

国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.500

(08/2005)

X系列：数据网和开放系统通信及安全
号码簿

**信息技术 — 开放系统互连 — 号码簿：
概念、模型和服务概述**

ITU-T X.500建议书

ITU-T X系列建议书
数据网和开放系统通信及安全

公众数据网	
业务和设施	X.1-X.19
接口	X.20-X.49
传输、信令和交换	X.50-X.89
网络概貌	X.90-X.149
维护	X.150-X.179
管理安排	X.180-X.199
开放系统互连	
模型和记法	X.200-X.209
服务限定	X.210-X.219
连接式协议规范	X.220-X.229
无连接式协议规范	X.230-X.239
PICS书写形式	X.240-X.259
协议标识	X.260-X.269
安全协议	X.270-X.279
层管理对象	X.280-X.289
一致性测试	X.290-X.299
网间互通	
概述	X.300-X.349
卫星数据传输系统	X.350-X.369
以IP为基础的网络	X.370-X.379
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	
组网	X.600-X.629
效率	X.630-X.639
服务质量	X.640-X.649
命名、寻址和登记	X.650-X.679
抽象句法记法1(ASN.1)	X.680-X.699
OSI管理	
系统管理框架和结构	X.700-X.709
管理通信服务和协议	X.710-X.719
管理信息的结构	X.720-X.729
管理功能和ODMA功能	X.730-X.799
安全	X.800-X.849
OSI应用	
托付、并发和恢复	X.850-X.859
事务处理	X.860-X.879
远程操作	X.880-X.889
ASN.1的一般应用	X.890-X.899
开放分布式处理	X.900-X.999
电信安全	X.1000-X.1999

欲了解更详细信息，请查阅ITU-T建议书目录。

信息技术 — 开放系统互连 —
号码簿: 概念、模型和服务概述

摘 要

本建议书|国际标准介绍了号码簿和 DIB（号码簿信息库）的概念，并对它们提供的服务和能力进行了概述。

来 源

ITU-T 第 17 研究组（2005-2008）按照 ITU-T A.8 建议书规定的程序，于 2005 年 8 月 29 日批准了 ITU-T X.500 建议书。相同的文本也作为 ISO/IEC 9594-1 出版。

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

本建议书为简要而使用的“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，这可能不是最新信息，因此大力提倡他们查询电信标准化局（TSB）的专利数据库。

© 国际电联 2006

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
1 范围	1
2 规范性参考文献	1
2.1 等同的建议书 国际标准	1
3 定义	2
3.1 通信模型定义	2
3.2 号码簿模型定义	2
3.3 分布式操作定义	3
3.4 复制定义	3
3.5 基本号码簿定义	3
4 缩写	3
5 惯例	4
6 号码簿概述	4
7 号码簿信息库 (DIB)	5
8 号码簿服务	7
8.1 介绍	7
8.2 服务限定	7
8.2.1 服务控制	7
8.2.2 安全参数	7
8.2.3 过滤器	8
8.3 号码簿查询	8
8.3.1 阅读	8
8.3.2 比较	8
8.3.3 列表	8
8.3.4 搜索	8
8.3.5 放弃	8
8.4 号码簿修改	8
8.4.1 增加条目	8
8.4.2 删除条目	8
8.4.3 修改条目	8
8.4.4 修改识别名	9
8.5 其他输出	9
8.5.1 错误	9
8.5.2 提名	9
9 分布式号码簿	9
9.1 功能模型	9
9.2 组织模型	10
9.3 模型的操作	10
10 号码簿的访问控制	14
11 服务管理	15
12 号码簿复制	15
12.1 介绍	15
12.2 号码簿复制的形式	16
12.3 号码簿信息的复制和一致性	17
12.4 复制视点	17
12.4.1 号码簿用户视点	17
12.4.2 主管部门用户视点	17

		页
	12.4.3 DSA 视点	18
12.5	复制和访问控制	18
13	号码簿协议	18
14	号码簿系统管理	18
14.1	介绍	18
14.2	DIT 域的管理	19
14.3	号码簿组件的管理	19
附件 A	— 号码簿的应用	20
A.1	号码簿环境	20
A.2	号码簿服务特性	20
A.3	号码簿的使用方式	20
A.3.1	介绍	20
A.3.2	查找	20
A.3.3	用户友好的命名	21
A.3.4	浏览	21
A.3.5	黄页	21
A.3.6	搜索限制和放宽	21
A.3.7	分组	22
A.3.8	认证	22
A.3.9	基于属性的定位	22
A.4	通用应用	22
A.4.1	介绍	22
A.4.2	个人间通信	22
A.4.3	系统间通信（为 OSI 定义）	23
附件 B	— 修正案和勘误	24

