国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1255

(09/2013)

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

发现身份管理信息的框架

ITU-T X.1255 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
生物测定安全	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
IPTV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
网络安全信息交换	
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
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1255 建议书

发现身份管理的信息框架

摘要

ITU-T X.1255建议书的目的是提供开放架构框架，在该框架中可发现身份管理（IdM）信息。这一IdM信息有必要以不同方式得到呈现，并由多种不同信任框架或使用不同元数据模式（metadata schemas）的其它IdM系统支持。例如，这一框架将方便在一个IdM环境中运行的实体获得得到准确解析的来自其它IdM系统的识别符。若不具备发现此类信息的能力，则用户和组织（或代表其运行的程序）则须确定如何最佳明确用户、系统资源、信息或其它实体的适当身份的可信度和真实性。在这一信息基础上，用户或组织可决定是否依赖特定的信任框架或其它IdM系统。本建议书确定的上述框架的核心成份包括：1) 数字对象数据模式，2) 数字对象接口协议，3) 一个或多个识别符/解析系统，4) 一个或多个元数据注册表（registry）。这些成份共同构成开放架构框架的基础。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T X.1255	2013-09-04	17

前言

国际电信联盟（ITU）是从事电信、信息通信技术（ICT）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）是国际电信联盟的常设机构，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。

每四年一届的世界电信标准化全会（WTSA）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1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“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或适用性等），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

国际电联提请注意：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、有效性或适用性不表示意见。

至本建议书批准之日止，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，这可能并非最新信息，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/。

© 国际电联 2013

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页码

1 范围 1
2 参考文件 1
3 定义 1
3.1 其它地方/建议书定义的术语 1
3.2 本建议书定义的术语 2
4 缩写词和首字母缩略语 3
5 惯例 3
6 建议 3
6.1 信任概念 4
6.2 信任信息 4
6.3 联邦发现注册表 5
7 联邦注册表的互操作架构 7
7.1 数字实体数据模式 7
7.2 数字实体接口协议 10
7.3 与注册表的互动 11
7.4 解析系统 12
7.5 联邦注册表中的分布式查询和汇集元数据 12
7.6 元数据模式 15
7.7 元数据互操作性 15
8 类别和类别属性 15
9 分层联邦和对等联邦 17
附录一 – 使用情形 20
附录二 – 类别记录的BNF表示法 24
参考文献 26

ITU-T X.1255 建议书

发现身份管理信息的框架

1 范围

发现身份管理信息涉及人们必须有能力获得有关识别符的相关信息，包括使用电子邮件地址句法和URL识别符的信息以及持续识别符。这种发现是促成异质信息系统之间互操作性的一项关键要素。

本建议书的范围是确立这样一种框架：

- 有助于发现与身份相关的信息及其出处，包括正在得到识别的诸如服务、程序和实体等的信息；
- 便于发现与身份相关的信息属性，包括但不限于视觉标识和人们可读的站址名称；
- 方便发现应用的属性和功能性；
- 描述数据模式和协议，以便于在元数据层面实现呈现互操作性、在异质IdM环境中获取和发现以上所述信息。

2 参考文件

下列ITU-T建议书和其他参考文献的条款，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，本建议书的使用者应查证是否有可能使用下列建议书或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。本建议书引用的文件自成一体时不具备建议书的地位。

[ISO 8601] ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times*.

3 定义

3.1 其它地方/建议书定义的术语

本建议书使用下列其它地方/建议书定义的术语：

3.1.1 实体[b-ITU-T Y.2720]：任何可被独特识别的单独存在的东西。在IdM范畴内，实体示例包括用户、使用者、网元、网络、软件应用、服务和设备。一个实体可能具有多个识别符。

3.1.2 身份提供商[b-ITU-T Y.2720]：创建、维护和管理其它实体（如，使用者/用户、组织和设备）可信赖身份信息的实体，它基于信任、业务和其它类型的关系提供与身份相关的服务。

3.1.3 依赖方[b-ITU-T Y.2720]：依赖于身份表述或申请/断言实体声明的实体。

3.1.4 信任[b-ITU-T Y.2720]：对某个人或某物特性、能力、优势或真实情况一定的依赖。

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 关联：两个被识别实体之间的关系（如有的话）。

3.2.2 数字实体：显示或转换为与机器无关的数据结构的实体，包括一个或多个数字形式的可由不同信息系统解析的元素；该结构有助于实现互联网上多种信息系统之间的互操作性。

3.2.3 发现：寻找或对目标信息予以定位的行为或过程，即，了解有关目标的信息。

3.2.4 元素：包含类别数值对的一部分数字实体，其中类别由可被解析的持续识别符呈现，数值是该类别的相关数字信息。

3.2.5 联邦注册表：一系列可互操作的注册表，对元数据进行注册并参与一套共同方法，以便可靠地、以共同理解的格式内分享信息。

3.2.6 识别符：一系列用以获得被识别数字实体状态信息的比特，通常通过相关解析系统完成。

3.2.7 身份管理：可证实用户、系统资源、信息或其它实体身份管理信息的手段。

3.2.8 身份管理信息：包括与身份、出处、关联性和信任相关的所有类型元数据的身份相关信息。

3.2.9 元数据：与用户、系统、服务、程序、资源、信息或其它实体有关的结构信息。

3.2.10 持续识别符：解析数字实体状态信息、且至少在数字实体存在时可得到解析的独特识别符。

3.2.11 出处：与任何信息源相关的信息，包括生成该信息、引入该信息和/或为该信息担保所涉的任何方面。

3.2.12 注册表：对有关数字实体的元数据进行注册并存储元数据模式的机制，它提供的能力有助于在所用元数据模式基础上搜索注册表，找出持续识别符。

3.2.13 存储库：接受数字实体交存的接口，有助于保留数字实体并通过其识别符安全获取数字实体。

3.2.14 解析系统：将系统了解识别符作为输入予以接受并提供正在得到识别实体的相关状态信息的系统。

3.2.15 触点：联邦注册系统中的一个注册表，被选则与另一个联邦中指定注册表进行连接，通常出于对等目的。

3.2.16 信任框架：一种IdM系统，在该系统中，一项交易所涉不同各方的每一方都向其交易对手做出一系列可核实的承诺，这些承诺需要包括：(a) 有助于确保承诺得到实现的控制机制以及(b) 不履行这些承诺的补救措施。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

API 应用程序界面

Bits 二进制数字

BNF 巴科斯范式

DE 数字实体

DEIP 数字实体接口协议

DNA 脱氧核糖核酸

HTTP 超级文本传送协议

ID 识别符

IdM 身份管理

IdP 身份提供商

MAC 媒体接入控制

P2P 对等

PKI 公共密钥基础设施

RP 依赖方

TCP 传输控制协议

TF 信任框架

URL 统一资源定位符

XML 扩展标记语言

5 惯例

无。

6 建议

本建议书旨在提出一个支持身份管理信息发现的开放架构框架，主要涉及下列主题：

a) 信任概念，这是身份管理的一个重要方面；

b) 信任信息，可用该信息确定在何种程度上依赖任何相关的IdM信息；

c) 用于发现的联邦注册表；

d) 有关联邦的互操作性架构；

e) 对分层和对等联邦均做出讨论。

身份管理信息的发现是以从注册表或联邦注册系统中获得的元数据的使用为基础的。相关框架包括，存在解析持续识别符的手段。总体而言，联邦注册表将由多方操作，因此，须支持数字实体数据模式，以呈现实现此类注册表互操作性的元数据记录和数字实体接口协议。现预先设想使用多模式，且每一个注册表均须提供其各自持续识别符公开和/或以私密

方式支持的元数据模式的细节。以私密方式支持的持续识别符的模式可在必要时公开化，亦或保持其秘密性以及相关的元数据模式，以仅限于在有限社区内使用。

本建议书附录一和二分别概要说明使用情形和类别记录的BNF描述示例（BNF是表示无语境语法的标准表示法）。

6.1 信任概念

“信任”一词是一种艺术术语，包含若干内含。信任某个人或某种程序通常意味着，对事件的特定结果具有一定程序的信心，即便这些事件未得到十分明确。然而，建立发现系统则需要有更多的规范。简单说A信任B，不意味着A在所有的可能事件结果方面都信任B。相信B会在得到特定付款后提供一种服务与相信B会保守支付秘密或不会将进行这种付款的所有人的名字都公开化不是一回事。

