的身份；如“学生”、“教员”。尽管角色值是代表权利集合的字符串或标签，但没有明确具体的词汇或句法。数值不具有规范类别。

来源 https://tools.ietf.org/html/draft-ietf-scim-core-schema-22



图II.1 – SCIM扩展文件

示例中右侧橙色显示用户如何拥有业务角色“讲述人”，角色由两个任务构成：“创建账户”及“激活卡”。另一个任务 — “注册特殊服务”是无需创建角色的直接额外权利。

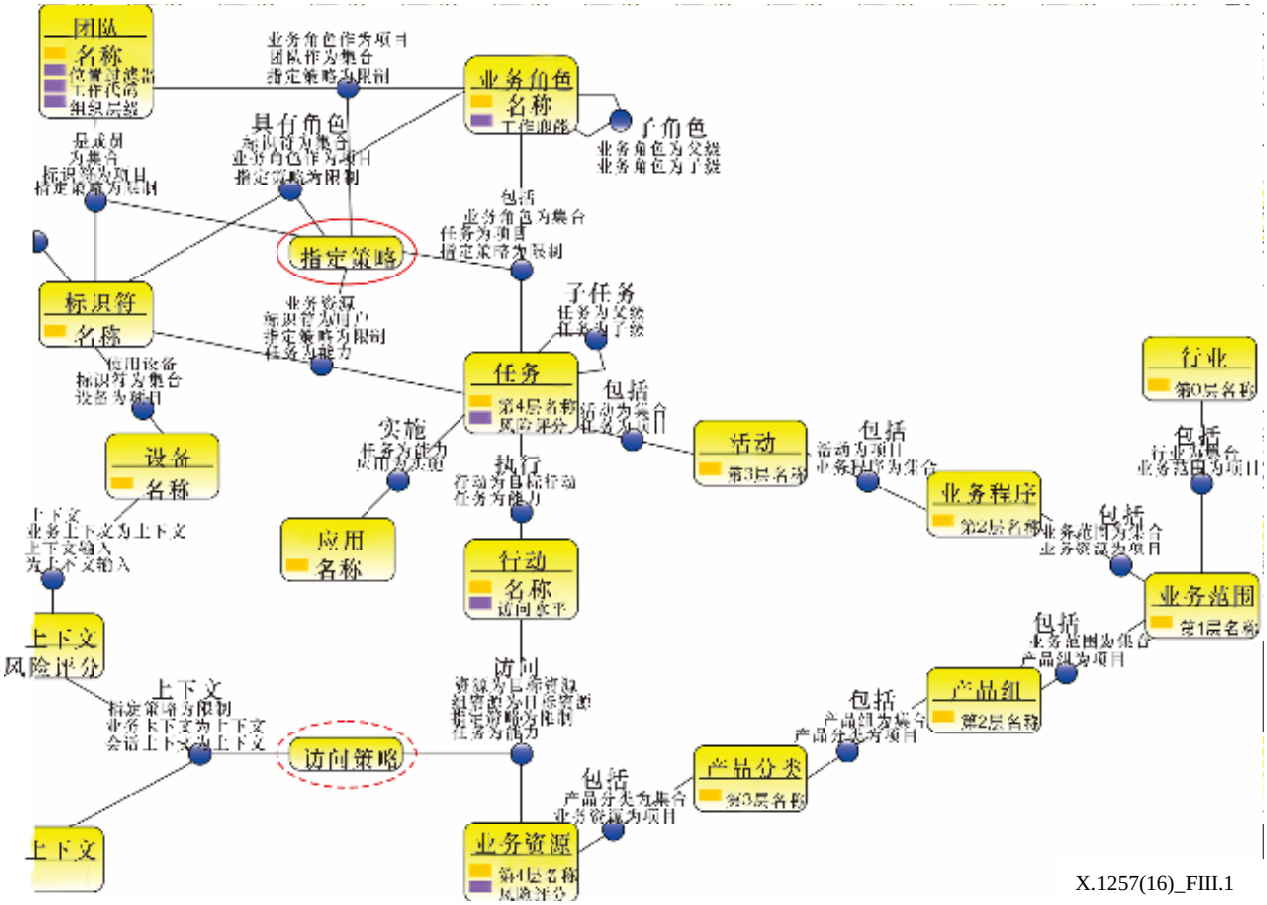
附录III

XACML 3.0扩展文件建议

（本附录不是本建议书的组成部分）

为实现本工作下的IAM数据质量目标，建议以下扩展文件。

本建议将介绍新的XACML 3.0 [b-OASIS XACML 3.0]策略类型 — 类型指定策略（红实线标记处） — 在接入请求时间内对该策略进行评估。例如，在接入分配时间评执行职责分配规则的接入策略。另一方面，接入类型策略（红虚线标记处）是在运行时间评估的策略，通常更为复杂（细粒度）。图III.1显示IAM方案的一个部分，侧重拟议的分配政策。