引言

本建议书|国际标准连同本系列其他建议书|国际标准是为方便信息处理系统之间的互连以提供号码簿服务而制定的。所有这些系统的集合，连同它们所拥有的号码簿信息可被视为一个整体，被称为号码簿。号码簿所拥有的信息，总称为号码簿信息库(DIB)，典型地被用于方便对象之间的通信、与对象的通信或有关对象的通信等，这些对象如应用实体、个人、终端和分发表等。

号码簿在开放系统互连中扮演了重要角色，其目标是在它们自身的互连标准之外做最少的技术约定的情况下，允许下述各种信息处理系统之间的互连：

- 来自不同生产厂商；
- 具有不同的管理；
- 具有不同的复杂程度，以及
- 有不同的年代。

本建议书|国际标准介绍了号码簿和 DIB 的概念并对其建模，同时对它们所提供的服务和能力进行了概述。其他建议书|国际标准在定义号码簿所提供的抽象服务以及定义获取或传播这些服务所使用的协议时，使用了该模型。

本建议书|国际标准提供了一个基础框架，在此框架基础上，其他标准化组织和业界论坛可以定义工业配置集。在本框架中定义为可选的许多特性，可通过配置集的说明，在某种环境下作为必选特性来使用。目前本建议书|国际标准的第 5 版是原有第 4 版的修订和增强，但不是替代。在系统实现时仍可以声明为遵循第 4 版。然而，在某些方面，将不再支持第 4 版（即不再消除一些报告上来的错误）。建议在系统实现时尽快遵循第 5 版。

第 5 版详细定义了号码簿协议的第 1 版和第 2 版。

第 1 版和第 2 版仅定义了协议第 1 版。本版本（第 5 版）中定义的许多服务和协议被设计为可运行在第 1 版下。然而，一些增强的服务和协议，如署名错误，只有包含在操作中的所有的号码簿条目都协商支持协议第 2 版时才可运行。无论协商的是哪一版，第 5 版中所定义的服务之间的差异和协议之间的差异，除了那些特别分配给第 2 版的外，都可以使用 ITU-T X.519 建议书| ISO/IEC 9594-5 中定义的扩展规则调节。

附录 A，作为本建议书|国际标准的组成部分，描述了号码簿应用的类型。

附录 B，不是本建议书|国际标准的组成部分，列出在本建议书|国际标准的本版本中考虑到的修正案和勘误。

国际标准 ITU-T 建议书

信息技术 — 开放系统互连 — 号码簿: 概念、模型和服务概述

1 范围

号码簿提供了 OSI 应用、OSI 管理进程、其他 OSI 层实体以及电信业务所要求的号码能力。它所提供的能力包括：“用户友好的命名”，即对象可以以人适合记忆的名字被引用（尽管并不是所有的对象都需要拥有用户友好名）；“名字与地址之间的映射”，即对象名称与它们的动态地址之间的绑定。后一个能力使得 OSI 网络可以是“自配置的”，当增加、删除和修改对象所在位置时，不会影响到 OSI 网络的运行。

号码簿并不是一个具有通用目的的数据库系统，尽管它可能是建立在这样的系统上的。比如有这样的假定，与号码簿之间通信，典型的、出现频率相当高的是“查询”而非修改。修改的比率是由个人和组织的动态性来决定的，而不是由网络的动态性来决定的。另外，也没有必要承诺对全局信息进行即时修改，存在同一信息的新旧版本均可用的瞬变过渡状态也是完全可以接受的。

除了区分访问权限或不传播修改等特性外，号码簿的另一个特性是其号码查询结果将不取决于请求者的身份或位置。这个特性使得号码簿不适合应用在某些电信应用中，如一些路由类型的应用。在结果取决于请求者身份的情况下，对号码簿信息的访问和修改可能会被拒绝。

2 规范性参考文献

下列建议书和国际标准所包含的条款，通过在本建议书中的引用而构成本建议书 | 国际标准的条款。在出版时，所指出的版本是有效的。所有的建议书和标准都面临修订，使用本建议书 | 国际标准的各方应探讨使用下列建议书和国际标准最新版本的可能性。IEC 和 ISO 的各成员有目前有效的国际标准的目录。国际电联电信标准化局有目前有效的 ITU-T 建议书的清单。

2.1 等同的建议书 | 国际标准

- ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.
- ITU-T Recommendation X.501 (2005) | ISO/IEC 9594-2:2005, *Information technology – Open Systems Interconnection – The Directory: Models*.
- ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- ITU-T Recommendation X.511 (2005) | ISO/IEC 9594-3:2005, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition*.
- ITU-T Recommendation X.518 (2005) | ISO/IEC 9594-4:2005, *Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation*.
- ITU-T Recommendation X.519 (2005) | ISO/IEC 9594-5:2005, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications*.
- ITU-T Recommendation X.520 (2005) | ISO/IEC 9594-6:2005, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.

