

国际电信联盟

ITU-T

国际电信联盟
电信标准化部门

X.1250

(09/2009)

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

**增强的全球身份管理和
互操作性的基本能力**

ITU-T X.1250建议书

ITU-T



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

欲了解更详细信息，请查阅 ITU-T 建议书目录。

增强的全球身份管理和 互操作性的基本能力

摘要

ITU-T X.1250建议书描述了全球身份管理（IdM）和互操作性的基本能力（即增强在电信/信息技术IT网络和服务中实体使用的各种身份的交换与信任）。身份管理信任的定义和必要性很大程度上与语境相关且常取决于不同国家的不同政策和实践。信任能力包括对个人可识别信息（PII）的保护和控制。

来源

ITU-T第17研究组（2009-2012年）于2009年9月25日，按照世界电信标准化全会（WTSA）第1号决议规定的程序，批准了ITU-T X.1250建议书。

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）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 2010

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 参考文献	1
3 定义	1
3.1 其它建议书中定义的术语	1
3.2 本建议中定义的术语	2
4 缩写	3
5 惯例	4
6 概述	4
7 全球身份管理和互操作性能力	5
7.1 可能的身份管理处理模型示例	5
7.2 可互操作身份管理 (IdM) 能力集	8
7.3 身份的四个基本组成部分	9
7.4 身份能力的发现	11
7.5 互操作性和桥接	12
7.6 IdM安全	13
7.8 审计与合规性	15
7.9 性能、可靠性和可提供性	16
7.10 国际化	16
参考资料	17

增强的全球身份管理和互操作性的基本能力

1 范围

本建议书描述了利用公众电信网络和服务增强全球身份管理（IdM）和互操作性的基本能力。这些基本能力是按照功能区域划分的：

- 通用的结构化身份管理模型
- 属性（包括标识符）、证书和能力的提供
- 身份提供方资源、能力和同盟的发现
- 包括身份服务桥提供方在内的管理平台、身份服务提供方和提供方同盟之间的互操作性
- 减轻身份威胁和风险的安全措施和其他措施，包括保护身份资源、个人可识别信息和隐私的措施
- 审计与合规性，包括个人可识别信息的政策实施和保护
- 身份管理能力的性能、可靠性和可提供性

当今的电信/IT网络和服务五花八门，分布极广，互联充分，但在身份管理（IdM）方面仍保持了显著的自主性。随着这些网络和能力不断演变，其规模和复杂性可能抑制IdM能力之间的互操作性。由于这个原因，本建议书中的IdM能力显著依赖于现有的网络能力和总体模型 – 包括那些有效的最佳做法。但是，为了实现全球身份管理和互操作性，本建议书描述了一种演变路径并尽可能描述了如何根据现有能力来构建该路径。此外，本建议书规定了一种身份桥能力，可用于许多IdM系统并支持综合了现有IdM能力的架构。

IdM能力在各国的实施须遵守各国管辖权特有的要求。

注 – 本建议书所用的涉及IdM的“身份”一词并非指其纯粹含义。特别是它不构成对个人的任何肯定验证。

2 参考文献

无。

3 定义

3.1 其它建议书中定义的术语

本建议书使用了下述在其它建议书中定义的术语：

3.1.1 声明人 [b-ITU-T Y.2720]和 [b-ITU-T X.811]： 作为认证主体的实体或实体代表。声明方包括代表主体参与认证交流的必要功能。

¹ 根据各国的法律，本建议书可能不适用于某些国家。

3.1.2 个人可识别信息 (PII) [b-ITU-T Y.2720]: 与活着的个人相关、可能用于识别该个体的信息（包括这样的信息，即使它不能单独明确地识别某个人，但与其他信息结合便可识别的情况）。

3.1.3 依赖方 [b-ITU-T Y.2720]: 在某些请求语境下，依赖于请求/断言实体提供身份特征或声称的实体。

3.2 本建议中定义的术语

本建议书规定下列术语：

3.2.1 代理: 代替另一实体行事的某一实体。

3.2.2 匿名: 一实体无法在一组实体中被识别的属性。

注 – 匿名防止对实体或其行为（如用户位置、使用服务的频率等）的跟踪。

3.2.3 属性: 针对一实体并说明该实体特性的信息。

3.2.4 认证: 参见实体认证。

3.2.5 认证保证: 认证过程中实现的信任，沟通伙伴为其所声称或预期中的实体。

3.2.6 捆绑: 一种明确建立的关联、结合或联结。

3.2.7 声称: 一个数字对象的一个或多个身份属性值的声称者做出的断言，通常该断言是有争议或存在疑问的。

3.2.8 实体: 单独和独立存在的任何事物，可在语境内识别。

注 – 实体可以为真人、动物、法人、组织、主动或被动之物、设备、软件应用、服务等或上述个体的组合。在电信中，实体的例子包括接入点、订户、用户、网元、网络、软件应用、服务和设备、接口等。