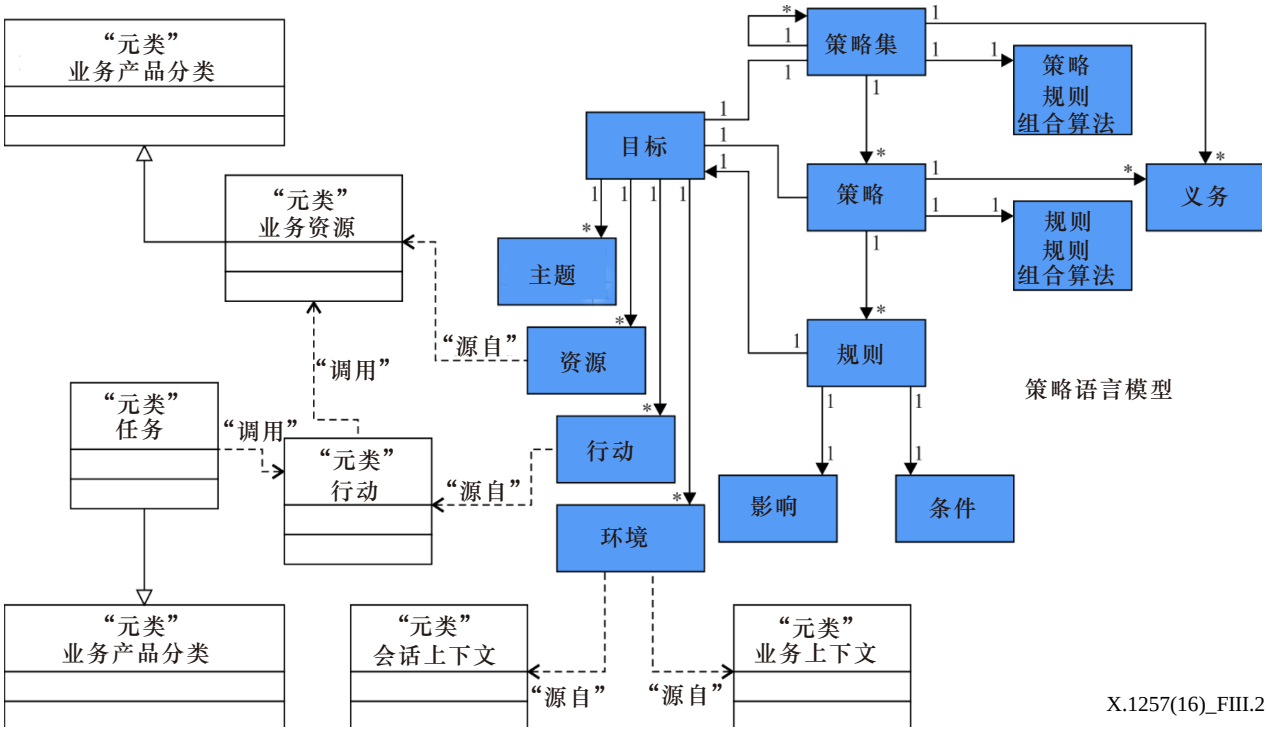
图III.1 – 强调分配策略的IAM模式片段

为可扩展访问控制标记语言（XACML）模型提供业务语义：

a) 通过业务资源概念id参考资源属性。业务资源是业务产品分类的叶节点。

b) 通过任务和行动概念id参考行动属性。任务是业务程序分类的叶节点。行动是在业务资源上执行的操作。

c) 通过业务上下文和会话上下文概念id参考环境属性。业务上下文能提供细粒度业务属性，如账号过滤器。知晓认证状态的会话上下文（凭证和设备元数据）能够为技术细粒度授权提供互联网协议（IP）地址和媒体接入控制（MAC）设备地址等信息。



图III.2 – XACML模型的建议语义扩展

附录IV

基于任务的接入管理用例

（本附录不是本建议书的组成部分）

以下相关用例显示了本建议书的作用：

1) 接入政策：
   a) 用户A通过业务角色A有权执行业务任务A、B和C。
   b) 用户A还通过直接权利有权执行业务任务D。
   c) 策略A明确任务B和任务D 对于同一账号相互排斥。
   d) 评估策略A，对上述给定场景得出否定决策。
2) 接入（权利）报告：
   a) 利用任务概念改善当前业务语言权利说明的可读性和含义。
   b) 利用业务资源概念改善当前业务语言权利说明的可读性和含义。
3) 业务任务使用
   a) 利用现有参考网络应用，并：
      i) 配置应用日志模板，使用业务任务id。
      ii) 在应用运行期间产生日志文件。
   b) 通过分析工具使用应用日志文件：
      i) 在生产运行期间使用业务任务报告。
      ii) 通过上述统计信息升级业务分类。
4) 权利使用
   a) 利用现有参考网络应用，并：
      i) 配置应用日志模板，使用业务任务id。
      ii) 在应用运行期间产生日志文件。
   b) 通过分析工具使用应用日志文件：
      i) 基于任务标识符关联业务任务执行事件。
      ii) 基于任务标识符关联授权否定事件。
      iii) 生成分析报告，说明SoD与场景在过去存在冲突。

附录V

实施业务分类接口的可能机制

（本附录不是本建议书的组成部分）

基于标准的解决方案，如SKOS[3] [b-Antonie]控制词汇或元数据注册机制，能够提供业务分类概念识别和注册。SKOS尤其利于表述分层关系。

另一种解决方案是使用基于JavaScript对象表示法（JSON）的链接数据序列化 (JSON-LD) [b-W3C JSON-LD]，也称为JSON-链接数据。尽管JSON-LD允许混合各种控制词汇，能够表示复杂的图形关系，分类接口并没有标准。在这一点上还没有REST或实施简单对象接入协议（SOAP）。

