

国际电信联盟

ITU-T

国际电信联盟
电信标准化部门

Y.4805

(08/2017)

Y系列：全球信息基础设施、互联网的协议问题
和下一代网络、物联网和智慧城市
物联网和智慧城市及社区 – 识别与安全

智慧城市应用互操作性的标识符服务要求

ITU-T Y.4805 建议书

ITU-T

ITU-T Y 系列建议书

全球信息基础设施、互联网的协议问题和下一代网络、物联网和智慧城市

全球信息基础设施	
概要	Y.100–Y.199
业务、应用和中间件	Y.200–Y.299
网络方面	Y.300–Y.399
接口和协议	Y.400–Y.499
编号、寻址和命名	Y.500–Y.599
运营、管理和维护	Y.600–Y.699
安全	Y.700–Y.799
性能	Y.800–Y.899
互联网的协议问题	
概要	Y.1000–Y.1099
业务和应用	Y.1100–Y.1199
体系、接入、网络能力和资源管理	Y.1200–Y.1299
传输	Y.1300–Y.1399
互通	Y.1400–Y.1499
服务质量和网络性能	Y.1500–Y.1599
信令	Y.1600–Y.1699
运营、管理和维护	Y.1700–Y.1799
计费	Y.1800–Y.1899
下一代网络	
框架和功能体系模型	Y.2000–Y.2099
服务质量和性能	Y.2100–Y.2199
业务方面：业务能力和业务体系	Y.2200–Y.2249
业务方面：NGN中业务和网络的互操作性	Y.2250–Y.2299
编号、命名和寻址	Y.2300–Y.2399
网络管理	Y.2400–Y.2499
网络控制体系和协议	Y.2500–Y.2599
安全	Y.2700–Y.2799
通用移动性	Y.2800–Y.2899
运营商水平的开放环境	Y.2900–Y.2999
未来网络	Y.3000–Y.3499
云计算	Y.3500–Y.3999
物联网、智慧城市和社区	
综述	Y.4000–Y.4049
定义和术语	Y.4050–Y.4099
要求和应用案例	Y.4100–Y.4249
技术设施、连接和网络	Y.4250–Y.4399
框架、构架和协议	Y.4400–Y.4549
业务、应用、计算和数据处理	Y.4550–Y.4699
管理、控制和性能	Y.4700–Y.4799
识别与安全	Y.4800–Y.4899
评估与评定	Y.4550–Y.4699

如果需要进一步了解细目，请查阅ITU-T建议书清单。

ITU-T Y.4805 建议书

智慧城市应用互操作性的标识符服务要求

摘要

ITU-T Y.4805建议书规定了智慧城市应用中标识符服务的一组要求，以确保这些系统的互操作性和安全性。这组要求还可作为开发新的智慧城市标识符服务的指导原则。其中包括服务完整性和数据机密性的安全特性。本建议书定义了完整的标识符服务要求，包括标识符服务的安全性要求。

历史沿革

版本	建议书	批准	研究组	唯一识别码*
1.0	ITU-T Y.4805	2017-08-22	20	11.1002/1000/13267

关键词

数据机密性，标识符，服务完整性，智慧城市。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL <http://handle.itu.int/>，随后输入建议书的唯一识别码，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、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）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，国际电联已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2017

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	他处定义的术语	1
3.2	本建议书定义的术语	1
4	缩写和首字母缩略语	2
5	惯例	2
6	面向智慧城市应用的标识符服务	2
6.1	服务模型	2
6.2	数据模型	3
6.3	操作模型	3
7	智慧城市应用中标识符服务的要求	3
7.1	标识符服务的一般要求	3
7.2	安全性的一般要求	4
7.3	与服务模型相关的要求	5
7.4	数据模型的要求	6
7.5	操作模型的要求	7

ITU-T Y.4805 建议书

智慧城市应用互操作性的标识符服务要求

1 范围

ITU-T Y.4805建议书规定了智慧城市应用中标识符服务的一组要求，以确保这些系统的互操作性和安全性。这组要求还可作为开发新的智慧城市标识符服务的指导原则。其中包括服务完整性和数据机密性的安全特性。本建议书定义了完整的标识符服务要求，包括标识符服务的安全性要求。