3.2.9 实体认证: 对实体和所介绍身份之间关联性实现充足信任的过程。

3.2.10 同盟: 用户、服务提供方和身份服务提供方的关联。

3.2.11 标识符: 用来在语境中识别实体的一个或多个属性。

3.2.12 身份: 以一个或多个信息元素表示一实体，使实体足以在语境内得到区分。在IdM中，术语身份被理解为语境下的身份（属性子集）即，属性的多样性受限于实体存在和互动的边界条件（语境）框架。

注 – 各实体通过一个综合身份表示，它包括所有描述这类实体（属性）的可能信息元素。然而，这种综合身份是一个理论问题，不包括任何描述和实用情况，因为可能的属性数量是无限的。

3.2.13 身份服务桥提供方: 作为其他身份服务提供方中可信赖的中介身份服务提供方。

3.2.14 身份管理：用于以下目的的一套功能和能力（如，管理、管理和维护、发现、通信交流、关联和绑定、政策执行、认证和声明）：

- 保证身份信息（如标识符、证书、属性）；
- 保证实体（如用户/订户、组、用户设备、机构、网络和业务提供商、网元和物件、虚拟物）身份；以及
- 支持业务和安全应用。

3.2.15 身份服务提供方：认证、维护、管理并可能创建和分配其他实体身份信息的实体。

3.2.16 身份模式：对实体属性的结构表示（如实体行为），可用于一些识别过程。

3.2.17 证明：所观察到或发现的（即非自我声称的）一实体的表述（与声称情况比较）。

3.2.18 假名：某一实体为自己虚构的身份，在某些语境中，实体可通过该方式使用该虚构的身份，甚至有可能完全匿名。

3.2.19 请求实体：在某种请求语境中向依赖方提出某种身份表示或主张的实体。

3.2.20 终端物体：与网络终端设备（如移动电话）可能有某种关系的物体（如SIM卡）

3.2.21 信任：在一定语境内，对信息可靠性和真实度或对实体适当行事能力的高度信任。

3.2.22 用户：使用如系统、设备、终端、流程、应用或公司网络等资源的实体。

3.2.23 以用户为中心：可向（IdM）用户提供加强实体之间各种有关身份信息交流的隐私和安全政策能力的IdM系统，如PII。

4 缩写

本建议书采用下列缩写：

DHCP	动态主机控制协议
ID	标识符
IdM	身份管理
IdSP	身份提供方
IT	信息技术
NGN	下一代网络
PII	个人可识别信息
RFID	射频标识
SIM	用户识别模块
URL	统一资源定位符

5 惯例

无。

6 概述

通信能力的增长和演变促进了各式各样的消费电子服务、商业电子服务和政府电子服务。通信已不再仅仅是浏览信息的资源，NGN之类的基于网际协议的通信技术正在成为开展日常电子事务处理的不可或缺的促发因素。

本建议书中所述的能力目的是在遵守区域或国家关于个人可识别信息和隐私政策的前提下，支持在所有电信/IT网络和服务系统共用的框架内结构化和可互操作身份能力的发展和部署。

本建议书中所述的能力包括：

a) 通用的结构化身份管理模型

身份管理通常涉及利用电信/IT网络业务在实体间交换一种或多种身份。为了确保合乎需要的认证保证级别，双方可能决定或被要求互通或向第三方提供额外信息。最初的通信交流中可能包含优先认证流程的表达或一项委托。交流的一方或双方还可能选择保持匿名或使用假名。这几种相互作用可由通用模型来表示 – 本建议书对这些模型的能力做了进一步阐述。这些模型在需要时允许多方提供身份能力，对实施所述并得到各网络（如NGN）支持可操作的IdM能力也非常重要。

b) 按已知的保证级别提供和保护证书、标识符、属性和模式身份能力。

c) 发现身份服务提供方资源、能力和同盟。一个重要的IdM挑战是在不断变化、复杂多样的网络能力与应用世界中发现目前的身份源及其提供的服务。发现能力对达成所需的保证级别往往是必不可少的。

d) 身份平台、提供方和身份同盟，包括身份服务桥接提供方之间的互操作性。在一个分布极广、游牧用户和提供方众多的公众网和能力基础设施中，身份管理或许涉及在其中运作的各方和同盟之间的大量查询和响应。提供身份管理能力的各方之间的全球互操作性是必不可少的，包括实施身份能力查询的公共协议。

e) 减轻身份威胁和风险的安全措施和其他措施，包括保护和控制身份资源和个人可识别信息。由于身份信息和网络资源是网络，特别是被视为关键的国家基础设施一部分的网络的宝贵、敏感和关键组成部分，并影响到个人隐私，身份信息和资源需要根据IdM环境的分析得到安全保护。

f) **审计与合规性，包括个人可识别信息的政策实施和保护。**身份管理提供通常受到各种各样法律、规则、政府和业界要求的制约，需具备一定程度的审计与合规能力。这些能力范围广泛，包括：合规性审计、保护个人可识别信息的措施、给消费者的通知和维护适当的时戳准确度和可跟踪性。

g) **可用性与可调整性：性能、可靠性、可提供性、国际化和灾害恢复。**

为了适应身份系统持续不断、极为分散的演变，身份管理能力必须是可用的和可调整的。鉴于身份信息和资源是实体相互认证，即将对方接受为通信伙伴的基础，常常成为关键基础设施的组成部分，因此需要遵守一定程度的性能、可靠性、可用性和能力。