信任框架中最为重要的问题是身份管理，即，任何给定交易中所声称的各方是否真正是他们声称的那样。然而，对涉及特定方的特定交易结果的信心不仅取决于该方的身份，而且取决于该方所做出的声称和断言的其它属性。为连贯一致地评估这些属性，就需要有一整套可用于这些属性的词汇或度量指标。这些措施和描述可由作为信任框架评级机构的第三方应用，或可在用户群评级结果间进行平均（如同在建议系统和其他“人群搜索”应用中所作的一样）。以下阐述建议的此类措施和描述的类别。

程度：可信程度。该方将在多大程度上实现诺言？身份断言（如，我是该软件的作者，版税应当归我）在多大程度上是正确的？这可能由数字或字母评分表示。

分类：得到断言的是何种类型的信任？是否可以确立标准类别？身份本身是一种类别，其它类别包括财务信任（如，特定方将在何种程度上按照承诺在财务交易中行事）、隐私（特定方将在何种程度上保守其声称不会予以泄漏的个人信息）和权威性（如，从特定方收到的信息在何种程度上是准确的）。还可进行其它高层分类并将每一类分为更细的层次。

信任链长度：一些信任交易取决于信任链，人们常常从证书分级或数字签名软件层次来考虑信任链。通常这一概念适用于所有信任领域：受信任的断言离信任源越远则最终信任程度越低。信任链长度这一度量标准是任何身份或其它断言可信度的关键度量标准。

所有这些属性（以及其它诸多属性）都可被考虑纳入描述身份提供商、依赖方和受信交易所涉其它成份的元数据记录中。

6.2 信任信息

以下讨论联邦发现和参与构成实体所涉功能和行动的三种不同方面信任信息。

6.2.1 发现响应中的信任信息

本建议书确立的开放架构的首要目标是促进发现身份管理信息，但是否予以信任则由用户决定。在该架构中还可以可选成份/模块（软件和/或硬件）的形式支持更多功能性或服务。在此方面，架构可将信任框架作为可选功能予以纳入，同时利用信任信息改善/充实发现响应，甚或支持信任决定。外部实体将能确定他们是否希望直接收到这一信任信息。外部实体可决定关闭这一功能并设法自己收集信任信息，亦或根据其自身信息渠道做出是否予以信任的决定。

6.2.2 对发现系统的信任

必须信任发现系统，这样外部各方才有信心利用其功能对身份管理信心进行注册或获得这一信息。可通过各种手段实现这类信任，包括确立具体方法以及有关可靠性的相关政策和程序，其中可包括评估作为框架、行动（措施）一部分予以实施的成份，目的是应对行为不妥的构成成份或外部各方，并做出调整，采用更强健的安全和私密性框架。然而，确定实现这类信任的确切方法不属于本建议书的范围。

6.2.3 信任外部各方

架构必须支持这样的政策和程序，即，鼓励外部各方使用该架构来注册信息。出于安全原因，直接参与身份管理信息注册的构成实体必须能够控制加入到系统中的数据，并发现和/或避免怀有恶意的相关方面试图进行虚假信息注册的情况。

应支持匿名请求，但诸多这类匿名请求不会得到有益响应，除非事先通过一些其它手段已了解提出请求的个人的身份。在此类情况下，应由适用于所有构成方（包括用户/请求方）的身份管理功能来提供核实身份能力。在框架内，每一个构成成份都会由经授权和认可的身份提供商分配一个独一无二的持续识别符，该识别符可被解析至关于该构成成份的相关信息。如前所述，不设想具体实例中任何构成成份将如何决定是否信任这一信息。

对诸多请求而言，必须在做出响应前对请求者（发出发现请求的外部方）的身份予以核实。一般情况下，在采取任何进一步行动前，都会对所有请求方做出评估。架构不对其中起动的任何决策能力做出设想，然而，在对发现请求做出最终响应前，可能会起用外部决策支持机制，以便事先从身份产生方那里获得许可。

6.3 联邦发现注册表

本建议书阐述一种联邦发现注册系统，目的是有助于找到和评估有关识别符的元数据和其它信息，以及信任框架和其它IdM系统。联邦注册表可合作工作，在遵守任何适用的限制前提下，共享其元数据实体。与该元数据实际对应的信息可能存储在其各自的注册表中（如果允许进行这种存储的话），或存储在一个或多个分布式存储库中，且在有些情况下，对应这一元数据的信息可能无法通过互联网获得。在后一种情况下，限制与否通常由将识别符解析至有关实体的相关状态信息的行为确定，然而，注册表应可选择提供该信息。

在联邦注册系统中，特定注册表可将特定实体的元数据记录的完整副本或原记录摘要贡献给第二个注册表。贡献的可以是最初记录，也可以是被改变的最初记录，但其描述方法应该明确其来源，且应表现出该注册表所代表社区或领域类别的特性。由此，该原始注册表可成为其它诸多注册表的跨领域集合点，并提供可将搜索者引向其它注册表（以收集更多信息）的搜索服务。这类集合点有时称作触点（touch point）。

架构的注册成份是围绕若干关键性理念设计的。除要求为每一个已注册的数字实体分配识别符外，注册表中的元数据记录本身是数字实体结构，每一个实体都拥有一个相关的识别符。这有助于元数据记录得到单独参引，且其识别符将解析至有关元数据实体的现有状态信息，即使记录从一个注册表转移至另一个注册表，或由多个注册表提供。

架构中没有任何东西限制单一数字实体可注册的元数据实体数量。有时由于看待角度不同，受众不同等，可能需要为相同信息生成多个元数据实体。如果使用独一无二的持续识别符可大大简化这些元数据实体的管理工作：如，可以轻而易举地确定两个元数据记录是否参引同一下层信息。还可创建更多实体来将单个元数据实体相互关联，其方法是在不同单个实体间进行搜索而无法实现的。

架构有助于在存储库与注册表之间实现双向的多对多关系。特定存储库可将相同实体的元数据贡献给多个注册表；特定注册表可接受来自多个存储库的元数据。将来自多个存储库的元数据收入一个单一注册表中有助于实现存储库的联邦。方便存储库为多个注册表贡献有关相同实体的元数据有利于单个存储库成为多个联邦的一部分，可以通过为不同社区服务、使用不同元数据模式、以不同方式进行索引和搜索以及其它功能来将自身与其它各方予以区分。

最后，注册表实例可与其它注册表进行联邦。多个注册表可向每一个其它注册表推送其元数据实体或作为原始元数据记录函数的实体。称为注册表1的特定注册表可向称为注册表2的第二个注册表贡献特定对象的元数据记录（原始元数据记录的完整副本或该原始记录的摘要）。这种贡献可以是原始记录也可以是经改变的原始记录，并被纳入数字实体（DE）中，纳入方法能够确定其源自注册表1，并表明注册表1所代表的社区或领域类别特性。如果注册表1始终与注册表2联邦，则注册表2可成为诸如注册表1等的诸多其它注册表的跨领域收集点，并提供可将搜索者引向其它注册表或直接引向DE本身的搜索服务（取决于合并和对潜在异质元数据记录进行索引的方式）。

尽管本建议书的重点是身份管理，但这类系统也利于在互联网上复杂的分布式系统（如涉及“云计算”或“物联网”的系统）中发现其它类型信息。可从单个IdM系统中获得联邦注册系统的解析信息。使用联邦发现机制能够更普遍地实现IdM系统的互操作性，并提供适合于实体了解其它IdM系统的信息，从而帮助建立起对使用其它系统识别符的信任。

目前诸多群体在使用基本注册技术，其中一些人使用了开放原代码版本，其它人则根据共同了解的规范，开发了专有客户化版本。可通过信息共享协议实现联邦。未来基于本建议书的一项重要工作是描述并最终正式确立这些规范，以便确定适当的协议和程序以及相关元数据模式，同时酌情确定可被共同接受的旨在维护私密性的方式。相关方面如何选择或依赖特定IdM系统不属于本建议书的范围。

7 联邦注册表的互操作架构

本建议书所述联邦注册系统以有助于任意信息系统互操作的开放架构为基础。该系统提供信息认证和信息获取（这些信息的结构为数字实体并存储于多种类型的标准存储系统中）手段。数字实体是一种通用数据结构，有助于互联网上的系统实现互操作性，DE元素包括数字资料，即类别化数据，包括该资料独特的持续识别符。