[3] SKOS提供基本分层管理，如更宽和更窄，但并不允许需要表述LAM数据元句法和含义的具体本体关系。

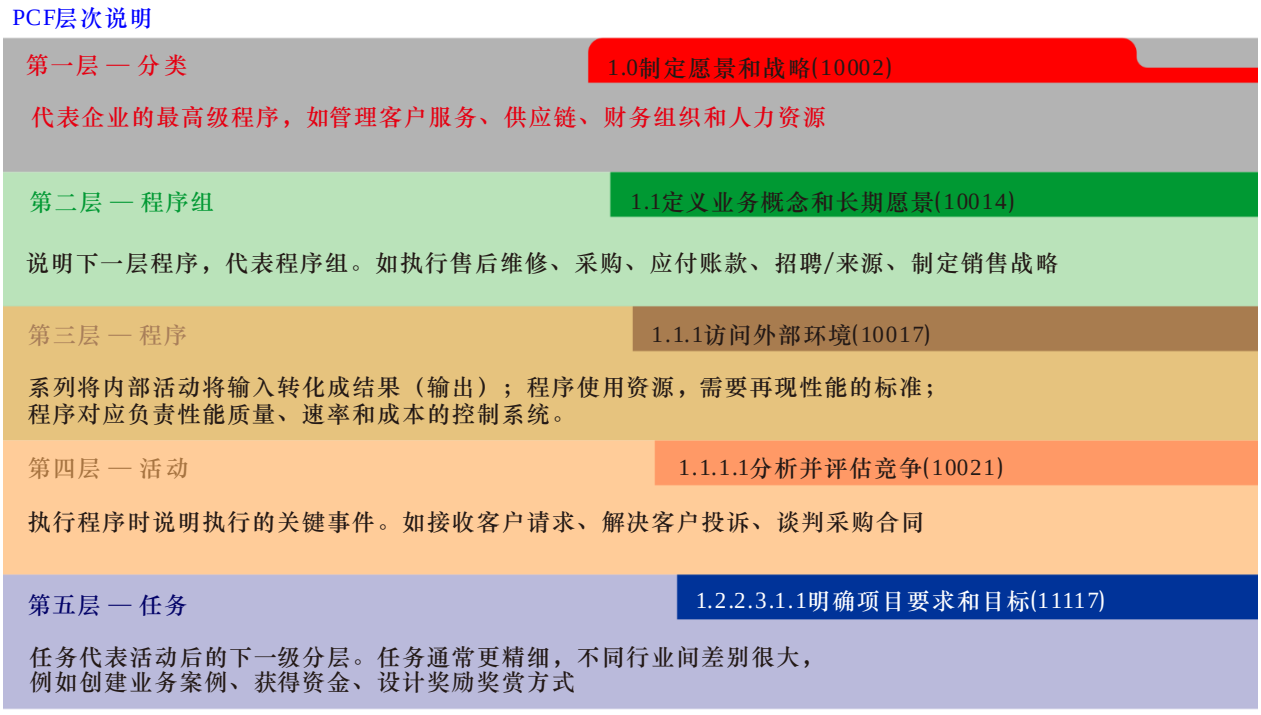
附录VI

业务程序分类标准

（本附录不是本建议书的组成部分）

本建议书至少参考了两类业务分类：业务程序分类和业务产品分类。这些术语由业务程序管理标准机构制定，如电信管理论坛增强电信运营图（eTOM）和中心产品分类目录（CPC）[b-CPC]。