7 全球身份管理和互操作性能力

本条给出了可用的身份管理处理模式范例；制定了一系列可互操作的身份管理（IdM）和基本身份组件。本条还讨论了发现身份能力、互操作性与桥接、IdM安全性、个人可识别信息（PII）的保护、控制与使用、审计和合规性。另外，此项工作亦考虑了国际化、性能、可靠性与可用性的因素。

7.1 可能的身份管理处理模型示例

身份管理的一种主要事务处理是多数结构化信息交换中常见的基本查询-响应过程，见图1。消息交换的最基本形式涉及采用商定的协议和信息模型的两个参与方。

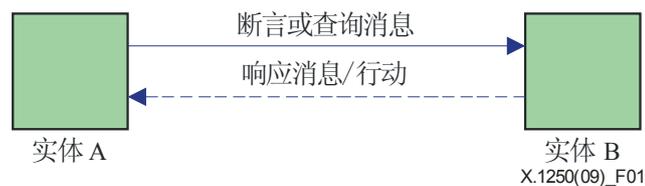


图1 – 基本的查询/响应信息交换过程

参与该过程的各方可以是任何种类的实体。此类实体可以为真人、动物、法人、组织、主动或被动之物、设备、软件应用、服务等或上述个体的组合。在电信中，实体的例子包括接入点、订户、用户、网元、网络、软件应用、服务和设备、接口等。参与方可以是任何物理的或虚拟的物体，如网络设备、软件、终端设备、传感器、加了有源标签的实物（例如采用RFID或光学代码）、加了无源标签的物体。例如，网络设备可以当做具有特定IdM能力的代表最终用户、提供商和政府机构的实体。在数字权利管理语境中，实体可以是知识产权或受版权保护的资料，如多媒体或IPTV内容。一种特殊类型的实体是组。组的身份是该组中所有参与方身份的交集（共同属性）。

身份管理用例大多涉及复杂的模型。例如，对于最先收到身份声称的依赖方不是身份服务提供方的情况，如图2a或2b所示，身份服务提供方的作用从依赖方中分离出来，不同于依赖方。依赖方评估来自身份服务提供方的响应，并决定其是否具备足够的实体认证保证级别。身份服务提供方的主要作用是管理身份信息的生成、更新、验证、中止和删除。

有多种可能的身份信息交换模型。常用的一种模型是三方查询响应模型，如下文图2a所示。一些新开放IdM协议的预测，便是基于这种模型。

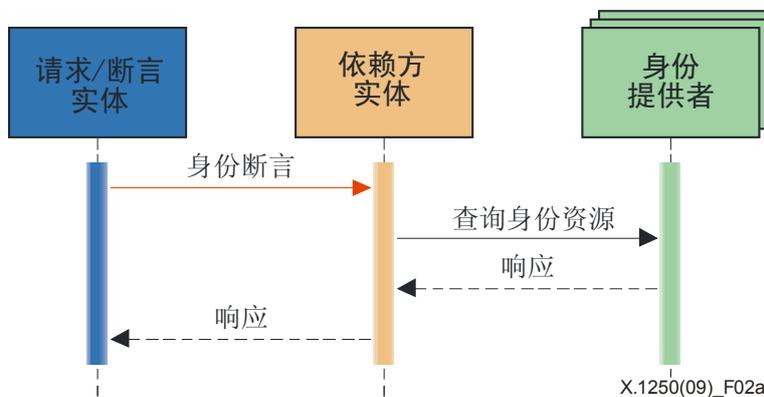


图2a – 三方身份管理模型示例

图2b描绘了另一种身份管理模型，其中请求拥有对身份关系更大的控制权。

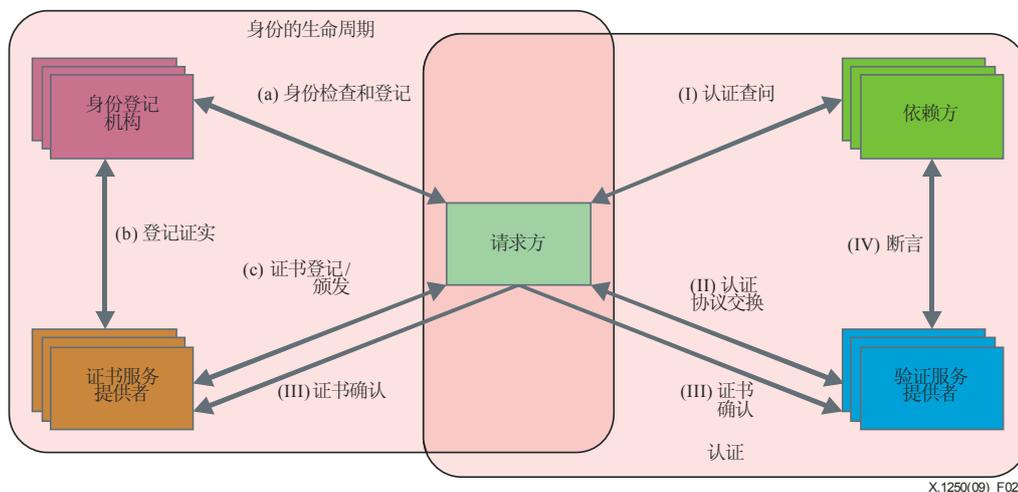


图2b – 以用户4E3A中心的五方身份管理模型示例

“以用户为中心”的模型（要求请求方能够全面控制其身份的使用）得到了广泛关注，可能在国家或区域管辖权中也可以是强制性的。在图2b的示例中，由不同的服务提供方为身份管理提供专门的角色和功能。所有查询/响应都是通过请求方进行的。在这几类模型中，实体指的是：