在管理DE方面采用三个架构组成成份，其中每一个都可以单独使用，但相互间又互为补充，且三项成份共同为互联网提供分布式和可扩展的信息管理功能。这三个成份是：

a) 识别DE和进行识别符解析的可扩展和分布式识别系统；

b) 获取和管理数字实体的存储库；

c) 联邦搜索和发现注册表。使用这些成份则可通过接口规范和协议而非具体成份的持续维护来管理最终形成的分布式系统。

数字实体是核心元素，所有其它成份和服务均围绕该核心创建和管理。数字实体并不取代现有数据格式和结构，而是提供通用的呈现这些格式和结构的手段，从而使其能够得到统一解释，以方便在异质信息系统中进出，并适应系统随时间推移发生的变化。尽管该模式核心简单，但其详细实施却并非无关紧要，且包括了通过存储库与DE连接的协议。在本建议书中，所有元数据都将符合DE模式，以实现互操作并方便参引。

以下所述的DE数据模式以及获取DE的数字实体接口协议与识别和/或解析系统以及获取DE的注册表/存储库方式结合一起即提供了开放架构的核心。这些成份一道促进实现长期的信息（其结构为可被独特和持续识别的数字实体）管理，从而提供一种获取对象当前状态信息的方法，并提供一种获取或使用实体的服务，以及基于元数据注册表中的信息确定DE识别符的手段。

7.1 数字实体数据模式

在此描述的DE数据模式提供呈现作为DE的元数据记录的统一手段，且可用于呈现作为DE的其它类型信息。这是一个合乎逻辑的模式，方便实现多种形式的编码和存储，并有利于实现互联网上提供的多种类型信息的单一参考点（即，识别符）。每一个DE都含有一套固有的属性、由用户定义的一套属性，这些属性体现在一个或多个元素之中，以及包含诸如文本、视频或图像（以数字形式呈现）信息的零或更多附加元素中。所有这些元素都可通过确切定义的DEIP规范加以提供（见第7.2段），该规范包含使用公共密钥安全性进行的认证功能，同时也包含使用更高级别API认证的其它手段（可能由DE存储库实施）。这就为获取DE提供了私密性和安全性。

DE的固有根本属性是与其关联的独特持续识别符，该识别符可被解析至有关DE的最新状态信息，包括其地点、接入控制和核实（通过向解析系统提出解析请求实现）。DE的其它固有元素属性示例包括：最后修改日期，创建日期和规模。用户可在得到适当许可后确立用户可扩展属性。

DE基本数据模式未具体涉及的属性包括所有权、认证和接入条款及条件。这些属性将是多数DE实施工作的重要组成部分，然而，单一的一种解决方案似乎是不可能的。所有权和接入控制信息很可能包含在用户可扩展DE属性或单独数据元素之中。这就提供了一种处理多种不同所有权和信息管理方案的方法，以及处理多种认证和授权机制的方法，同时无需设想将对各领域和用户社区使用完全统一一致的方式。

标准数据模式、得到定义的与数据模式连接的协议和识别/解析系统合并一起提供了互联网上信息得到长期连贯一致管理的关键手段。解析系统应当是分布式的、安全的和高性能的，旨在方便长时间以及在地点、接入方式、所有权和其它可变属性发生变化时对数字实体进行持续参引。

发现IdM信息的核心功能源自包括存储库的注册构成成份的使用。单个注册表的功能是实现一系列DE的联邦，以方便最终用户和应用对经注册的实体进行搜索和浏览。包含一系列DE的存储库可向一个或多个注册表贡献其所负责的相关DE的元数据。单个注册表可收集来自多个存储库的元数据，单个存储库可向多个注册表发送元数据。注册表可提供被呈现实体的搜索和报告功能，并成为DE结构世界和存储库的进入点。

有些情况下，并非严格需要注册表，如，当以其识别符形式直接参引的DE置于另一个DE或另一条信息或其它文件时。然而，在许多情况下，最终用户或代表最终用户的自动程序不了解应开始的识别符，因此将不得不使用多种搜索或排序（sorting）程序来发现所需参考信息。即便用户了解识别符，他也可能不了解如何对其进行解析，或如何解释解析结果。在注册表中记录DE的存在有助于从总体上解决该问题。

通过确定与具体数据模式互动的操作，可创建数字实体，并用以呈现多种类型的结构信息。下一节将对此进行详细讨论。图1具体说明标准数字实体数据模式。以独立于相关存储系统的实施细节形式呈现实体是一种基本的互操作功能，因为这有利于将多种存储格式和方式标准化至一个单一的逻辑模型上。

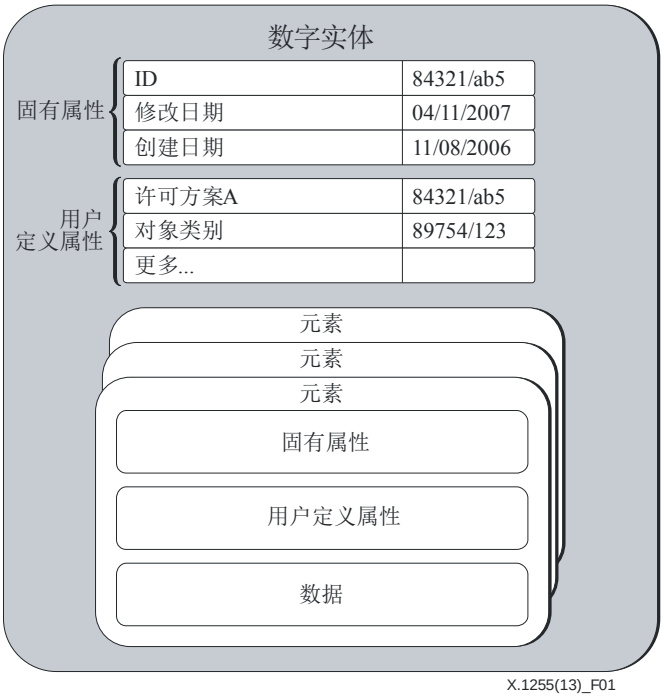


图 1 – 数字实体说明示例

除顶部的持续识别符外，图1中所示的所有数据均仅为概念数据。数字实体的每一个元素都可以有不同形式，即，通过识别符、实际数字实体、类别合适的普通本地数据进行的数字实体参引。

注册表可使用或包含存储库来存储元数据记录，存储库是通过数字实体接口协议提供接入一系列DE的信息管理系统。存储库可被整体上认为包含其提供接入的数字实体，然而，更详细的视图将表明，它们是进入多种不同存储和信息系统的门户，将原始数据映射到在本地或远程存储的数字实体上。这可以简单的是一个保存有特定DE（在一个或多个用户不了解或看不到的文档中）数据的文档系统，或者，对于复杂数字实体而言，数据可能分布在多个位置和系统中，仅在提出需求时才被以DE形式集合，其中一个存储成份持有实体“图”，而多数数据则保存在其它系统中。这种与现有系统互动的技术是实现联邦的关键，因为任意一个复杂的信息系统中的信息都可在逻辑上被分为DE，这些DE可通过采用以用户为中心应用中的DEIP实例，以标准方式加以提供。

DE客户机可通过解析特定DE识别符找到该DE的一个或多个存储库。解析请求发出后会返回客户机可与之启动DE交易的一个或多或相关存储库位置。

通常DE存储库软件提供多个网络接口，以便在数字实体上进行操作，即，与DE本身连接的数字实体接口协议以及由现有技术选择方案确定的本地需要的接口。每一个不同的接口都在安全性、与代理服务器的兼容性和使用无处不在的客户机软件方面具有自身优势。数字实体接口协议含有冗余以及强健的单个和群认证能力。映射系统对冗余予以支持，其中每一个DE存储库都与其它存储库进行通信，确保被复制实体保持同步。认证以秘密或公共/私人密钥或其它认证机制为基础。

其它突出特点包括复制、方便在不同存储库间进行容易的映射以及通过插入机制实现的可扩展性。可建有插入功能，以管理针对具体实体类别的活动（如解析视频格式和分配请求部分），或管理面向网络服务的活动（如为DE注册表贡献元数据）。