图VI.1的另一个示例显示了美国生产和质量中心（APQC）[b-APQC-PCF]的程序分类框架（PCF），展示了程序如何分类。



图VI.1 – PCF业务程序分类结构定义

附录VII

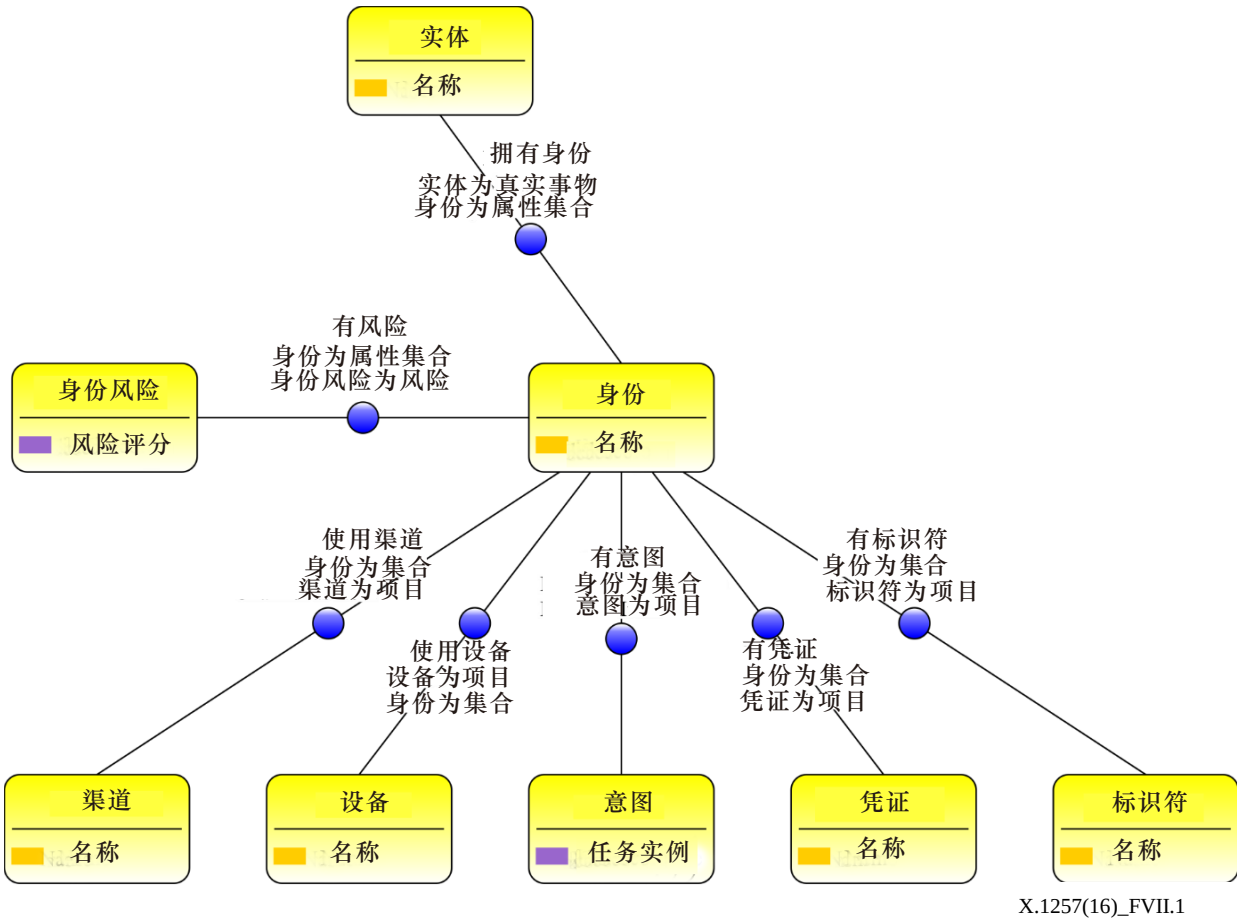
IAM本体域模型

（本附录不是本建议书的组成部分）

本附件最后一图VII.5描述了整个IAM本体域模型。为使读者便于理解IAM域，首先介绍以下IAM主题范围：

- 图VII.1，IAM域模型 – 用户主题范围
- 图VII.2， IAM域模型 – 接入指定主题范围
- 图VII.3， IAM 域模型 – 接入控制主题范围
- 图VII.4，IAM域模型 – 业务域主题范围

最后，以上主题范围将融合成整个IAM域模型。第一个主题范围涉及用户概念类型。根据ITU-T X.1252建议书 [ITU-T X.1252]和X.1254建议书 [ITU-T X.1254]，用户由实体从多个方面代表，如是主题或以主题存在。一个实体有一个或多个身份。一个身份有一个或多个标识符。