- **身份提供方**：维护和管理并有可能创建其它实体（如，最终用户、组织和设备）可信赖身份信息的实体，并提供基于身份的服务。此实体负责指配或发布属性（即在某种特定语境下涉及身份（例如对订户而言的证书提供方） – 也称为注册 – 负责包括身份的检查、登记和维护在内的身份生命周期管理，包括撤销。
- **证书服务提供方**：提供与证书和令牌（例如将令牌与可验证的标识符和属性捆绑的证书）发布有关能力的实体。
- **验证服务提供方**：提供评估身份信息（例如声称和证书）和有效性分类能力的实体。
- **依赖方** [b-ITU-T Y.2720]：在某些请求语境下，依赖于请求/断言实体提供身份特征或声称的实体。

总体而言，查询-响应活动可分为两大类：

a) 身份生命周期

- **身份登记和检查（即注册）**：该信息流表示某实体进入某特定的语境，即在此语境下，涉及此类实体身份属性指配的相关登记和检查过程。例如，它可能涉及表明某自然人与某订户名或假名相关的证据验证和记录。
- **登记证实**：该信息流表示身份服务提供方与证书服务提供方之间的互动，用于证实已登记的身份。
- **证书登记/颁发**：该信息流表示证书服务提供方与请求方之间的信息交换，用于身份登记和获得将令牌与姓名或假名及其他与身份有关的属性捆绑的证书。

b) 认证和断言

- **断言**：该信息流表示信息交换依赖方与验证服务提供方之间为传送断言信息而进行的信息交换，用于对声称实施分类。
- **认证查问**：该信息流表示依赖方为了认证而对请求方进行的查问或提示。例如，依赖方可以将请求方提出实体改换到一个特定验证服务提供方，而请求方也可以选择了一个特定的验证服务提供方。
- **认证协议交换**：该信息流表示为了让验证服务提供方认证请求方而进行的协议消息交换。
- **证书验证**：该信息流表示验证服务提供方与证书服务提供方之间为在必要时验证证书进行的信息交换。

在本建议书中，这些模型并未穷举。它们的目的是提供灵活性，有可能包括存在许多身份服务提供方的语境以及请求或依赖方亦为身份提供方的语境。

c) 其它断言

- **委托**：断言可能还含有优先验证的表示或“委托”。优先验证表示用于通知依赖方向哪个身份提供方查询，条件是依赖方能建立起优先身份服务提供方的信任链。委托在一个实体代表另一个实体行事的情况下提供了一种适应手段。这种委托是常见的，例如，家长可代孩子行事，某成年人可代另一个丧失能力的成年人行事，雇员可代表公司行事，或代理人可代表客户行事，或国家可代表公民行事，反之亦然。
- 委托可用于将身份相关的实体得到的某些能力或获准的权利提供给受托实体。此时，依赖方对身份服务提供方的查询有可能包括附加的请求，以验证委托方已将受托方登记为授权代理。这种请求属于对代理的认证之外。共用的或受托的身份关系在这些模型中可能存在于许多实体之间。委托链的范围（例如委托的委托）受限于可用的技术以及、法律、法规或商业、同盟和法律政策。
- **匿名和假名**：一个实体也可能使用匿名身份或假名身份。此时，由于可能无法达到实体保证的水平，身份保证的程度取决于依赖方需要考虑的外部因素。涉及的活动种类不需要实际验证（例如该活动无足轻重，不需要任何种类的身份管理开支）时，可能使用匿名和假名。此外，一些法律、法规或数据保护政策可能要求使用假名或匿名。

7.2 可互操作身份管理 (IdM) 能力集

身份管理是作为基本网络模型所有层（如NGN中各层）的一种通用能力出现的[b-Y.2012]、[b-Y.2720]。IdM能力作为基础运输功能的一部分用于应用部分的网络服务控制以及用于控制这些层的管理能力。