7.2 数字实体接口协议

与DE实例的每一项互动都包含在DE上启动或应用一项操作。有关实体的身份管理信息、每一项操作以及操作目标都以独一无二和持续方式得到识别。此外，多种类型资源也是经识别的实体，有关资源的相关状态信息可包括其公共密钥。

操作由存储库应用于数字实体，存储库本身是数字实体且提供其所含实体的接入。数字实体接口协议定义实体与存储库通信、以启动在存储库为之提供接入的数字实体上的操作的方法。这些操作可特别用以通过其识别符获取具体元数据记录，但此类记录也可通过其它手段（如专用注册“应用”和网络浏览器）以句法方式加以获取。

数字实体上的操作涉及下列元素：

- 实体ID：请求启动操作的数字实体识别符；
- 目标实体ID：将在上操作的数字实体识别符；
- 操作ID：对将进行的操作予以规范的识别符；
- 输入：含有操作输入的一系列比特，包括任何参数、内容或其它信息；
- 输出：包括操作输出的一系列比特，包括任何内容或其它信息。

身份管理信息可作为证书（明确或隐含信任信息断言）的一部分加以提供或沟通。然而，如果证书并非由令人接受的信任主管机构创建，则接收方可接受或不接受该证书。可用令牌取代证书来对类似信任结果产生影响。这种证书或令牌能够加大得到传送的身份信息的准确度，然而，作为本开放架构一部分得到实施的固有安全机制可独立进行核实，证明使用身份管理信息的实体拥有用以核实被识别数字实体的适当私人密钥。涉及被识别数字实体的交易请求双方都可要求对方用其私人密钥对字符串进行加密并将其返回提出请求的一方，以进行核实。系统中任何交易的各方都可以启动其它认证手段，但无需事先就此类其它手段进行谈判。以下所述的默认机制使用公共/私人密钥对，这是DEIP实例的功能不可或缺的组成部分。然而，必要时可通过双方的协议使用其它认证机制。DEIP实例的启动须至少包含下列非选择性步骤的实施：

a) 建立A方与B方，即交易双方之间的关联性，除非已存在可用于这一目的的这种关系；

b) 作为选择方案，A方可要求B方向A方证实自己，如通过使用PKI方法；

c) 之后A方酌情向B方发出具体请求；

d) 作为选择方案，B方可请求A方向B方证实自己，如通过使用PKI方法；

e) B方酌情接受或拒绝请求；

f) 交易结束，之后酌情产生新的请求或确立新的关联性。

[b-DOIP]中描述了一种可能的DEIP规范示例，但它不构成本建议书的正式内容（亦见[b-DO Repo]）。

7.3 与注册表的互动

与注册表的每一次互动都涉及被识别的数字实体，这个实体可能是个人或系统资源，而且每一个数字实体均拥有可用于对其进行认证的持续识别符。在设置期间，可对注册表预先进行配置，使其信任通过识别符以某种具体方式被识别的任何客户机。客户机也可使用同一程序来对注册表进行认证。此外，可对具体客户机进行配置，使其按照联邦程序的具体要求操作。除所有受信任客户机共同拥有的操作外，这将方便在注册表上进行具体操作。当客户机与注册表互动时，注册表发出质询响应，以确认客户机拥有匹配的私人密钥。一旦得到核实，则注册表确认所涉识别符属于该数字实体。

注册接口支持下列操作：

- **数字实体注册：**注册信息可仅包含元数据，但也可是元数据加适用元数据的DE。注册表使用其内部存储库管理被注册数字实体。此外，注册表使用预先配置的规则（确定如何解析、如何进行令牌化和如何对所持信息进行索引）对结构为数字实体的信息进行索引。在得到要求时，注册表创建数字实体识别符并使其能被插入到解析系统之中。
- **对此前注册数字实体进行消户（De-register）：**注册表从其内部存储库中删除数字实体，不再对其进行索引，同时更新解析系统，以记录实体的被删除状态。
- **通过其识别符检索此前注册的数字实体：**注册表对在其内部存储库中管理的数字实体进行系列化，并将其前转至客户机。
- **搜索：**注册表解析关键词、确切匹配或一系列查询的搜索表达，以确认是否与被索引的数字实体吻合，之后将吻合的数字实体识别符返回。更为先进的搜索技术，如自然语言查询，也可在研究结果允许时轻而易举地得到合并。
- **获得最新交易号码：**以顺序方式为每一个注册和消户操作分配号码的注册表向客户机（其配置是能够参与与注册表之间进行的联邦程序）返回这一最后号码，这将便于潜在客户机（参与联邦程序的其它注册表）确定注册表状态，以便根据配置的联邦拓扑和选定的汇集程度推送经注册的实体。

虽然可以关闭认证功能，但注册表最好对客户机进行认证，反之亦然。交换信息的编码不尽相同，且是一种详细的实施工作。可将信息编码为数字实体存储库操作，在此点上，注册交易将是一系列存储操作，如，创建实体，增加元素。备选方法是，使用第三方数据编码库对信息进行编码，前提是信息来源方和接收方都（事先）同意使用同一个编码库。

7.4 解析系统

框架的一个组成成份是解析系统（可能存在一个以上），该解析系统可将识别符映射到被识别数字实体的有益状态信息中，如其在互联网中的位置，该实体的认证信息，或与识别符相关的公共密钥。框架的开放架构性质方便了解析系统的互操作，这是本建议书的一个必要目标。可视需要改变状态信息，以便在不变更实体识别符的前提下反映被识别实体的当前状态，从而使识别符在地点和其它相关状态发生改变时依然保持不变。

如果已知一项所需资源的识别符，则解析系统和一套存储库提供经授权最终用户或程序观看或接入数字实体所需的操作。然而，如果不了解所需资源的身份，则需要发现这一身份。用图书馆和信息科学术语讲，前者称作“已知书目”检索（即，你知道自己的需要，只是要了解如何获得所需材料）；后者通常要求进行主题检索，主题检索中所用工具的目标是将其缩减为已知书目检索。数字实体注册表有助于实现这一作用。

尽管注册表实例可独立操作，但这只能满足其了解的发现请求。通过实现多个注册表的联邦，还可以了解其它地方注册的数字实体，因此，可以实现全部数字实体的更广泛检索。确定哪个注册表可能含有与身份相关的信息的能力是发现身份管理信息的一个重要方面。一个系统中提供的信息可能需要由另一个系统（设计可能不同）发现。假设某实体已确定了将这些不同系统及其所含信息予以关联的方法，那么发现框架应方便发现这种关联系统。然而，本建议书不讨论谁或哪个事物负责建立关联关系、应将哪类信息进行关联、或应如何建立关联和获取关联。这些问题总体上依据语境的不同而不同，因此本建议书不提出任何形式的关联做法。为澄清该问题。“关联”这一术语被加入到了定义之中，且该概念也已被纳入身份管理信息的定义中。

许多情况下，私密性至关重要，这通过基于个人、团体、职责和资源识别符的IdM技术的使用以及从存储元数据中获得的条款和条件进行管理。

7.5 联邦注册表中的分布式查询和汇集元数据

本建议书确定的联邦注册系统应能被广泛获取，并形成开放架构发现系统的基础。本建议书规定的系统提供发现身份识别信息的统一方法。联邦注册系统便于IdM提供商参与提供可互操作的注册表，并确定他们愿意与其它注册表分享何种信息。

注册技术提供一种手段，通过该手段，负责在互联网中创建数字实体的各方（包括服务和其它实体）可以注册特定一套此类实体的存在，并在注册时提供有关实体的描述和结构元数据，包括来源信息，从而方便普通大众或特定群体更好地发现实体。必须与数字实体一起注册的一项关键元数据是其持续识别符，且每一个持续识别符都必须在互联网上得到解析。对于尚未识别的实体，可通过对注册表配制，将识别符创建为注册程序的一个组成部分，并提供数字实体管理员需要的工具，以充实和完善解析信息。

联邦注册系统将在发现方面实现四项主要目标。首先将方便在参与信任框架和其它IdM系统之间采用统一的选择政策；第二，将有助于用户获得注册信息并允许用户在无需与多个注册表打交道的前提下进行访问；第三，为私密性和单个IdM系统设定的其它访问限制提供基础设施支持；第四，有助于实现对注册表的句法访问，以支持多语言化。