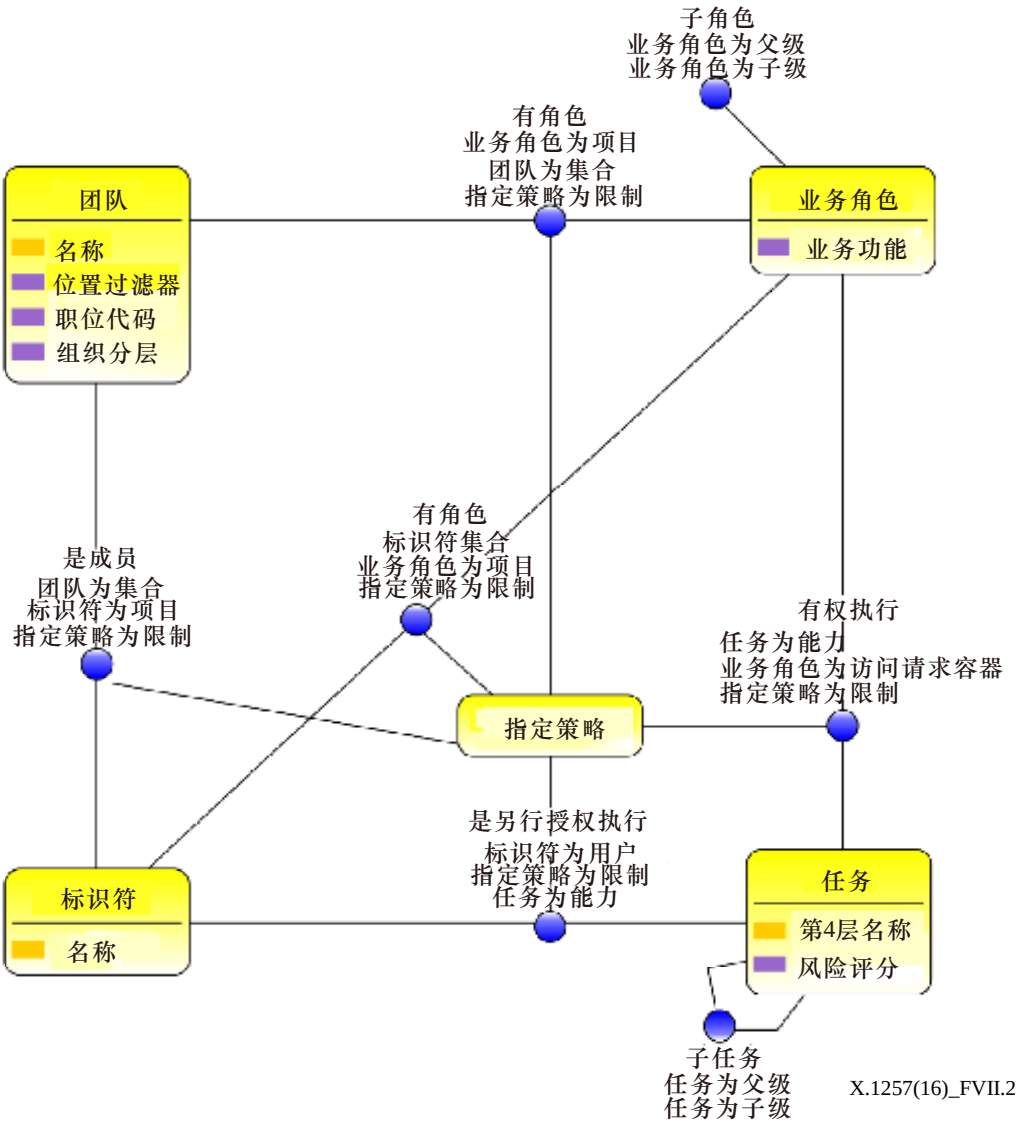


图VII.1 – IAM域模型 – 用户主题范围

示例：一个人拥有体现姓名、生日等特征的实体。这个人可以同时是雇员和客户，因此至少拥有两个身份。因此，雇员和客户将分别拥有雇员身份和客户身份作为标识符。

注 – 在一些情况中，设备代表人发挥人的角色。

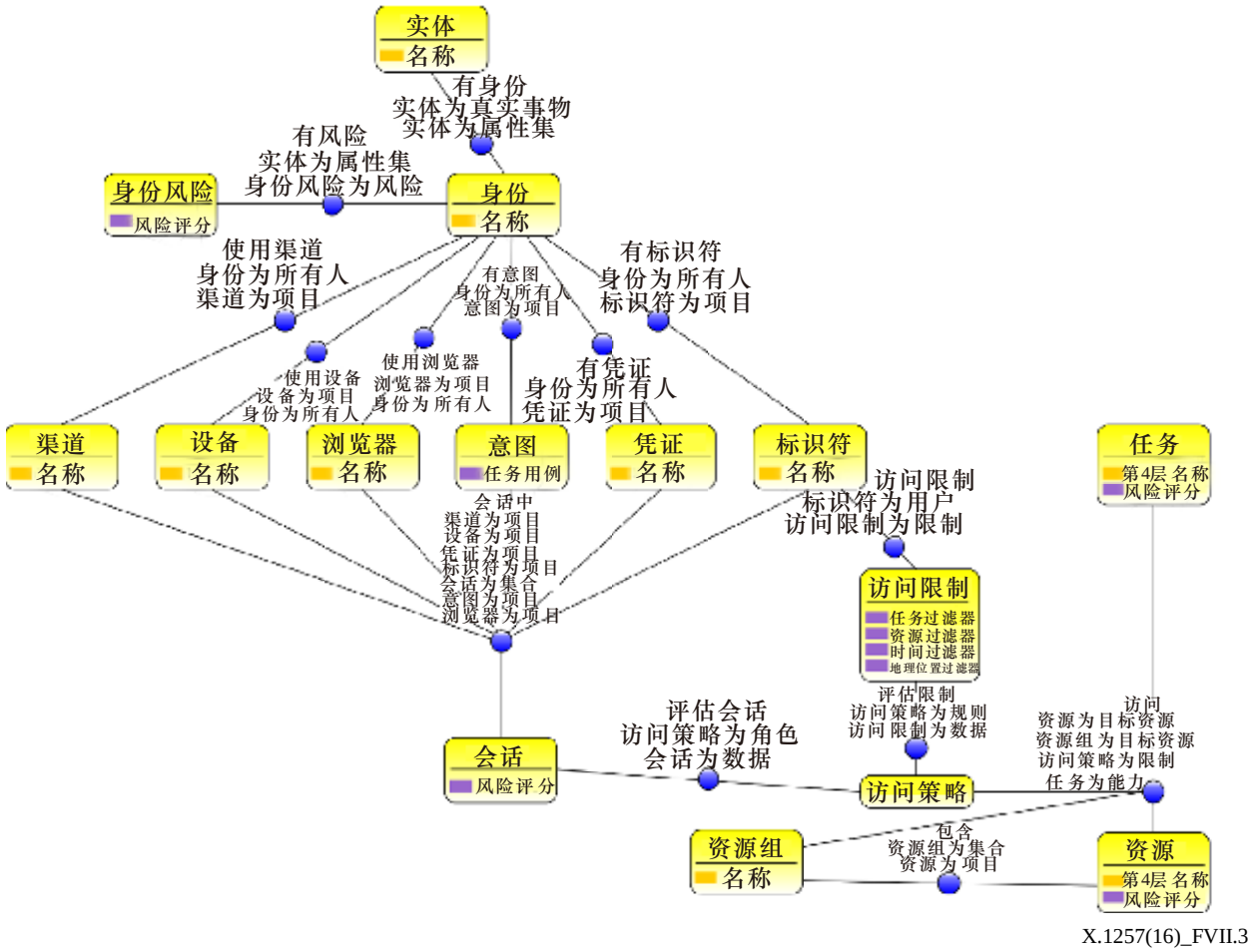
下图VII.2显示主题范围是接入指定，处理通过用户标识符向用户指定接入权利。接入权利可通过他或她隶属的团队进行指定。此处上下文中的团队是人力资源推动型接入权利的容器。除团队成员接入权利外，用户还可通过他或她的业务角色获得接入权利。最后在例外情况下，用户可有权执行部分业务任务。但是，需通过适用的“指定策略”评估所有用户至任务的指定。“指定策略”用于排除不良授权组合，执行职责分离规则。