- ITU-T Recommendation X.521 (2005) | ISO/IEC 9594-7:2005, *Information technology – Open Systems Interconnection – The Directory: Selected object classes*.
- ITU-T Recommendation X.525 (2005) | ISO/IEC 9594-9:2005, *Information technology – Open Systems Interconnection – The Directory: Replication*.
- ITU-T Recommendation X.530 (2005) | ISO/IEC 9594-10:2005, *Information technology – Open Systems Interconnection – The Directory: Use of systems management for administration of the Directory*.

3 定义

就本建议书|国际标准而言下列定义适用。

3.1 通信模型定义

下述术语在 ITU-T X.519 建议书 | ISO/IEC 9594-5 中定义：

- a) 应用实体；
- b) 应用层；
- c) 应用进程。

3.2 号码簿模型定义

下述术语在 ITU-T X.501 建议书 | ISO/IEC 9594-2 中定义：

- a) 访问控制；
- b) 公用号码簿管理域；
- c) 别名；
- d) 祖先；
- e) 属性；
- f) 属性类型；
- g) 属性值；
- h) 认证；
- i) 复合条目；
- j) 上下文；
- k) 号码簿信息树（DIT）；
- l) 号码簿管理域（DMD）；
- m) 号码簿系统代理（DSA）；
- n) 号码簿用户代理（DUA）；
- o) 识别名；
- p) 条目；
- q) （条目的）家族；
- r) 层次分组；
- s) LDAP 客户；
- t) LDAP 请求者；
- u) LDAP 响应者；
- v) LDAP 服务器；
- w) 名称；
- x) （感兴趣的）对象；
- y) 专用号码簿管理域；
- z) 相关的条目；
- aa) 相对识别名；
- bb) 根；

- cc) 模式;
- dd) 安全策略;
- ee) 下级对象;
- ff) 上级条目;
- gg) 上级对象;
- hh) 树。

3.3 分布式操作定义

下述术语在 ITU-T X.518 建议书 | ISO/IEC 9594-4 中定义:

- a) 单链接;
- b) 多链接;
- c) 提名。

3.4 复制定义

下述术语在 ITU-T X.525 建议书 | ISO/IEC 9594-9 中定义:

- a) 高速缓冲;
- b) 高速缓冲拷贝;
- c) 条目拷贝;
- d) 主 DSA;
- e) 复制;
- f) 镜像使用者;
- g) 镜像提供者;
- h) 镜像信息;
- i) 镜像合约。

3.5 基本号码簿定义

下述术语在本建议书|国际标准中定义:

3.5.1 the Directory 号码簿: 为提供号码簿服务而协作的开放系统的集合。

3.5.2 directory information base (DIB) 号码簿信息库: 由号码簿管理的信息的集合。

3.5.3 (directory) user (号码簿) 用户: 号码簿的最终用户, 即访问号码簿的实体或个人。

4 缩写

就本建议书|国际标准而言, 下列缩写适用:

ACI	访问控制信息
ADDMD	公用号码簿管理域
DAP	号码簿访问协议
DIB	号码簿信息库
DISP	号码簿信息镜像协议
DIT	号码簿信息树
DMD	号码簿管理域
DOP	号码簿操作绑定管理协议
DSA	号码簿系统代理
DSP	号码簿系统协议
DUA	号码簿用户代理
LDAP	轻量级目录访问协议

OSI	开放系统互连
PRDMD	专用号码簿管理域
RDN	相对识别名

5 惯例

除少数例外，本号码簿规范是根据“ITU-T | ISO/IEC 通用文本的表述准则（2001 年 11 月）”的要求制定的。

术语“号码簿规范（或本号码簿规范）”指的是 ITU-T X.500 建议书|ISO/IEC 9594-1。术语“系列号码簿规范”指的是 X.500 系列建议书和 ISO/IEC 9594 的所有部分。

本号码簿规范使用术语“第 1 版系统”来指遵循系列号码簿规范第 1 版的所有系统，即 1988 年版本的 CCITT X.500 系列建议书和 ISO/IEC 9594: 1990 版本。本号码簿规范使用术语“第 2 版系统”来指遵循系列号码簿规范第 2 版本的所有系统，即 1993 版本的 ITU-T X.500 系列建议书和 ISO/IEC 9594: 1995 版本。本号码簿规范使用术语“第 3 版系统”来指遵循系列号码簿规范第 3 版的所有系统，即 1997 版本的 ITU-T X.500 系列建议书和 ISO/IEC 9594: 1998 版本。本号码簿规范使用术语“第 4 版系统”来指遵循系列号码簿规范第 4 版的所有系统，即 2001 年版本的 ITU-T X.500、X.501、X.511、X.518、X.519、X.520、X.521、X.525、X.530 建议书和 2000 年版本的 ITU-T X.509 建议书以及 ISO/IEC 9594: 2001 年版本的第 1 到第 10 部分。