联邦注册概念基于在此规定的开放框架，具有以下优点：

- 统一选择政策：注册表及其相关信任框架或更广泛的其它IdM系统可根据其声称包含的信息特性得到选择，并进行询问。进行某种程度背景调查以确认相关信息的IdM系统通常会得到选择。另一种替代方法是，最起码信任框架或其它IdM系统（仅检查信用卡信息或驾照）可得到选择。比较极端的情况是，可选择对个人进行DNA检测的IdM系统。充实完善相关政策，以确保系统完整性的组织可能被选定。通过这一手段，可在诸多注册表及其IdM系统之间采用统一的选择方法。
- 共享元数据：在联邦注册系统中提供的信息被称为共享元数据。通用模板与共享元数据相关联，且明确元数据如何得到呈现，从而确定如何对其进行访问，以进行随后处理。模板不包含特定条目。
- 联邦访问：如果一个注册表不包含人们所需的信息，则可通过另一个或更多其它注册表获取信息。的确，在普通操作中，系统的运作是随时向用户提供此类信息，无论其被包含在哪个注册表中。可通过多种不同手段实现这种访问，包括分层联邦和对待系统。
- 专门访问：一些注册表限于特定用户群、应用类别或与使用系统相关的职责使用，而一些注册表则对所有方面开放。根据此类限制标准给出的限制发现信息访问权的手段是系统不可分割的组成部分。由参与注册表认可的一种或多种机制将被用于维护系统内的私密性。
- 句法访问：用一种归类系统解释被插入“类别”。IdP可按照规范导则指定其自身选定的类别，这将便于对相关信息进行句法访问，无论其存储在系统的何处，同时将有助于满足多语言要求。

此类系统中的元数据作为结构数据提供，只要数字实体存在就会有相关的独特持续识别符存在。源自多个不同注册表的元数据可能在主题和/或元数据模式方面不同，因此很难提供简单、但连贯一致的所有记录的搜索方法。如果将源自不同模式或主题领域的元数据减少至最小公分母模式（lowest common denominator schema） – 汇集这类数据的解决方案之一 – 则最佳搜索战略可以是确定成为更详细搜索最佳候选方的注册表。可以由源注册表或收集注册表实现向最小公分母模式的转变。其替代方法是，搜索本身可通过某种方式映射为适当查询多种不同元数据模式，从而得出一套源自最初查询的查询。

尽管来自多个领域的发现信息元数据实体汇集是一种可能性，在多个注册表之间分布查询，并由每一个注册表管理其领域的元数据实体是另一种可能性。各注册表的联邦包括多种其它可能性，如图2的三维空间所示。

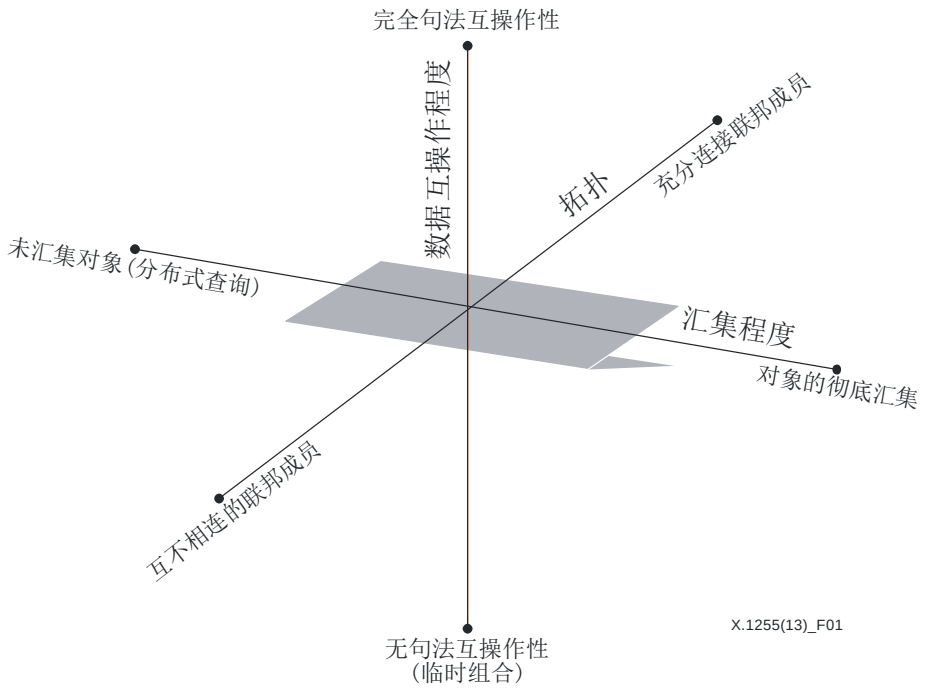


图 2 – 多个注册表之间的分布式查询

图2给出三个轴。一个轴表示注册元数据从无汇集到完全汇集的汇集程度；第二轴表示注册表之间拓扑连接程度；第三轴与来自不同注册表的信息互操作性有关。以下详述各轴。

汇集程度轴表示此前在何种程度上做出安排，将不同注册表中的元数据实体进行汇集。轴上最左侧的点表示查询前未汇集的各注册表的实体，而轴的最右侧点则表示查询前已得到汇集的所有实体。沿该轴的各点表示其它可能性，包括最小公分母元数据信息汇集，搜索指数汇集等。随着我们从左向右移动，汇集信息的现实性也降低，分布式查询能够产生更新的结果，而汇集元数据实体最新与否取决于其上一次得到汇集的时间。

拓扑轴表示注册表的连接程度。在轴的一端，注册表相互之间没有网络连接，因此，不能形成信息共享；而轴的另一端则表明注册表完全相互连接。请注意，注册表“如何”连接目前还由汇集程度决定，拓扑仅仅决定其可能的联系。

数据互操作程度轴表示服务于特定信息域的一个注册表的元数据实体在何种程度上与满足不同信息域的另一个注册表元数据实体之间进行互操作。换言之，一个注册表采用的元数据模式可能与另一个注册表采用的模式实现互操作，也可能无法实现这种互操作。有时，需要对元数据实体进行转变，以实现某种程度的互操作，如果不是充分互操作的话。在其它一些情况下，当模式在句法上相去甚远时，任何数量的转变都不能实现有益的互操作程度。

请注意，并非图2所示的三维空间上的各点都是有效的。例如，在未连接节点上的分布式查询即意味着根本没有查询分布。同样，不可互操作实体的完整汇集意味着这是一种不连贯（incoherent）实体系统。关于图中所示三维空间的有效点，其注册表的基本设计应有助于实现这些配置可能性。同样，映射是在元数据记录变换还是在搜索中进行，以及元数据记录由来源注册表还是由收集注册表变换等都是实施细节。这中间可能存在较为重要的性能方面的后果，但基本设计应便于进行多种不同的灵活实施。

本建议书采用的方式本身不解决异质信息系统之间信息搜索和检索问题，但提供一种公共框架，在该框架中可使用不同方式。的确，对该问题可能没有万全之策，最佳方式会随做法和主题领域的不同而不同。

7.6 元数据模式

本建议书的一个主要目标是提供确定一套“高层”元数据模式的基础，以支持有关下列方面的发现信息：a) 多种不同IdM系统使用的识别符；b) 身份提供商；c) 依赖方；d) 各个层面的信任框架和其它IdM系统，包括政策、程序和下层技术基础设施。这些元数据模式的必要元素将受到特定使用情形的驱动，但必须在元素层和模式层上是可扩展的，以便支持增长和动态领域的变化。

参与身份管理的多种不同实体都可确定其自身的特定模式，并在必要时将其映射到这些高层标准化元数据模式中，以描述其服务、政策和程序，并将这些描述注册在一套联邦注册表中的一个或多个之中。这些注册表将支持各注册实体之间的发现服务。

尽管可以创建一个单一元数据模式来满足IdM技术、相关组织和相关政策与程序的所有方面要求，但我们建议开始时为每一类所涉实体创建一个单一模式。实现相互认可的一套元数据模式的程序是一种协作程序，其间有关各方需要贡献其模式必须加以涵盖的相关属性的知识，之后对照不同使用情形对不同演进的模式进行测试，看其是否真正提供支持发现程序的信息，并酌情对其予以扩充。