图VII.2 – IAM域模型 – 接入指定主题范围

示例：用户A是团队X的成员。每个位于总部（即地区=主要，服务台=主要）的X团队成员拥有5个业务角色，每个业务角色使用户能够执行十个任务。因此默认状态下，任何团队X成员都能执行50个任务。此外，还向用户A指定了另外三个业务角色，使用户能另外执行五个任务。作为例外情况，用户A还有权直接再执行一个任务。最终，用户A有权执行66个任务。但是，不在总部的用户只有三个业务角色---即不到30个业务任务。

接入控制室另一个主题范围，根据用户权利和会话上下文执行基于策略和任务的授权。若对应接入策略允许接入，则具体任务能接入资源。接入策略将分析拥有会话上下文和对应用户接入限制的规定。会话上下文将拥有用户认证元数据，如渠道、设备、意图、凭证和标识符。

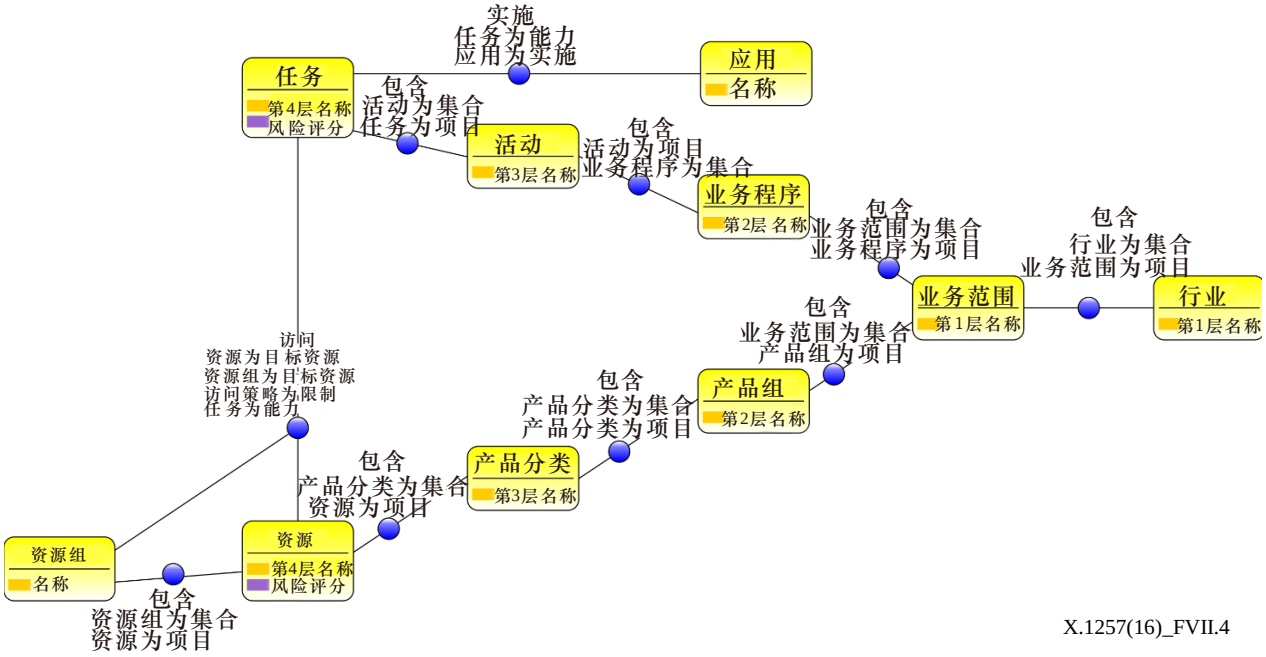


X.1257(16)_FVII.3

图VII.3 – IAM域模型 – 接入控制主题范围

示例：用户A计划执行“创建账户”任务。此任务将接入（即创建）“优势活期账户”业务资源。若对应接入策略评估为真，将发生接入。接入策略将确保特定用户必须为此处理过程使用合适的渠道，IP地址属于有效的IP地址范围。由于已经不再业务时间，策略此时还可查询未授权任务的瞬态缓存。