本号码簿规范使用术语“第 5 版系统”来指遵循系列号码簿规范第 5 版的所有系统，即 2005 年版本的 ITU-T X.500、X.501、X.509、X.511、X.518、X.519、X.520、X.521、X.525 和 X.530 建议书，以及 ISO/IEC 9594: 2005 版本的第 1 到第 10 部分。

本号码簿规范使用粗体字体来表示 ASN.1 符号。若在常规文本中要表示 ASN.1 的类型和值时，为了区别于常规文本，使用了粗体字表示。为了表示过程的语义而引用过程名时，为了区别于常规文本，使用了粗体字表示。访问控制许可使用斜体字表示。

6 号码簿概述

号码簿是为提供号码簿服务而协作的开放系统的集合，这些开放系统拥有一个关于现实世界中各种对象信息的逻辑数据库。号码簿的用户，包括个人和计算机程序，在拥有权限的情况下，能够读取或修改这些信息的全部或一部分。每个用户通过一个号码簿用户代理（DUA）或一个 LDAP 客户机来访问号码簿，DUA 或 LDAP 客户机都被认为是一个应用进程。上述概念在图 1 中举例说明。

注一 本系列号码簿规范指的是单一号码簿，且可以通过一个单一的、统一的命名空间来创建一个由多个系统组成的，为多种应用服务的逻辑号码簿。这些系统之间是否选择要进行交互将取决于它们所支持的应用。如果应用处理的是不需要交互的对象，则系统间没有交互需求。若该需求有变化，则单一的命名空间将会简化未来所需的交互。由于各种原因，如安全、连接性或商业决定等，对使用第 3 版的号码簿系统来说，有可能号码簿的某些部分对号码簿的其他部分来说是不可获取的。这就使得所看到的号码簿视图不相同。这种视图的不同可能包括与某个现实世界中对象相关的条目。这些相关的条目可能具有相同的识别名或不同的识别名。若使用第 4 版或后续版本规范的系统，则可以跨多个不同的视图来执行操作，以便对用户提供一个整体的响应。具体说明如下：

- DMD 的主管部门（见第 9.2 节）可能会有发布他们自己对某些特定的现实世界对象的视图的需要，因此一个现实世界的对象在号码簿中可能会通过多个独立的条目来建模。无论这些对象间是否需要交互都可能发生这种情况。使用 DSP 的交互可能也不会被支持。
- 尽管如本注的最后一句话所说，但对某些 DMD 来说，还是有可能选择在他们自己独特的号码簿命名空间（即 DIT 之一）中发布关于现实世界对象的信息；在这种情况下，某一个特定的现实世界的对象在相同的或不同的 DIT 命名空间中可能会被建模为不同的条目，每个条目都有相同的或不同的识别名。注意，当不同的对象被允许共享识别名时，某些类型的号码簿工具（例如，证书的获取以及基于数字签名的相关功能等）是无法实现的。

- 相关条目的目的是提供一种方法，由此用户能够访问到这些条目，并且在可能的情况下共同提供结果信息。这将应用于上述两条所描述的情况。

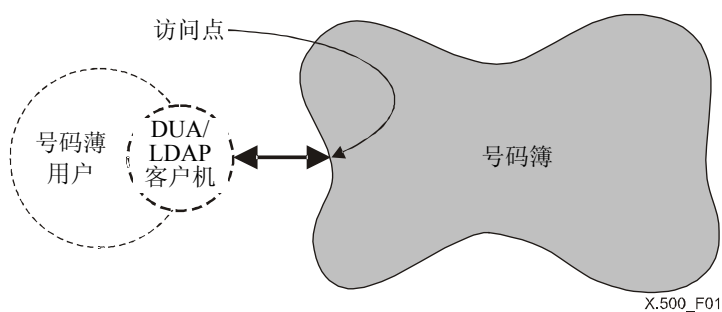


图 1—号码簿的访问

号码簿中存储的信息被统称为“号码簿信息库 (DIB)”。第 7 节给出了 DIB 结构的概述。

号码簿向用户提供了一个定义良好的访问能力集，它被称为号码簿抽象服务。该服务提供了一个简单的修改和查询能力，在第 8 节中给出了概要描述。该服务与本地 DUA 功能联合，可提供终端用户所要求的能力。