7.7 元数据互操作性

识别符是实现元数据互操作性的重要组成成份。然而，有关元数据互操作性的其它特定方面，包括人文定义和描述语境等方面，不属于本建议书的范围。元数据规定的其它属性，如描述或促进特定配置（如具体连接模式和汇集方式）属于注册操作范围。为管理多种不同注册表之间的元数据实体，如果协作各方就共同元数据模式做出决定，则可促进实现元数据的互操作。之后，元数据将作为同质实体得到管理，注册表以统一方式对其进行解释和处理。以下第9节具体说明在汇集和拓扑（通常适用于该框架的两个维面）程度语境内的两个具体联邦案例。

8 类别和类别属性

注册表以旨在与其它联邦注册表进行交换的数字实体形式提供元数据记录。每一个这种记录都由一套元素组成，每一个元素都包含“类别”字段和“数值”字段。理解每一类别的含义对于以非透明比特顺序形式或一套比特顺序以外的方式表示相关数值至关重要。

为理解类别的含义，通过持续识别符表示类别，这些持续识别符可被解析为有关类别的有益信息。尽管类别描述通常由个人创建，但需要一种标准的类别描述和表示手段。

预计随着时间的推移，最终构成类别定义的特定方面和具体属性会发生变化，但以下四个方面是最基本的方面：

- 第一类属性最为简单，包含人们可读的类别目的描述。这种描述旨在说明类别的目的，类别描述的资源和概念及其使用。这些属性将支持多语言描述；
- 类别描述的第二类属性包含其来源信息。每一种类别定义都应包含其创建日期、最新更新日期、其来源、状态和可能的化名（alias）□识别符；
- 第三类属性与描述类别的类型化以及类别充分利用其它类别的能力有关；
- 第四类属性为多种不同系统提供就特定类别资源动态采取行动的能力。

以下详述后三个类别。

类别通常用于描述符合特定一套特点的具体资源类别和/或概念。该类别表示适用的类别域，被称作类别类型（type’s genre）。例如，用以在二进制格式中具体规定如何表述字符的字符编码类别已拥有一个编码类型。用以规定如何将结构表示为一套比特的数据格式类别即拥有格式类型。

每一类别描述都包含具体说明其类型的一个属性。类别类型描述属性提供简单的分类机制，实现新类别发展的正常化，从而帮助类别用户发现现有类别。类别类型本身是一个是需要进行增加的类别和新类别类型，以便扩大类别分类。

为在最大程度上重复使用类别并将重复创建降低到最小程度，每一类别都将能够在现有类别方面对自身做出描述。例如，如果一个新类别需要明确其资源在XML中序列化（serialized），则应当通过包含对现有XML序列化类别进行参引的方式实现这一目标。类别可以通过拓展或实例化来充分利用其它类别。

每一类别都应包含其充分利用和如何利用的任何和所有其它类别。类别能够在其它类别方面定义自身的能力不仅将降低类别的重复，而且有助于类别用户以更加细腻的方式确定其对特定类别的了解程度。

最后，类别描述应有助于多种不同系统动态地就任何类别资源采取行动。类别描述应包含具体说明网络服务绑定和/或具体模块的实施属性、其平台以及其相关接口。这将方便一般性类别处理库动态和安全地与此种服务进行绑定，或获得、加载和运行不同的类别实施模块并处理资源。

如上所述，类别得到独特识别。在一些预确定的解析系统中解析类别识别符将会返回一个类别记录。附录二以示例说明类别记录的BNF表示法，它从概念上确定形成这一类别记录的实体群。

如需毫无歧义和连续一致地定义一个类别，至少需要四个部分，即描述、来源、类型和处理。

描述部分是一个或多个人们可读描述的序列，确定类别的目的和使用，符合[b-IETF RFC 1766]的语言（用以进行描述）须由其类别进行独特表示，并处在描述之前。

来源指数据创建、最后一次修改日期、贡献者（来源）、化名（或替代识别符）以及状态。日期须符合[ISO 8601]标准。贡献者是为在指定类别注册表中为类别创建或注册做出贡献的个人或组织的名称。化名系指此前在其它本地类别注册表中注册的识别符，在此得到声明的目的是建立确立类别的语境。状态则明确类别是否正在得到使用，或被否决，或过时。

类型是类别的本质所在。在现有类别基础上定义新类别是一种强有力的概念，对于确定复杂类别至关重要。有关类型的最后一个概念是具体确定类型信息是否是一个用以确定其它类别的构件（building block），或定义类别特定表示法的构件。例如，二进制编码类别本身是一个构件，方便定义其它类别。

可将信息传至了解如何解析和处理类别信息的服务。客户机启动服务，以便将特定信息进行综合。服务定义应明确如何找到服务、如何启动服务、该服务的预期结果如何。在此不提出有关确定此类服务的表示法建议。

9 分层联邦和对等联邦

在分层方式中，主注册表用于跟踪多个注册表中保存的信息，以方便只进行一个注册表的寻址。可以存在多个主注册表，但为进行完整搜索，必须了解所有这些注册表且对其进行查询。

在对等方式中，特定注册表选择实现与其它注册表的对等，进行特定对等安排的理由多种多样，其中包括相关组织围绕注册表管理采取的政策、禁止或支持注册表之间联邦触点的信任政策以及P2P网络中注册表的可用性/可靠性，这此理由可能决定着注册表选择哪些注册表作为对等对象。

然而，分层和P2P结构仅仅意味着联邦拓扑，并不决定两种情形下的汇集程度。尽管可采用繁复多样的汇集程度，但为具体说明情况，以下给出两个具体示例。表1强调说明两个联邦系统的优势（以加号表示）和劣势（以减号表示），这是使两个元数据实体中的任何一个都事先得到彻底汇集，或针对IdM系统查询，实时将查询传播至所有注册表中。

表 1

	分层联邦	对等联邦
在收集注册表层面彻底汇集元数据实体	+ 通过确定的汇集程序完全实现跨域发现 + 通过汇集期间元数据实体的正常化，保证跨域信息具有意义 + 由于进行本地搜索和检索，因此效率很高 – 结构僵化，需要进行完整的设置程序，可能会干扰组织政策 – 在主收集注册表或中间收集注册表上会出现单点故障 – 由于汇集刷新频率很低，因此可能出现过时信息 – 在最高层可能出现向上扩展问题	+ 有助于实现灵活、不僵化的组合，满足特定方面的需求 + 不会出现单点故障，因为可实现多路由联邦 + 通过汇集期间元数据实体的正常化，保证跨域信息具有意义 + 由于进行本地化搜索和检索，因此效率很高 – 不能保证跨域发现的完整性，除非信息完全互连 – 当注册表可通过多个路由结成联邦时，需要成本极高的去重复工作 – 除非所有触点都得到信任，否则存在安全顾虑
在注册表间发布查询	+ 元数据实体以及实体中的信息保持最新 + 可向上扩展系统 – 无法保证跨域发现的完整性，因为很可能在发布查询时不能提供注册节点 – 由于结果合并的运行时间，可能危害结果排序的实用性 – 结构僵化，需要可能与组织政策产生干扰的完整设置程序 – 在主注册节点或向下传播查询并向上推送结果的中间注册节点上可能出现单点故障 – 由于用于注册部署的硬件不强健，因此存在性能问题	+ 元数据实体以及实体中的信息保持最新 + 可向上扩展系统 – 由于在查询发布时可能无法提供注册节点，因此不能保证跨域发现的完整性，即使部署冗余联邦路由也是如此 – 由于结果合并的运行时间，可能危害结果排序的实用性 – 当注册表可通过多个路由结成联邦时，需要成本极高的去重复工作 – 由于用于注册部署的硬件不强健，因此存在性能问题

注册软件支持并方便实现表1所示各成份之间的组合。一些组合比其它组合带来更大的实施挑战。通过使用存储库技术可以解决向上扩展问题，因为该技术提取实际存储系统，并便于同时使用多个存储系统。注册表的复制和负载平衡也得到实现，从而缓解了向上扩展问题。在多对多的注册表关系中可能存在的重复发现问题，可以通过使用持续识别符大大得到缓解。