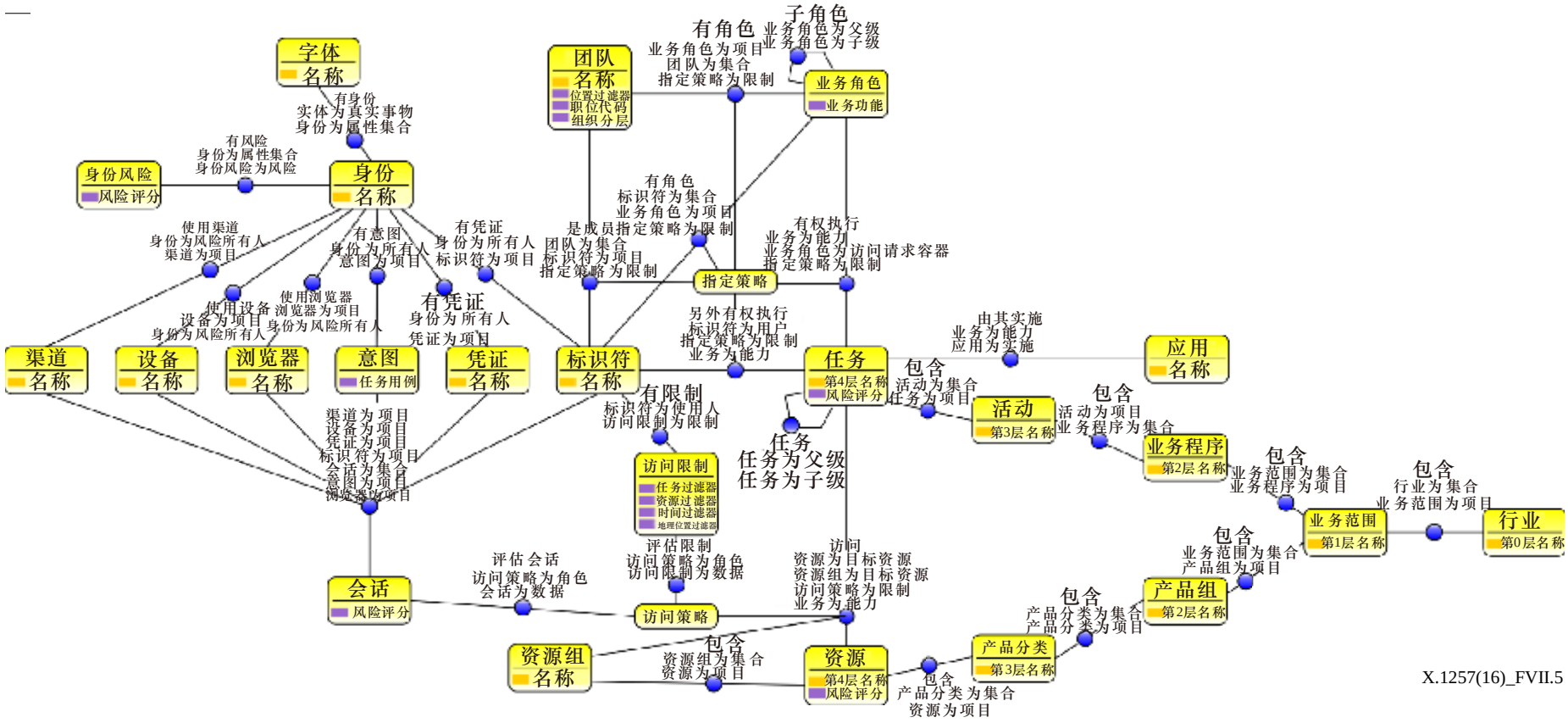
最后一个主题范围 – 业务分类 – 展示了IAM域和业务域如何互动。业务域由业务程序和产品构成。我们可以看到（从右至左）行业和业务范围是此分类的头两级。业务程序和业务产品分类从业务范围和右侧两个相关分解结构中进行展示。通常，任务在业务程序分类中是叶节点，业务资源在业务产品分类中是叶节点。应用代表用户实施对应的任务，执行资源接入。



图VII.4 – IAM域模型 – 业务域主题范围

示例：行业为金融业。业务范围为客户服务。业务程序为组织。活动为账户活动。任务是“创建账户”。从业务产品分类角度看 – 产品组是账户、产品分类为活期账户、业务资源是“优势活期账户”。

最后，图VII.5展示了整个IAM域模型，与上述四个主题范围相连。



图VII.5 – IAM域模型

根据对相应部分规定的要求，以上域模型对概念之间的关系进行建模。本图展示了以下关键原则：

- 用户由实体、身份、标识符和其他特征代表。在权利指定程序中，用户通过团队和角色有权执行具体任务（通常占80%的时间），或者直接指定执行具体的任务（以特例形式占20%的时间）。
- 团队是角色的人力资源容器。团队和业务角色类型的主要目的是加速和简化权利指定和批准程序。
- 业务角色应从对应业务任务中继承业务含义。

注 – 目前，由IT创建和维护IAM角色，因此不具有可直接追溯的业务含义。在许多案例中，仅靠角色名称传递业务含义不足以成功校验接入权利。

- 任务是业务程序分类的叶节点，业务程序分类由业务架构师和业务建模师创建和维护。
  - 任务比实施任务的应用具有更细的粒度。
  - 任务由对应应用实施。
  - 任务在职责分离用例中代表职责。