2 参考文献

无。

3 定义

3.1 他处定义的术语

本建议书使用以下其它地方定义的术语：

3.1.1 应用[b-ITU-T Y.2261]：一个结构化的能力集合，这些能力在一个或多个业务的支撑下提供增值功能，它可以由API接口提供支撑。

3.1.2 标识符[b-ITU-T Y.2091]：标识符是用来识别订购用户、用户、网络元素、功能、提供服务和应用的网络实体和其它实体（比如物理或逻辑物体）的一系列数字、字符、符号或其它任何形式的数据。标识符可用于注册和授权。它既可对所有网络公开，也可在有限数目的网络间共享，或是只在特定网络中专用（专用的ID一般不向第三方透露）。

3.1.3 标识符解析[b-ITU-T Y.4108]：将标识符解析为相关信息的功能，反之亦然。

3.1.4 物联网 (IoT) [b-ITU-T Y.4000]：一种信息社会全球基础设施，它基于现有的和新兴的、可互操作的信息通信技术，将物理的和虚拟的“物”相互连接，以提供先进的服务。

注1 – 通过使用标识、数据捕获、处理和通信能力，IoT充分利用物体向各项应用提供服务，同时确保满足安全和隐私要求。

注2 – 从广义而言，IoT可被视为技术和社会影响方面的愿景。

3.1.5 互操作性[b-ITU-T Y.4000]：两个或多个系统或应用交换信息并相互使用已交换信息的能力。

3.2 本建议书定义的术语

本建议书定义了如下术语：

3.2.1 标识符管理：执行支持标识符及标识符属性的生命周期管理的相关功能的能力。这些功能包括注册新标识符、删除现有标识符、修改和更新与标识符相关的任何信息以及根据上述定义3.1.2在具体标识符方案内定义的任何其他相关管理功能。

3.2.2 标识符服务：通过互联网运行的网络信息服务，根据定义3.1.3执行标识符解析，按照上文定义3.2.1进行标识符管理。

3.2.3 标识符服务的根服务：根服务是分层标识符或命名服务顶层的关键组件。例如，域名系统（DNS）将其根服务定义为互联网命名系统顶层的根域名服务器和数据的集合。

4 缩写和首字母缩略语

本建议书采用了以下缩写和首字母缩略语：

ID	标识符
IoT	物联网
TTL	生存时间值
UTF-8	8位Unicode转换格式

5 惯例

关键词“**需**”（**is required to**）指必须严格遵守的要求，如果要宣称符合本文件，就不得违反。

关键词“**建议**”（**is recommended**）指建议但并非需要绝对遵守的要求。因此宣称符合本文件不需要说明已满足此要求。

关键词“**可作为选项**”（**can optionally**）指允许可选的、但并非建议遵守的要求。该术语并非旨在暗示销售商的实施必须提供该选项且该功能部件可作为选项由网络运营商/业务提供商激活，而是指厂商可作为选项提供该功能部件并仍根据规范宣称符合本文件。

在本建议书及其附件中，有时会出现“**须**”（**shall**）、“**不得**”（**shall not**）、“**应**”（**should**）、“**可**”（**may**）等词语。在这些情况下，这些词语应分别理解为“**需**”、“**禁止**”、“**建议**”和“**可作为选项**”。在附录或标为“**用于通报情况**”的材料中出现这些短语和关键词应理解为并非出于规范性的意向。

6 面向智慧城市应用的标识符服务

在服务、数据和操作模型方面对面向智慧城市应用的标识符（ID）服务进行了论述。服务模型探索标识符服务的服务结构以更好地支持智慧城市应用，包括服务组件以及这些组件之间的关系。数据模型定义了智慧城市应用中支持标识符属性所需的以及对安全性和在标识符及标识符属性基础上进行管理操作而言必要的数据结构。操作模型讨论了应由标识符服务提供的基本操作，以及视情况在不同标识符服务组件之间实现协同、透明和可信操作的关键特性。