号码簿在功能上和组织上都是分布式的。第 9 节给出了相应的号码簿模型的概述。这些模型的开发，为不同组件间进行协作提供了一个框架。

号码簿存在于这样的环境中，即不同的主管当局分别对他们所拥有的部分信息的访问进行控制。第 10 节给出了访问控制的概述。

由于号码簿是分布式的，因此为了提高性能和可用性，可能会有复制信息的需求。第 11 节给出了号码簿复制机制的概述。

号码簿服务的指配和使用将要求用户（实际上是 DUA 和/或 LDAP 客户机）与号码簿的各种功能组件间相互合作。在许多情况下，会要求不同开放系统中的不同应用进程间进行合作，因此会要求一个标准化的应用协议，第 11 节将对影响这些合作的应用协议给出概要描述。

由于需求的多种可能性，号码簿被设计为可以支持多种应用。根据所支持应用的特性决定了号码簿中应列有哪些对象、哪些用户可以访问信息以及用户可以执行哪种类型的访问等。应用可能会非常特定，如电子邮件分发列表的指配；可能会很通用，如“个人间通信号码簿”应用等。号码簿可以提供机会在不同的应用间挖掘到共性，如：

- 一个单独的对象可能与多个应用相关，甚至可能一个对象内的一部分信息就具有这种相关性（与多个应用相关）。
- 为了支持该特性，定义了一系列的对象类和属性类型，可跨多个应用来使用。这些定义包含在 ITU-T X.520 建议书 | ISO/IEC 9594-6 和 ITU-T X.521 建议书 | ISO/IEC 9594-7 中。
- 在不同的应用中使用这些号码簿的方式是相同的：附件 A 给出了这方面的概述。

7 号码簿信息库 (DIB)

注 1 — DIB 及其结构在 ITU-T X.501 建议书 | ISO/IEC 9594-2 中定义。

DIB 由对象相关的信息构成。它由（号码簿的）条目组成，每个条目包括一个对象的信息集合。一个条目可能由一个成员条目集组成，每个成员条目都包含一个对象的某个特定方面的信息。这样的条目集被称为一个复合条目。每个条目都由属性组成，每个属性拥有一个属性类型和一个或多个属性值。出现在一个特定条目中的属性类型独立于该条目所描述的对象类。一个属性的每个值可能会加上一个或多个上下文的标签，这些上下文描述了关于该值的特定信息，可用来对属性值的适用性进行判断。

DIB 的条目以树型结构进行组织，即号码簿信息树（DIT）；号码簿信息树的各顶点代表条目，树中较高的条目（接近根节点）常常代表如国家、组织等对象，而较低的条目常常代表个人或应用进程。

注 2 — 在本系列号码簿规范中定义的服务仅对树型结构的 DIT 进行操作。本系列号码簿规范不排除未来（根据需求）存在其他结构的可能性。

每个条目都具有一个识别名，惟一地、无二义性地标识了条目。识别名的这种特性来自信息的树型结构。每个条目的识别名由其上级条目的识别名加上本条目的特定命名属性值（即识别值）共同组成。

位于树叶节点的条目有一些是别名条目，而其他条目则是对象条目和复合条目。别名条目指向对象条目，并且为相应对象提供了可替代名称的基础。

复合条目代表了一个单独的对象，它是由多个成员条目组合而成的，每个成员条目都代表了对象的某部分信息。

号码簿执行一系列的规则，确保经过长期的修改后 DIB 仍能够保持良好的形状。这些规则被称为“号码簿模式（Schema）”，该模式可以保护条目的对象类不具有错误的属性类型，保护属性类型不具有错误的属性值形式，甚至保护条目不具有类不匹配的子条目等。