与分布式查询不同，数据汇集假设启动元数据记录变动的注册表推送这些记录，而非对收到的请求做出响应。此外，提供记录的注册表被称作来源，接收方被称作目的地。在联邦关系中，目的地是联邦注册系统的触点。来源注册表向目的地前转元数据中成功得到执行的变更，如，元数据记录的创建或编辑。这些交易涵盖数字实体状态变化，即，创建、修改、化名、删除以及增加/去除/替换关系。提交给注册表的每一个注册记录都在注册核心中被转换为注册和消户行动，每一个这类行动都是一项带有交易识别符的交易 – 识别符是通常从零开始逐步增加一个数字。该方法同样适用于这样的情形，即，注册表可按对等方式进行安排，以及按分层方式进行安排。

将单个注册表针对具体查询进行配置并向选定注册表传播查询（无论其形式是分层的还是P2P的），有助于实现查询传播。数字实体注册表除支持具体针对社区的接口外，还支持作为默认接口的数字实体接口协议。根据该协议的使用情况，可向其它注册表传播查询。

附录一

使用情形

（本附录不构成本建议书的组成部分。）

若干使用情形将有助于说明如何使用联邦注册系统。以下具体说明一些情形，同时给出需要得到注册、以使发现程序正常工作的可能属性。

- 客户（机）（人或机器）希望在互联网上获得服务提供商的一项服务。服务提供商要求证明身份，并接受来自任何一家身份提供商提供的身份证书。客户机（通常为软件）必须能够确定可接受哪家IdP（身份提供商），客户机是否已拥有由一家或多家被接受IdP提供的相关证书，如果尚不拥有，将如何获得这一证书。

  服务提供商必须说明对相关服务而言哪家IdP是可以接受的，这可以由服务提供商以标准方式直接进行，也可依赖注册表（以标准方式进行）。在这二者的任何一种情况下，IdP都必须得到独特和准确识别。之后，客户机可对IdP组织的现有参与情况进行对比，或了解如何满足IdP要求，并将相关证书提交服务提供商。在由服务提供商直接告知的情况下（对相关IdP进行独特和准确识别，且客户机有能力提供针对具体IdP的证书），不需依赖注册表。然而在所有其它情况下，必须能够发现某种程度的有关被接受IdP的信息。在拥有独特和持续识别符的前提下，可以直接查找有关IdP详细情况的注册表。为满足该使用情况要求，描述特定IdP的元数据需要向客户机提供确定选择特定IdP来使用特定服务是否合理的信息。相关属性包括IdP本身的独特持续识别符（用于潜在的交叉参引，如审查站址）、IdP参与的信任框架、政策和程序、法律要求、所需软件、收费表等。其中一些信息是第二级别间接寻址形式的信息，如，特定IdP的许多技术和政策细节是由IdP参与一个或多个确定信任框架而得到确定的。

- 有助于客户机明确特定IdP是否适当的相同细节也有助于服务提供商发现一个或多个其证书可被接受的IdP，因此，可被加入到他们的可接受IdP清单中。IdP元数据涵盖这两种使用情形。

- 第一种情形的相反情况是，客户机接入一项服务，并提交该服务此前从未遇到过的身份证书。假设提交的这一证书至少在开始时包含IdP识别符，则服务必须决定是否接受这一证书，还是不做任何进一步调查即予以拒绝。在这种情况中，注册表必须发现有关识别符类别及其代表的IdP的一般信息。这反过来会导致在注册表中进一步查找IdP所使用的具体技术，包括相关信任框架。

- 参与身份管理的多种不同实体通常都是一个或多个信任框架或其它IdM系统的成员（无论是明确还是隐含成员）。将需要确定每一个IdM属性的规范，以创建描述该信任框架的元数据模式。在此会出现若干重要问题：描述IdM系统的组织（为之提供一套实施标准）是否提供一种衡量符合标准与否的方法等？无论对这些问题的答案如，，显然，一些IdM，甚至一些RP将被有益地连接至更高层描述，如，InCommon、Kantara、Safe-BioPharma和OIX组织，这些在注册表或注册联邦中可被发现。