6.1 服务模型

面向智慧城市应用的标识符服务必须支持在不同城市操作并由不同组织和/或服务提供商管理的应用。分布式服务模型可实现这种标识符服务。

标识符服务的服务模式是指在分布式网络环境下，标识符服务在服务组件方面的服务结构。

面向智慧城市应用的标识符服务可由多个服务组件组成，其中每个组件由不同组织和/或服务提供商管理。标识符服务的每个组件可负责在智慧城市应用中使用的的一个本地标识符域。这些服务组件必须协同工作，从而根据全球唯一标识符识别智慧城市实体，有助于解析和实时更新与标识符相关联的信息。

另一方面，标识符服务的服务组件可由独立于其他组织的各个组织来操作和管理。任何一个组件的中断都不应影响其他组件的服务。标识符及标识符信息的管理可由一个标识符服务组件单独执行，无需依赖于其他组件。

6.2 数据模型

标识符服务的数据模型是指支持其标识符的解析和管理所必需的数据结构。数据结构应足够灵活，以支持现有的智慧城市应用，并允许向后兼容。

智慧城市标识符服务中的标识符不仅可识别智慧城市实体，还可用作对与所识别对象相关的信息的参考。标识符服务的数据模型应定义使所有数据类型能够与标识符相关联的数据结构，以及根据与标识符相关的信息建立信任和/或凭证的通用机制，以使用户可以根据需要验证信息。

6.3 操作模型

标识符服务的操作模型是指应由标识符服务提供以支持智慧城市应用的基本操作，以及标识符服务如何执行这些操作。操作模型还应定义可在不同标识符服务组件之间实现协同运作的特性。

更重要的是，面向智慧城市应用的标识符服务应在每项服务操作中提供明确定义的内置安全服务。安全服务应包括保护服务完整性和数据机密性以及必要时服务不可否认性的选择方案。

7 智慧城市应用中标识符服务的要求

7.1 标识符服务的一般要求

7.1.1 与现有的智慧城市做法兼容

面向智慧城市的标识符服务应考虑到智慧城市应用中的现有做法。要求现有的智慧城市应用能够继续运行，并提供建立与其他智慧城市应用的接口的机制。标识符服务须具备足够的灵活性，以支持现有智慧城市应用中的任何命名约定。

7.1.2 可扩充性

不同的智慧城市应用可能需要与其标识符相关的不同数据。要求智慧城市的标识符服务支持应用定义的数据和元数据结构，使应用能够注册其数据和元数据结构。标识符解析和管理系统须能够处理与标识符相关的所有数据类型。

7.1.3 解析效率

要求智慧城市的标识符服务，特别是对于标识符解析而言，从时间角度是高效的。如果标识符服务亦支持标识符管理，建议考虑为管理定义单独的服务接口。

解析服务可以选择性地使用多种技术来提高效率。这包括但不限于对其他标识符服务的响应时间的测量、缓存、减少或优化查询次数以及处理有缺陷或无响应的标识符服务器。

为提高性能，标识符服务亦可定义缓存机制，以便减少由解析请求产生的网络流量。

7.1.4 可扩展性

要求标识符服务具有可扩展性，以支持智慧城市不断增加的标识符及其日益增长的应用。需要建立分布式服务模型来支持这种可扩展性。在分布式服务模型中，服务的管理方式使各个组织可以独立地管理和运营自己的标识符服务。可选择使每项标识符服务操作均能够建立多个服务复制（镜像），以提供服务冗余，确保负载均衡。还可定义支持服务集群、标识符和/或服务请求的概念的机制。

7.1.5 国际支持

要求智慧城市标识符服务支持Unicode，其中包括目前全世界使用的大多数字符。在网络传输中Unicode字符有多种编码方式。为实现效率和兼容性最大化，对于智慧城市标识符服务，建议使用8位Unicode转换格式（UTF-8）的编码方法。

7.2 安全性的一般要求

7.2.1 安全解析

要求标识符服务在标识符解析方面具备适当的安全水平。须保证服务完整性，以便客户端可验证从标识符服务接收到的数据。在网络传输过程中，还须在解析进程中提供具备适当的数据机密性水平的选择方案。