这些层之间在身份管理方面通常欠缺协调。在区域或国家政策允许的范围内，互操作IdM能力应得到各网络层的支持。

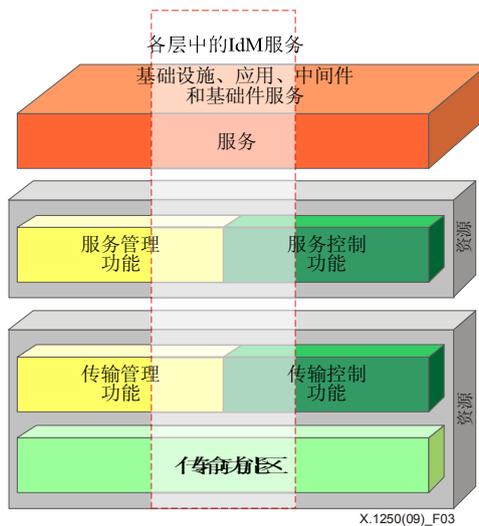


图3 – 身份管理网络各层互操作性范围

图3表明，IdM相关能力可能存在于网络架构的所有垂直层中，需要同步和协调。

7.3 身份四个基本组成部分

为加强互操作的IdM能力，本建议书将身份信息细分为下列四种基本类型：

- 标识能力，
- 证书能力，
- 属性能力，
- 模式能力。

集合四类身份信息中的每一类可用于支持更高级别的身份保证，可由不同实体作为身份能力单独或以某种组合提供，如图4所示。此图可视为图2的扩展。在某种IdM实施中不一定要用到所有这些身份能力。这些能力的使用 – 及这些能力的存在 – 取决于IdM语境，特别是合乎需要的或必需的实体认证保证级别。

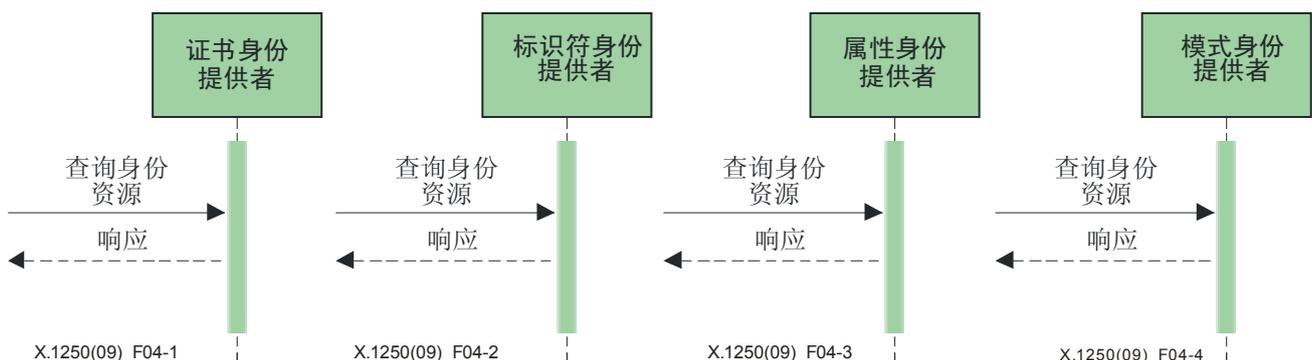


图4 – 四类基本身份查询-响应能力示例

这些身份能力的区分从功能上讲可能不那么明确。例如，证书都有各自的标识符，提供方维护证书所属的相关身份的某种属性信息，提供方可能还维护含有证书使用情况的日志文件，用于模式分析以尽量减少身份盗窃和欺诈。

IdM提供方在电信/IT之类的许多实施中有可能提供成为一种组合的所有这些能力，金融服务提供方或者与最终用户或客户有特殊关系的机构或组织也有可能提供成为一种组合的所有这些能力。“IdM的开放性”和IdM提供方的互操作性是由信任和类似需求、业务关系以及监管和法律要求决定的。

7.3.1 标识能力

标识符是通常指配给一个实体的属性（名称），用于信息系统管理或通信寻址。因此，它们通常有专门用途。如电话号码、URL和电子邮件地址既可用于服务/设备访问，也可用于通信网的路由。

7.3.2 证书能力

证书用于为实体认证提供支持 – 一方或多方的认证，以进行信息交换或处理。一种出现最早且至今仍是使用最广的证书形式以ITU-T X.509数字证书标准[b-ITU-T X.509]为基础。其他证书形式包括政府签发的证书，如与就业相关的徽章、移动无线SIM卡以及金融机构信用卡或自动取款机（ATM）卡。

有时，证书还包括生物统计表达方式。有些应用需要快速快速验证的能力，验证证书的有效性且该证书未被撤消。但是，必须考虑到证书检查可能会产生大量IdSP追溯信息，可能会产生隐私方面的风险。因此，无需检查的强力证书十分重要。

通过采用以用户为中心的IdM方法以及证书管理能力（如数字钱包），可降低公共广泛使用和管理数字证书的复杂性[b - ITU-T X.1251]。视情况，证书支持可能包括能够使用不同证书来满足所需的不同实体认证保证级别。

7.3.3 属性能力

作为实体的特性，属性往往是相对静态的 – 作为证书或标识符指配过程的一部分捕获（例如名称、物理地址、联系人信息等）。在其它情况下，如当时的地理空间位置，属性可以是高度动态的。

属性发现和查询能力可能需要专门的可互操作协议。这种协议一般应支持某种形式的验证 – 特别在涉及到PII的情况下，以保护和控制个人可识别信息。以用户为中心的可互操作协议和平台也可为供最终用户提供一种方法，用以指定处理理属性信息的方式。