图 2 说明了上述关于 DIT 及其组件的概念。

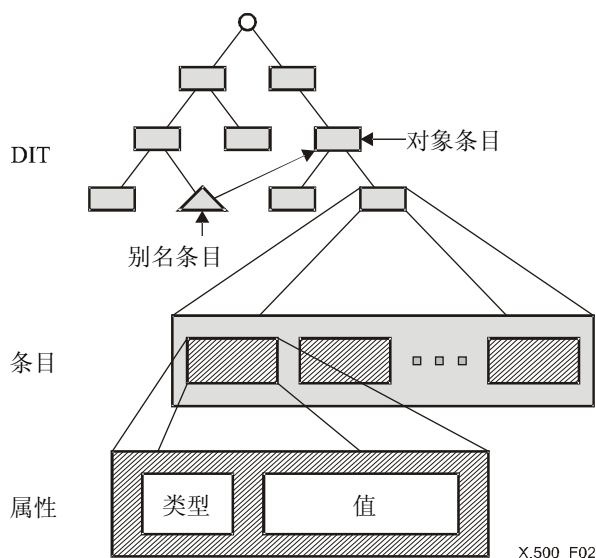


图 2—DIT 及其条目的结构

图 3 给出了一个 DIT 的假设示例。该树提供了用于标识不同对象的属性类型示例，例如，名字

{C=GB, L=Winslow, O=Graphic Services, CN=Laser Printer}

表示应用实体“Laser Printer（激光打印机）”，在它的识别名中包含了其所在地的地理属性。

居民，John Jones，他的名字是{C=GB, L=Winslow, CN=John Jones}，在他的识别名中包含了同样的地理属性。

DIT 的发展和构成形式、号码簿模式的定义和增加条目时对识别名的选择等，可由不同的主管当局来负责，它们之间的层次关系可以从树的形状中体现出来。这些主管当局必须通过认真地管理识别名中出现的属性类型和属性值，来确保在他们的权限范围内所有的条目都具有无二义性的识别名。通过对模式执行控制，这些职责从树的高层主管部门传递到底层主管部门。

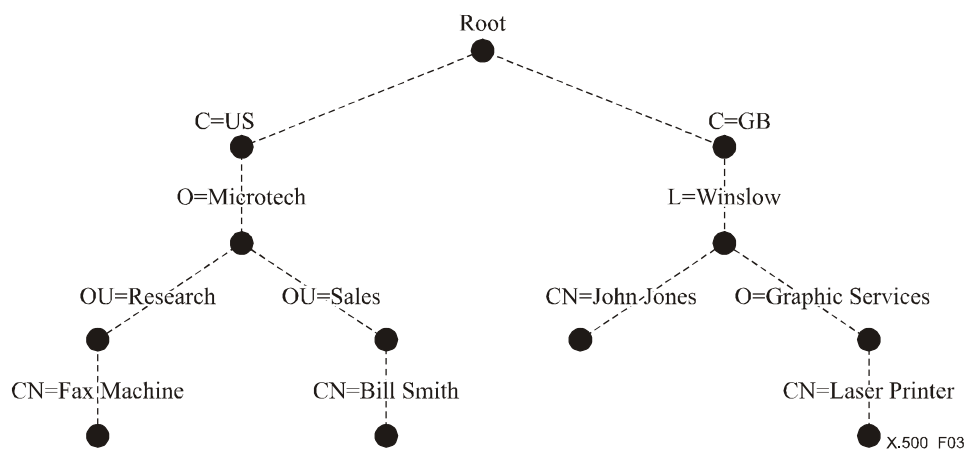


图3—一棵假定的号码簿信息树

层次分组功能允许在条目间建立可替换的层次关系，这种层次关系独立于 DIT 结构所反映出的层次关系。号码簿查询操作（见第 8.3.4 节）不仅能够返回匹配条目的信息，而且能够返回匹配条目可能属于的层次分组中其他成员的信息。层次分组功能还有一个好处是它允许改变层次关系，而不会改变 DIT 的结构，因此也不会改变条目的识别名。

8 号码簿服务

注 — 号码簿抽象服务的定义见 ITU-T X.511 建议书 | ISO/IEC 9594-3。

8.1 介绍

本节概述了号码簿通过它们的 DUA 和/或 LDAP 客户机提供给用户的服务。号码簿提供的所有服务都是对 DUA 和/或 LDAP 客户机服务请求的响应。这些请求可以允许对号码簿进行查询，在第 8.3 节描述；可以允许对号码簿进行修改，在第 8.4 节描述。另外，对服务的请求可以进行限定，在第 8.2 节描述。号码簿总是会报告对每个请求的响应结果。正常结果的格式是与特定请求相对应的，并且会在请求中给出明确的描述。许多异常结果对多种请求来说是通用的。这些可能性在第 8.5 节描述。

号码簿将确保 DIB 的任何改变，无论是由于服务请求引起的，还是其他原因（如本地）引起的，都不会影响 DIB 继续遵循号码簿模式中的规则。

在对号码簿进行访问的访问点，用户和号码簿将被绑定一段时间。在绑定的时间内，用户和号码簿可以可选地验证对方的身份。

8.2 服务限定

8.2.1 服务控制

许多控制可应用于各种服务请求，主要是允许用户对资源的使用加以限制，使得号码簿不应超越该限制，同时还可以控制号码簿操作的进程。控制可以应用在如次数、结果的长度、查询的范围、交互模式以及请求的优先级等方面。