7.2.2 自主访问控制

许多智慧城市应用要求对其识别的信息进行自主访问控制。要求智慧城市的标识符服务能够针对与其标识符相关的信息定义访问控制。这种访问控制的定义须独立于服务器管理员，以实现最大的灵活性。为实现这一目标，要求标识符服务实施用于客户端认证和授权的接口。

7.2.3 分布式管理和实施界面

参与IoT设备的实时控制和管理的智慧城市应用亦需更改或更新与其标识符相关的状态数据。要求智慧城市的标识符服务提供安全的管理界面，以便应用及时管理和更新标识符属性。

7.3 与服务模型相关的要求

7.3.1 互操作性：分布式服务模型

要求面向智慧城市应用的标识符服务支持分布式服务模型。标识符服务须由支持对等级和层级服务分配的分布式服务组件组成。

对等级分布式服务模型是不同智慧城市应用（在城市边界内外）间标识符服务的分布式管理必需的，使每项智慧城市应用能够独立地提供自己的标识符服务，但在对等应用之间进行协作（见图1）。

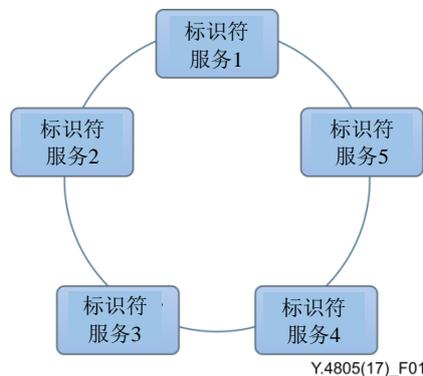


图1 – 对等级分布式服务模型

层级分布式服务模型适合智慧城市应用，反映了层次化组织管理结构，使任何组织能够跨多个子公司域提供共享的标识符服务，同时也使每个子公司都可在必要时运行自己的标识符服务（见图2）。



图2 – 层级分布式服务模型

7.3.2 互操作性：分布式根服务

所有分层服务都需要根服务来锚定服务层次结构。DNS根服务是这类服务的一个示例。要求面向智慧城市应用的标识符服务提供根服务，用作注册服务分层结构下任何服务组件的起点。需要时，还可用于向任何服务组件提供可信的服务转介。面向智慧城市应用的任何分层标识符服务均需要此类根服务。根服务须分散开来，从而不受任何单点故障的影响。还须实现利益攸关多方的对等级管理，从而使该根不受任何单一实体的控制。在不同国家或组织操作自己的根服务器提供标识符服务的情况下，须采取适当措施，防止出现单点故障。

7.3.3 安全性：信任根

需要根服务来建立对分层标识符服务的信任。在分层标识符服务下，标识符服务向其衍生的标识符服务发放凭证。建议将任何标识符服务的凭证作为由上级标识符服务签名的公共密钥，并用于在客户端请求时提供服务完整性方式。要求任何使用标识符服务的客户端都能够跟踪其凭证直到根服务，以验证标识符服务的真实性。

7.3.4 安全性：复制和镜像

分布式标识符服务中的任何标识符服务可作为选项建立多复制服务，以防止任何单点故障。需要在复制站点之间提供多项对等级标识符服务，以实现标识符的同时管理。在这种情况下，需要建立防止竞态条件的机制，其中多个复制站点尝试同时更新同一标识符记录。

7.3.5 互操作性：缓存服务

要求标识符服务支持缓存来帮助减少不必要的网络流量。建议标识符解析结果包含标准的生存时间值（TTL）字段，以表明数据有效的的时间。可作为选项部署专用缓存服务来支持特定的用户社区。

7.3.6 互操作性：支持迭代和递归解析服务

建议由标识符服务来代替终端客户端将查询迭代地或递归地发送至另一个标识符服务执行个体。进行这些查询的标识符服务可缓存返回的答案。

7.4 数据模型的要求

7.4.1 安全性：对标识符属性进行访问控制的通用方案

许多智慧城市应用要求对标识符属性实施访问控制。对于任何特定的标识符，可能只有一部分属性可以向普通公众公开，而对于所有其他属性，只有某些被授权方才可在标识符解析后进行访问。