在图I.1中，我们具体说明与具体使用情形一道得到使用的联邦注册系统（“系统”）的使用方法。

步骤1：在该示例中，最终用户要求使用依赖方服务。

步骤2：依赖方以RP信任的一个或多个信任框架身份做出答复，在此情况下为一个框架（TF1）。

步骤3：最终用户利用TF1识别符到系统中去。

步骤4：系统以TF1的相关记录做出答复。有关TF1的信息包括在框架中得到信任的最低限度属性。

步骤5：最终用户对这些最低要求做出评估，以确定是否能够获得RP的信任。在此我们假设最终用户通过评估做出正面回应，并表明最终用户可满足最低属性，如，驾照。

步骤6：此时最终用户可回到系统中，请求使用属于TF1且满足最终用户支持的协议（如HTTP和电子邮件）要求的IdP，在此我们仅简单地将其表示为X协议。

步骤7：系统找出TF1与X协议相匹配的身份提供商（IdP）。

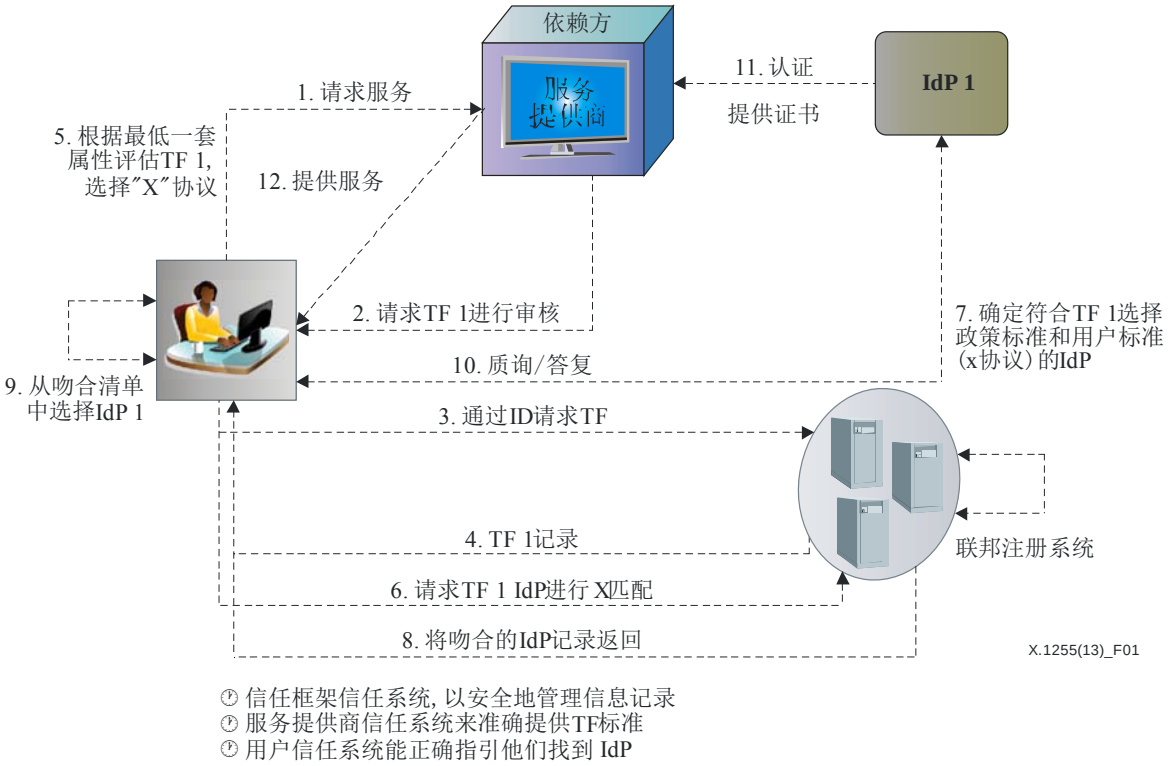
步骤8：系统以一系列符合依赖方和最终用户要求的IdP向最终用户做出答复。

步骤9：最终用户对由系统返回的这一系列IdP做出评估，并做出选择（IdP1）。

步骤10：拥有IdP所需属性且使用IdP1理解的协议的最终用户参与与IdP1进行的质询/答复互动。

步骤11：成功的质询/答复互动会使IdP1提供对RP证书的认证。

步骤12：信任最终用户的依赖方现在可以提供所请求的服务。

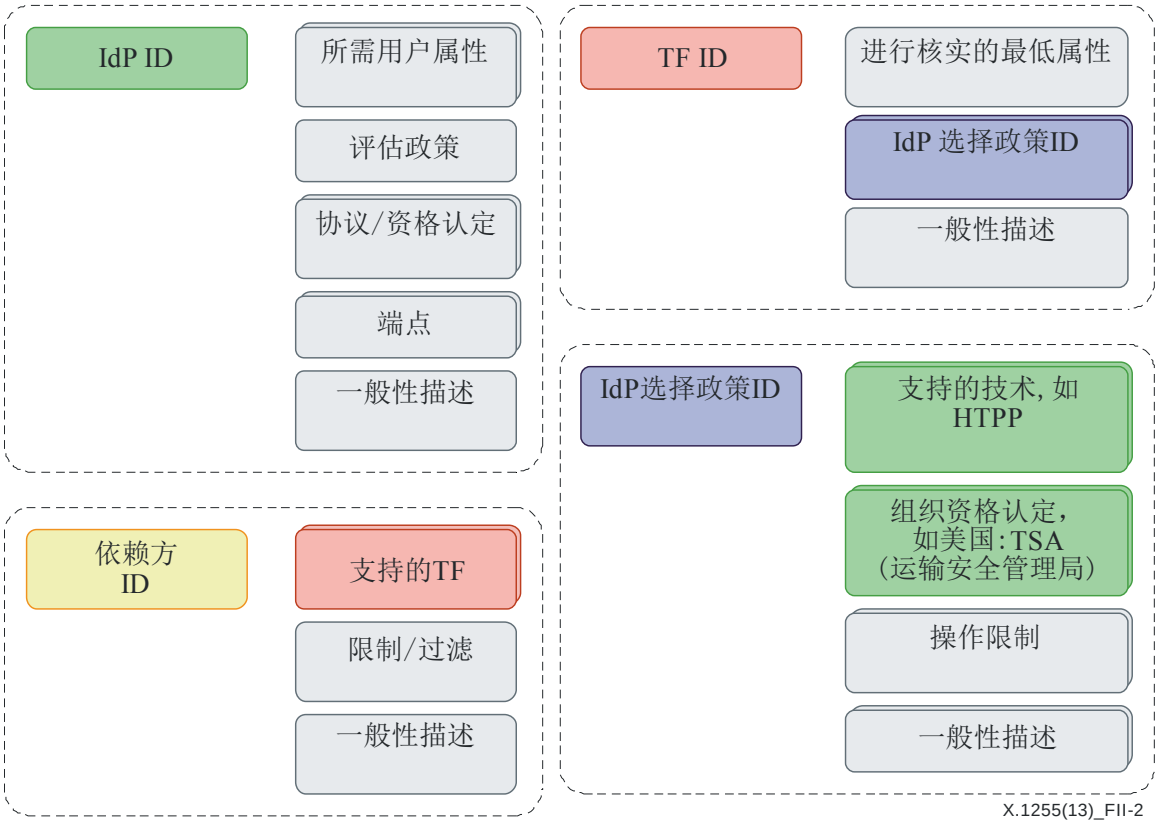


图I.1 – 涉及信任框架的认证

在图I.2中，我们表明了联邦注册系统保存的高层记录模式，这有助于实现图I.1描述的交易以及以上所述的其它使用情形。这些记录由系统作为数字实体保持，每一个实体都拥有一个持续识别符。每一个实体还必须进一步发展为具体模式，以便形成样板（prototyping）。

每一个信任框架都有一个识别符、对框架的总体描述、进行认证的一套属性和指向一个或多个IdP选择政策的指针，这些在系统中与数字实体分别保存。这些相当于补充的间接寻址，其方法是一个单一TF中的所有IdP都可通过标准而非枚举（enumeration）被组合。每一个IdP选择政策实体都有一个识别符、总体描述、可接受技术清单（如支持的协议）、组织资格审定机构清单（如政府组织）、任何特别的操作限制。在两个方向中，TF和IdP选择政策之间的关系是多对多关系，即给定TF可容纳多项IdP选择政策，且给定IdP政策可由多个TF加以使用。

其余提议由系统保存的两个实体类别为IdP和依赖方。每一个IdP都拥有一个持续识别符、一般性描述、所需的用户属性、评估这些属性的政策、具体协议和被接受的资格认定，以及具体端点，如，以可接受协议形式出现的IdP位置。每一个依赖方都有一个持续识别符、一般性描述、其依赖的一套TF以及任何具体的操作限制。


IdP ID
所需用户属性
评估政策
协议/资格认定
端点
一般性描述
TF ID
进行核实的最低属性
IdP 选择政策ID
一般性描述
依赖方
ID
支持的TF
限制/过滤
一般性描述
IdP选择政策ID
支持的技术, 如
HTPP
组织资格认定，
如美国:TSA
(运输安全管理局)
操作限制
一般性描述
X.1255(13)_FII-2

图I.2 – 高层模式

附录二

类别记录的BNF表示法

（本附录不构成本建议书的组成部分）

类别记录的BNF：

```
<type identifier> := <unicode string>
<type> := <description section> <section delimiter>
    <provenance section> <section delimiter>
    <genre section> <section delimiter>
    <processing section>
```

```
<description section> := <language> '=' <human readable description>
[<repetition delimiter> <description section>]
<language> := Any item from RFC 1766
<human readable description> := <unicode string>
```

```
<provenance section> := <creation date> <list delimiter>
<last modified date> <list delimiter>
<contributors> <list delimiter>
<aliases> <list delimiter>
<status>
<creation date> := Conforms to ISO 8601
<last modified date> := Conforms to ISO 8601
<contributors> := <unicode string>
[<repetition delimiter> <contributors>]
<aliases> := <unicode string>
[<repetition delimiter> <aliases>]
<status> := 'in use' | 'deprecated' | 'obsolete'
```

```
<genre section> := <genre> '=' <genre details>
 [<repetition delimiter> <genre section>]
<genre> := 'data structure' | 'encoding' | 'format'
<genre details> := <human readable description>
 [<list delimiter> <genre subsection>]
<genre subsection> := 'form='<form> <list delimiter>
     'relationship=' <relationship> <list delimiter>
     'related to=' <type identifier>
     [<repetition delimiter> <genre subsection>]
<form> := 'expression' | 'manifestation'
<relationship> := 'is equivalent to' | 'is derived from' |
'is informed from'
```

```
<processing section> := <processor type> '=' <processor>
[<repetition delimiter> <processing section>]
<processor type> := 'network service' | 'downloadable program' | 'parsing
function'
<processor> := <network service type> '=' <network service binding> |
   <compatible platform> <list delimiter>
   <program network location> <list delimiter>
   <program arguments> |
   <pseudo code>
<compatible platform> := 'Linux' | 'Windows' | 'Mac OS'
<program arguments> := <type>
     {<list delimiter> <unicode string>}
<pseudo code> := <unicode string>
```

```
<unicode string> := <visible character> [<unicode string>] |
  <whitespace character> <[unicode string>]
<visible character> = Any visible character in Unicode presumably encoded in
UTF-8
<whitespace character> := Any whitespace character in Unicode presumably encoded
in UTF-8
```

说明：

1 向全局解析系统发出的<type identifier>解析至一个<type>记录。

2 所有定界符（delimiter），即，<section delimiter>、<repetition delimiter>和<list delimiter>，都是具体针对实施的细节，有意未在此加以确定。

3 <network service type>未在此确定，但应由实施机构在认为合适时包含常用网络服务。

4 <network service binding>也未在此定义，但应以网络服务类别为基础。应在此表明符合每一服务类别的实际定义。

5 <program network location>也未在此定义，但应确定客户机使用其从网络上下载程序的网络协议。

6 <compatible platform>可得到扩展或以比此处更详细的方式得到明确。

参考文献

[b-ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

[b-IETF RFC 1766] IETF RFC 1766 (1995), *Tags for the Identification of Languages*. <http://www.ietf.org/rfc/rfc1766.txt>

[b-DO Repo] Reilly, S. and Tupelo-Schneck, R. (2010), *Digital Object Repository Server: A Component of the Digital Object Architecture*, D-Lib Magazine, Vol. 16, No. 1/2. <http://dx.doi.org/10.1045/january2010-reilly>

[b-DOIP] Reilly, S. (2009), *Digital Object Protocol Specification*, *Version 1.0*, Corporation for National Research Initiatives. <http://hdl.handle.net/4263537/5045>

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2013年，日内瓦