7.3.4 模式能力

身份模式是实体属性的结构化表达，可用于某些识别进程。

此类模式可能包含观察到的或被发现的（即未声称或断言）实体，例如：模式身份由与某实体有关的名誉信息或事务处理信息组成，对检测身份盗用往往非常重要。专门化模式身份能力也用于支持网络安全能力，如病毒或基础设施攻击中的模式签字。

与属性身份能力类似，若涉及自然人，则规定中还有可能援用同盟能力与可能的法律及监管要求的组合，这种组合是显著扩充的，有时还有冲突 — 特别是对于保护个人可识别信息而言。在某些管辖权内，在涉及到PII而又没有什么目的的情况下，模式数据保留和分析能力要执行大量数据保护和保密政策，包括禁止数据采集和删除数据的机制。

7.3.5 一般性IdM数据管理能力

若干IdM能力适用于IdM系统管理和所有身份能力IdM数据的管理。这些能力包括为下面各项提供支持：

- 请求方访问/删除/改动/监测/控制其自身身份信息的能力，但须遵守法律、法规和/或适用的政策；
- 授权实体（例如系统管理员、家长、公共安全、法律实施和其他授权第三方）访问/改动/监测/控制其身份信息的能力，但须遵守法律、法规和/或适用的政策；
- 输入、输出身份信息，但须遵守法律、法规和/或适用的政策；
- 指出某些信息，表明向依赖方提供的信息质量水平的机制。这要求各方就信息的价值达成协议；
- 请求方将其身份信息管理委托给另一实体。
- 对所有身份的生命周期管理，包括一种快速验证当时信息的状态的手段，但须遵守法律、法规和/或适用的政策；
- 识别和控制所有身份的散播的通用机制，但须遵守法律、法规和/或适用的政策；

7.3.6 实体保证级别

资源及其提供都有相关的保证级别，主要取决于大量的技术和管理因素，应遵守适用的政策和标准。

能力包括对下面各项提供支持：

- 表明公共标识符信息的保证级别，特别是公众电信登记机构，包括分级名称和编号系统中获得指配者的子划分标识符；
- 表明与所提供信息相关的保证级别的共同协议。建议采用通用的全球开放机制；
- 为请求方、依赖方或身份服务提供方等提供一种机制，用于规定某种身份服务的保证和验证条件并规定条件若不满足将采取何种措施。

7.4 身份能力的发现

IdM的一个重要难题是在不断变化、复杂多样的网络能力与应用世界中，为四类核心能力中每一类的发现信息源。目前可提供众多的分布式自主信息来源。仅凭IdM能力存在是不够的。依赖方需要标准的手段了解其存在以及如何到达这些源，如下面的图5所示。发现过程可能需要新的发现协议的支持，性质类似于客户机能够发现DHCP服务器和获取IP地址及网关信息所用的动态主机控制协议。因此，发现过程有可能像身份持有者给依赖方提供有效URI或OID那样简单。

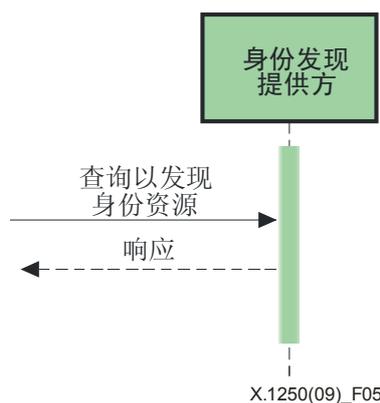


图5 – 任何实体身份发现查询-响应能力和示例

此外，身份能力的发现还应包括通过同盟发现可用的能力。有些采用特定协议的联盟和社区已经制定了解决部分问题的方案以在其用户社区的边界内满足发现要求。不过最近还无法提供全球的或同盟间的发现方案。需要一种支持发现功能的系统。合乎需要的发现能力包括对下面各项提供支持：

- 跨同盟或域的身份服务提供方经营协议政策；
- 单次登入/单次退出，并以一种标准的方式公布该能力，以便使之成为可以发现的能力。

7.5 互操作性和桥接

提供身份管理资源的各方之间的全球互操作性是必不可少的提供要求。本条描述了在同盟内或通过桥接提供方建立信任查询的能力。

同盟是基于两参与域间认证结果互认的原则，而非域间身份信息共享。

7.5.1 同盟相关能力

同盟相关能力包括：

- 依赖方能够通过联盟和参与同盟建立认证（即安全）域；
- 获得请求方的授权以将请求方的身份组成同盟，但须遵守法律、法规和/或适用的政策；
- 请求方能够授权将其身份组成同盟，但须遵守法律、法规和/或适用的政策。