要求面向智慧城市应用的标识符服务的数据模型包括用于对标识符属性进行访问控制的通用方案，特别是，该方案须支持在标识符属性的任何子集上定义基于角色或组的访问控制。

7.4.2 安全性：支持凭证验证

在分布式计算中，服务完整性仅提供证明数据来自授权服务的方式，并不一定提供数据可信的凭证。要求面向智慧城市应用的标识符服务提供本建议书前面所述的服务完整性，并提供凭证验证的选择方案。建议通过与标识符属性相关的第三方数字签名的方案或者参考可用于验证标识符属性的真实性或可信性的第三方验证服务来定义凭证验证。

7.4.3 安全性：支持自主管理和标识符所有权

要求标识符服务的数据模型为每个标识符管理员提供独立于托管服务的方案，并实现对该标识符及其属性的自主管理。标识符服务的实现须提供保护标识符及其属性的手段，从而只有在获得授权后才能对标识符或其属性进行更改。

在智慧城市应用中，每个已识别的对象可直接与标识符服务进行交互以便对其属性进行实时更新，而不依赖于任何集中式服务器管理员，因此在智慧城市应用中实现自主管理很重要，亦可最大限度地降低未经授权的更改对在标识符服务上托管的标识符的潜在安全风险。

7.4.4 互操作性：可扩展数据模型

智慧城市应用的标识符用于将不同类型的信息与其识别的对象联系起来。要求标识符服务的数据模型足够灵活，以支持针对智能城市应用中的标识符属性定义新的数据类型。智慧城市应用选择定义自己的数据类型并将其注册到标识符服务。

7.4.5 互操作性：适应性命名方案

许多智慧城市应用都有自己的识别方案。几乎很难更改这些应用的命名方案。要求智慧城市应用的标识符服务定义灵活的命名方案，以支持对现有智慧城市应用使用的名称做出调整。

7.5 操作模型的要求

7.5.1 安全性：安全操作

要求智慧城市的标识符服务支持一整套安全标识符操作，包括：

- 1) 创建或注册新的标识符并确定一组与该标识符相关联的属性；
- 2) 解析或查询与任何已注册标识符相关联的属性；
- 3) 安全地更新或修改与现有标识符相关联的标识符属性；
- 4) 删除标识符或删除与标识符相关联的任何属性。

标识符服务应提供标准协议接口来支持这些操作。标识符服务亦提供适当的认证和授权机制，以提高这些操作的安全性。

7.5.2 互操作性：分布式环境下标识符服务的协同运作

服务分层结构中的每项标识符服务都需要在分布式环境下协同工作。接收到服务请求后，接收请求的标识符服务以递归或迭代方式对其进行解析。在递归模式中，标识符服务将服务请求转发给负责的标识符服务，从负责的标识符服务获得响应，并将结果反馈给客户端。在迭代模式下，标识符服务向客户端反馈对负责的标识符服务的参照，并指示客户端将其请求重新发送到负责的标识符服务。

7.5.3 安全性：标识符服务层级之间的信任

分布式分层结构下的每项标识符服务都需要从分层结构中的上级标识符服务接收其服务凭证。建议以签署的公钥或某种公钥证书的形式发放该凭证。在分布式环境下提供服务完整性时，这种凭证是必需的。在特定条件下亦可作为服务不可否认性的方式。与任何标识符服务交互的客户端都可选择一直跟踪其服务凭证直到根标识符服务，以验证其真实性。建议缓存此类验证，以避免不必要的重复操作，前提是缓存的验证有过期或超时设定。

参考文献

- [b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.
- [b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*.
- [b-ITU-T Y.2261] Recommendation ITU-T Y.2261 (2006), *PSTN/ISDN evolution to NGN*.
- [b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.
- [b-ITU-T Y.4108] Recommendation ITU-T Y.4108/Y.2213 (2008), *NGN service requirements and capabilities for network aspects of applications and services using tag-based identification*.

ITU-T 建议书系列

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	数据网、开放系统通信和安全性
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题