8.2.2 安全参数

为保护号码簿中的信息，每一个请求都可以携带支持安全机制的信息。这些信息可能包括用户为各种类型的保护而提出的请求、服务请求的数字签名以及帮助合法方验证签名的信息等。

8.2.3 过滤器

许多请求的结果中都包括了来自多条条目的信息或者与多条条目相关的信息，这样的请求一般都带有一个或多个过滤器。一个过滤器描述了一个或多个条件；当某些条目或复合条目满足这些条件后，才会作为结果的一部分被返回。过滤器的使用可将返回结果限定在这些相关的条目中。

8.3 号码簿查询

8.3.1 阅读

阅读请求的目标是一个特定的条目或复合条目，操作结果是该条目的所有属性或部分属性的值被返回。若目标为一个复合条目，则其家族成员的信息将包含在一个包（语法与一个属性语法类似）中返回，包中包含了所选择的家族信息。若仅需要有部分属性被返回，则 DUA 在请求中将提供感兴趣的属性类型的列表。一个 DUA 还可能在请求中提供一个或多个感兴趣的属性类型的一个或多个上下文，以便仅仅选择适用于这些指定上下文的值。

注 — LDAP 代理不支持阅读操作。

8.3.2 比较

比较请求的目标是一个条目或复合条目的一个特定属性，操作结果是号码簿检查给出的属性值是否与该属性的值相匹配。一个 DUA 可能也会在请求中提供一个或多个关于感兴趣的属性值的上下文，以便对比较操作进行限定。

注 — 例如，该服务可用于对口令的检查，号码簿中的口令可能不能被阅读服务所访问，但对比较服务而言是可访问的。

8.3.3 列表

列表请求将使号码簿返回 DIT 中某个特定条目的直接下属列表。一个 DUA 可能也会在请求中提供一个或多个上下文，以便用于在返回的 RDN 中进行选择。

注 — LDAP 客户机不支持列表操作。

8.3.4 搜索

搜索请求将使号码簿返回符合某些过滤条件的一个或多个 DIT 部分中的所有条目或复合条目的信息。从每个条目中返回的信息包括该条目的部分或所有属性，与阅读服务的返回信息相同。从其他相关条目中返回的信息可能会根据某些联合条件进行组合。

可以对搜索的类型加以限制，这些限制通过使用搜索规则来执行。或者作为搜索规则的一种方便用法，可在一个单独的号码簿操作中逐渐地放宽或加强搜索条件，否则太少的或太多的条目信息将被返回。

8.3.5 放弃

放弃请求应用于一个正在进行的查询请求，通知号码簿该请求的发起者不再对正在执行的请求感兴趣了。结果是，号码簿可能会终止请求的执行，并放弃到目前为止获取到的任何结果。

8.4 号码簿修改

8.4.1 增加条目

增加条目请求的结果是一个新的叶节点条目增加到 DIT 中。在新条目的属性值中可以包括上下文。

8.4.2 删除条目

删除条目请求的结果是一个叶节点条目从 DIT 中删除，或者如果需要时，组成一个复合条目的成员条目从 DIT 中删除。

8.4.3 修改条目

修改条目请求的结果是号码簿对某个特定的条目或某个家族成员执行一系列的修改。或者是所有的修改都被执行，或者是没有任何修改被执行，而 DIB 总是处于与架构保持一致的状态。所允许的修改包括对

属性或属性值的增加、删除、替代等。在增加条目的属性值时，可以在属性值中包括上下文。修改条目操作仅可应用于一个单独的家族成员，而不能将整个复合条目作为一个整体来修改。

如果需要的话，当一个修改条目操作成功执行后，该操作的返回结果中可以提供条目或复合条目所包含的信息。

8.4.4 修改识别名

修改识别名 (DN) 请求用来修改一个条目 (或者是对象条目，或者是别名，或者是一个家族成员) 的相对识别名，或者用来将一个条目 (非家族成员条目) 移动到 DIT 中的另一个上级条目下。如果这个条目有下级条目，则所有的下级条目都被相应地重命名或移动。在条目的新相对识别名 RDN 中可能会包含上下文。如果条目是家族成员，则只有当它们仍然处于同一个复合条目中时，它们才可以被移动到一个新的上级条目下。

8.5 其他输出

8.5.1 错误

任何服务都可能失败，例如由于用户提供的参数有问题，在这种情况下，将会报告错误。在返回的错误中会携带信息，以便尽可能地帮助纠正错误。然而，一般来说，仅仅是号码簿遇到的第一个错误被上报。除了上面提到的由于用户提供的参数错误的例子 (尤其是不合法的条目名称或不合法的属性类型) 外，其他如违反了安全策略、架构规则以及服务控制等也会引起错误。