注 – 没有基础业务任务，无法实施职责分离。

- 用户无法直接接入业务资源。用户可以有权执行业务任务，业务任务可代表用户接入业务资源。
- 程序—活动—任务是逻辑结构，也是业务程序分类的一部分，用于以标准[b-APQC PCF 5.0.1]方式确定和组织业务程序，通常由业务架构师和业务程序建模师维护。
- 产品组—产品分离—业务资源是逻辑结构，也是业务产品分类的一部分，用于以标准[b-CPC Ver 2]方式确定和组织业务产品，通常由业务架构师和业务程序建模师维护。
- 指定策略是在权利指定阶段使用的权利指定限制机制，用于防止虚假及静态不良业务任务组合。
- 接入策略是在运行接入阶段使用的接入运行限制机制，用于防止虚假及动态运行时的不良组合。
- 业务资源是概念，如病例、贷款账户和活期账户。业务资源使细粒度资源水平上的权利指定和接入控制成为可能。
- 业务权利是用户有权执行的任务（即粗粒度业务权利）。
- 业务权限是接入具体业务资源的任务，受策略限制。
- 在用户权利配置阶段，必要的话业务权利可映射至对应业务权限。
- 系统权限处理系统资源，如数据库、表格、列、文件或大型机数据。

参考目录

[b-ITU-T X.1255] ITU-T X.1255建议书（2013年），身份管理信息发现框架。

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2011，信息技术 – 安全技术 – 身份管理框架 – 1部分：术语和概念。

[b-Antonie] Antoine Isaac, E. S.（2009年8月18日），SKOS简单知识组织系统基础，2013年8月7日检索，来源w3: http://www.w3.org/TR/skos-primer/

[b-APQC-PCF] Tesmer, John （2014年3月），程序分类框架*6.1.1*. http://www.w3.org/TR/skos-primer/（2016年5月18日检索）

[b-APQC PCF 5.0.1] APQC PCF. (2011年6月)，银行程序分类框架。2013年8月7日检索，来源美国生产力和质量中心(APQC)：http://www.apqc.org/knowledge-base/download/33193/PCF_Banking_Ver_5.0.1_2011.pdf

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

[b-CPC Ver 2] CPC工作组。（2008年12月31日）。中心产品分类目录，第二版本，详细结构和注解。2013年8月7日检索，来源联合国统计署：http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=25

[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年4月15日），跨域身份管理系统：核心模式。2013年8月7日检索，来源IETF: http://tools.ietf.org/html/draft-ietf-scim-core-schema-01

[b-IETF SCIM 2.0] Hunt, e. a.（2015年6月8日），跨域身份管理系统：核心模式。2015年8月6日检索，来源IETF工具：https://tools.ietf.org/html/draft-ietf-scim-core-schema-22

[b-NIST-RBAC 2000] Sandhu, R.、David, F.和Khun, R.（2000年），基于角色的接入控制NIST模型：向统一标准发展。

[b-OASIS XACML 3.0] Erik Rissanen.（2013年1月22日），可扩展的接入控制语言（XACML），版本3.0。2013年8月7日检索，来源OASIS：http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[b-OBAC] Mohammad, A.（2011年3月7日），语义网基于本体论的范文控制模型。2013年8月7日检索，来源世界学术出版社：http://www.worldacademicunion.com/journal/1746-7659JIC/jicvol6no3paper03.pdf

[b-schema.org 2011] 谷歌、雅虎、Bing、Yandex.（2011年），schema.org。2013年8月7日检索，来源schema.org：http://schema.org

[b-SCIM REST] SCIM 2.0 REST网络服务协议，C. Mortimore, Ed.，2013年：http://www.simplecloud.info/

[b-W3C JSON-LD] Manu Sporny（2013年8月6日），JSON-LD 1.0，基于JSON的链接数据序列化。2013年8月7日检索，来源JSON-LD.org：http://json-ld.org/spec/latest/json-ld/

ITU-T 系列建议书

系列 A	ITU-T 工作安排
系列 D	一般关税原则
系列 E	整体网络运营、电话业务、服务运营和人为因素
系列 F	非电话电信服务
系列 G	传输系统和媒体、数字系统和网络
系列 H	视听和多媒体系统
系列 I	综合服务数字网络
系列 J	有线电视网络和电视的传播，合理的计划和其他多媒体信号
系列 K	干扰防护
系列 L	环境和信息通信技术、气候变化、电子垃圾、能源效率；结构、安装和电缆保护以及外部设备的其他因素
系列 M	电信管理、包括电信管理网和网络维护
系列 N	维护：国际广播节目和电视传输电路
系列 O	测量设备说明书
系列 P	终端和主观及客观的评价方法
系列 Q	交换和信令
系列 R	电报传输
系列 S	终端服务终端设备
系列 T	远程信息处理服务终端
系列 U	电报交换
系列 V	电话网络之上的数据通信
系列 X	**数据网络、开放系统通信和安全**
系列 Y	全球信息基础设施,网络协议方面和下一代网络
系列 Z	电信系统的语言和通用软件方面

瑞士印刷
2016年，日内瓦