7.5.2 身份桥接相关能力

身份桥接相关能力包括：

- 请求方能够批准和禁止身份桥接功能的能力；
- 发现相关请求方的身份服务提供方的机制；

- 某种身份桥接机制，用于：
 - a) 将某一身份服务提供方处的请求方账户与另一不同认证域中的依赖方组成同盟，条件是每一方都得到了请求方和身份服务桥提供方的适当许可；以及
 - b) 在给依赖方的响应消息中携带身份服务提供方的地址；
- 完成从身份服务提供方处得到的断言/请求实体信息的互操作性，并使之得到不同域（例如两个网络）中相关身份服务提供方和依赖方认可和使用的机制；
- 在通过身份服务桥提供方创建同盟的情况下通知依赖方或身份服务提供方何时身份服务桥提供方的政策发生变化的手段。该机制可让依赖方或身份服务提供方选择终止参与同盟。
- 在通过身份业务桥提供方创建同盟的情况下，当身份业务桥接提供方政策发生变化时可做为通知请求方的手段。该机制允许请求方终止接受同盟或加入同盟。

7.6 IdM安全

由于身份信息和网络资源是网络，特别是被视为关键的国家基础设施一部分的网络的宝贵、敏感和关键组成部分，这种信息和资源需要得到安全保护。保证IdM基础设施的安全包括行政政策、操作实务、技术和技巧，以防止IdM系统和数据损害，而不论数据是稳定的还是过渡性的。

本条为可在[b-ITU-T X.1205]中查到的安全最佳做法补充了若干有助于IdM基础设施安全的能力，包括：

- 所有各方（请求方、依赖方、身份服务提供方）之间安全事务处理（例如采用机密性、完整性、抗重放保护）；
- IdM事务处理的不可抵赖机制；
- 保证身份能力发现的安全，例如避免身份服务提供方模仿；
- 审计IdM事务处理的安全信息；
- 实现根据IdM事务处理分析检测和应对侵入活动的的能力以及在身份信息受到疑似攻击时向身份拥有者发出预警。
- 采取可让依赖方将身份损害信息快速通知身份服务提供方的手段。保证该报告能力不受恶意利用。

使用政策和指令 – 有时也称为“身份治理” – 也是多重身份服务提供方环境中减轻威胁和风险以及保护个人可识别信息的重要措施。凡涉及同盟、同盟或桥提供方，这些措施可由所有参与的依赖方和身份服务提供方颁布。对以用户为中心的IdM应用的使用日益增多，促使提出请求的最终用户规定与其身份属性捆绑的政策，如第7.7节的说明和建议。参与同盟的各方之间实施通用的安全能力有显著的益处。同盟应制定完善的安全规范。

合乎需要的IdM安全和政策能力包括：

- 符合适用的指导原则的实体认证保证能力；
- IdM事务处理的不可抵赖机制；
- 为短时或不断变化的关系动态地确定限时的机制。这可能要求一个双方信任的桥提供方属于一个或多个同盟；
- 同盟之间的安全，包括为应对网络安全威胁而开展的同盟间安全的通信和同盟之间的信息交换的协商机制；
- 让终端物体上的应用能够授权终端用户访问该终端物体的身份信息，但须遵守法律、法规和/或适用的政策；
- 在得到身份受损害或被撤销的报告时相关身份服务提供方所有受影响当事方发送通知的机制；
- 了解身份能力的安全方法；
- 足够详细地记录IdM事务处理的安全信息，以确定责任和启动取证分析；
- IdM事务处理的侵入检测和响应能力；
- 可让依赖方报告身份损害的机制。

7.7 个人可识别信息的保护、控制和使用（PII）

保护个人可识别信息包括几个方面。其中两个方面包括IdM基础设施中安全能力的使用，以及向实体提供透明度和通知的能力的使用，后一种涉及实体身份信息的使用和将其偏好捆绑在该信息上的能力。在这种语境中，“捆绑”指的是某种持续存在的机制，可让某个第三方处理身份信息以发现相关实体的PII政策能力。以用户为中心的产品平台及身份服务桥提供方能力都越来越多地考虑了要实施的这几类偏好。

在某些国家或区域管辖权内，必须公平地收集PII，并且必须符合明确的合法的最终目的。通信各方之间交换的相关信息应限于让“依赖方”可以提供服务所需的数据或及仅限于向“请求方”提供的资源。

从隐私的角度看，在某些国家的管辖权内存在着若干必须考虑的原则：

- 收集绑定PII必须出于具体、明确和合法的目的，在不符合这些目的的情况下不得进行进一步处理；
- 针对所收集和/或进行进一步处理的目的，PII必须充分、相关且不得过度；
- PII必须准确，并随时更新；考虑到所收集或进行进一步处理的目的，必须采取一切合理的步骤确保删除或纠正不准确或不完整的数据；
- 在不超出数据收集或进一步处理的目的所需的时间内，必须确保PII的形式可使数据对象得以识别；
- PII不得在不同用途的应用之间共享；

- PII须仅限用于某具体用途所需的最少情况中；
- 必须确保PII的安全。必须采取适当的技术和组织性措施保护PII免遭意外或非法破坏或意外丢失、更改、非经授权的披露或使用（特别是数据处理涉及在一个网络上的数据传输时），并免遭所有其他形式的非法处理；
- 人有权使用、纠正或删除与其相关的PII；
- PII的保留时间不得超过其特定目的所需的时间。

其他管辖要求有保护机制，包括凡遇到访问账户或遇到信息变动则使用通知。在电信/ICT网络和服务中PII的使用应符合明确的最终目的。正是本着这种最终目的，人们才能够理解已记录数据的相关性、充足性和适量性，理解可能接受这些数据的人或组织的类别，理解已收集数据可以存储的时间长度。

能力包括：

- 根据数据保护和隐私原则及立法收集、处理和保护PII。最低限度应把OECD规定的全球隐私保护指导原则纳入保护措施中。区域/国家的适用规则可能对合规性提出附加的强制性要求（例如95/46/EC号欧洲数据保护指令）；
- 确认并保护经认可的限制，以尽量减少对个人可识别信息的收集。获得PII应有具体、明确和合法的目的，且须经数据主体同意；
- 若身份服务提供方将某个请求方的身份分别与两个或更多依赖方组成同盟，则依赖方应不可能使用身份服务提供方向其提供的信息来确定这些身份指的是同一请求方的功能；
- 在请求方的身份属性变更时的通知服务；
- 在请求方的同意声明变更时的通知服务；
- 对被身份服务提供方理解为试图损害身份拥有者身份的IdM事务处理活动向其提供预警；
- 将身份服务提供方的系统和能力的损害通知身份拥有者；
- 对PII的存储执行时间限制的能力，以便其保留时间不超过其特定目的所需的时间。
- 相关实体根据法律、法规和政策检查、更正和删除PII的能力。

7.8 审计与合规性

IdM受到各种各样法律、监管和业界经营要求的制约，可能有必要提供一定程度的审计与合规性。审计与合规性措施的例子包括维护安全日志，保护和适当使用个人信息，以及向通知中所含的信息适用的实体提供通知。审计应符合上述第7.7节所述的PII保护能力，特别是这可能将会涉及新的一方，造成与隐私法律、法规和政策的冲突。

这些能力包括：

- 启动取证分析的机制；
- 交换身份管理审计信息的安全的共同机制；

- 时戳；
- 根据被审计信息的重要性的时间的价值，在记录中添加与环境有关的时戳；
- 须谨慎确保实施的身份管理审计满足适用的隐私要求。

7.8.1 时戳准确度的能力

精确的时戳对于管理身份的生命周期和维护IdM系统内的安全非常重要，因为所有身份信息都是存在于限定的时间段内的。审计描述了在这些时间段内发生的事件。就审计而言，时戳必不可少，审计数据的质量，甚至其可用性，是由适当事件所处位置的时戳准确度决定的，这种位置可充分审计高度异步且分布极广的网络和应用能力。

合乎需要的能力包括用于足以在商定的共同基准位置进行审计的时戳准确度能力，与双方商定的保证水平相称。

7.9 性能、可靠性和可提供性

IdM是一种重要的网络能力，需要设计和实施以达到性能、可靠性和可提供性目标。建议IdM的可靠性和可提供性目标应与其他关键网络功能不相上下，因为IdM构成了访问认证和授权以及网络中所有事务处理的核心。这是指，例如，确认IdM的能力、环境支持和连通性指标已达到要求。IdM性能（例如查询响应时间）应满足预期IdM查询负荷。

IdM系统的可提供性在所有组成部分（发布要素、看管要素、撤销要素）之间并不是同质的，最终必须与证书中的保护级别联系起来。下面的可提供性要求是合乎需要的，但因构件（库、注册系统、撤销能力）而异：

- 可靠性和可提供性的级别与其他关键网元、系统及能力不相上下；
- 在提供方灾害恢复规划中并入IdM能力；
- 在IdM实现中为IdM事务处理提供合理的响应时间。

7.10 国际化

对于全球互操作性而言，有必要支持使用各种字符集和语言。国际化目标被认为是包括IdM能力在内的所有基于公众网的应用都必需的重要设计和支持。

参考资料

- [b-ITU-T X.509] ITU.T X.509 (2005) | ISO/IEC 9594-8:2005建议书，信息技术 - 开放系统通信 - 号码簿：公开密钥与属性证书框架。
- [b-ITU-T X.805] ITU.T X.805(2003)建议书，端对端通信系统的安全架构。
- [b-ITU-T X.811] ITU-T X.811 (1995) | ISO/IEC 10181-2:1996建议书，信息技术 - 开放系统连接 - 开放系统安全框架：认证框架。
- [b-ITU-T X.1205] ITU-T X.1205(2008)建议书，网络安全概述
- [b-ITU-T X.1251] ITU-T X.1251 (2009) 建议书, 用户控制数字身份的框架
- [b-ITU-T Y.110] ITU-T Y.110(1998)建议书，全球信息基础设施的原则和框架架构。
- [b-ITU-T Y.2012] ITU-T Y.2012 (2006) 建议书，NGN第一版的功能要求与构架。
- [b-ITU-T Y.2702] ITU-T Y.2702(2008)建议书，NGN第一版的认证和授权要求。
- [b-ITU-T Y.2720] ITU-T Y.2720(2009)建议书，NGN身份管理框架。
- [b-IETF RFC2560] IETF, RFC2650(1999)， X.509互联网公开密钥基础设施在线证书状态协议 - OCSP

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