8.5.2 提名

当 DUA 或 LDAP 客户机绑定的某个服务的特定访问点不是很适合执行某个请求时，该服务也可能会失败，例如，一个请求所影响到的信息 (在逻辑上) 距离访问点很远。在这种情况下，号码簿可能会返回一个提名，给出一个替代访问点的建议，DUA 或 LDAP 客户机可以对这个替代访问点发起相应请求。

注 — 关于是否使用提名，或者请求是否被链接 (见第 9.3 节)，号码簿和 DUA 可能各自都会有一个倾向。DUA 可以通过服务控制来表达自己的倾向，最后由号码簿决定使用哪种方法。

9 分布式号码簿

注 — 号码簿模型在 ITU-T X.501 建议书 | ISO/IEC 9594-2 中定义，同时，分布式号码簿的操作过程在 ITU-T X.518 建议书 | ISO/IEC 9594-4 中定义。

9.1 功能模型

号码簿的功能模型如图 4 所示。

号码簿系统代理 (DSA) 是一个应用进程，构成号码簿的一部分，它的作用是为 DUA、LDAP 客户机和/或其他 DSA 提供对 DIB 的访问。DSA 在执行请求时，可能会使用存储在本地数据库中的信息，也可能与其他 DSA 或 LDAP 服务器交互来获取信息。作为一种选择方案，DSA 可以将请求者直接转到另一个 DSA 来帮其执行请求。DSA 如果它能够发起一个 LDAP 请求，并且理解相应的 LDAP 响应，则被称为 LDAP 请求者。DSA 如果它能够理解一个 LDAP 请求，并且可对此 LDAP 请求进行响应，则被称为 LDAP 响应者。本地数据库的实现是完全独立的。

LDAP 服务器是一个应用进程，构成号码簿的一部分，它通过 LDAP 协议响应请求，它的作用是为 LDAP 客户机和/或 LDAP 请求者提供对 DIB 的访问。LDAP 服务器可能会使用存储在本地数据库中的信息，也可能直接将请求者转接到另一个能够帮助其执行请求的 LDAP 响应者或 LDAP 服务器。与 DSA 类似，本地数据库的实现是完全独立的。

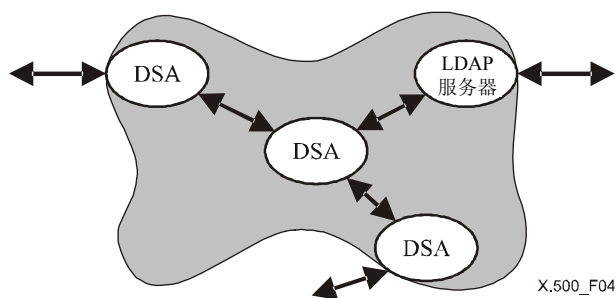


图 4—号码簿的功能模型

9.2 组织模型

由一个独立的组织所管理的一个或多个 DSA、LDAP 服务器、零个或多个 DUA 以及 LDAP 客户机等集合，构成了一个号码簿管理域（DMD）。相应的组织可能选择或不选择使用本系列号码簿规范来管理 DMD 内的各功能组件之间的通信。

其他的号码簿规范定义了 DSA 行为的某些特定方面。为了这个目的，根据管理该 DMD 的组织的选择，一个 DMD 内的 DSA 组的行为可能与一个单独的 DSA 相同。

DMD 可能是一个公用号码簿管理域（ADDMD），或者是一个专用号码簿管理域（PRDMD），这取决于它是否被一个公用电信管理组织运作。

9.3 模型的操作

DUA 或者 LDAP 客户机通过与一个或多个 DSA 和/或 LDAP 服务器来与号码簿进行交互，一个 DUA 或 LDAP 客户机不必绑定到某个特定的 DSA 或 LDAP 服务器。它可直接与不同的 DSA 和/或 LDAP 服务器进行交互发出请求。由于某些管理方面的原因，它可能不能总是与执行请求（如返回号码簿信息）的 DSA 或 LDAP 服务器直接交互。还有一种可能是 DUA 或 LDAP 客户机通过一个单独的 DSA 访问号码簿。为了这个目的，不同的 DSA 之间需要进行交互。

DSA 的工作是执行 DUA 和 LDAP 客户机的请求，并且获取它所没有具备的信息。它可能还负责代表 DUA 或 LDAP 客户机，通过与其他 DSA 和/或 LDAP 服务器交互来获取信息。

图 5 到图 7 举例说明了一些请求处理的情况，描述如下。

在图 5a 中，DSA C 从 DSA A 中获得了一个提名，它将负责或者将请求转发到 DSA B（在 DSA A 给出的提名中的 DSA 名称），或者将提名返回给发起请求的 DUA。

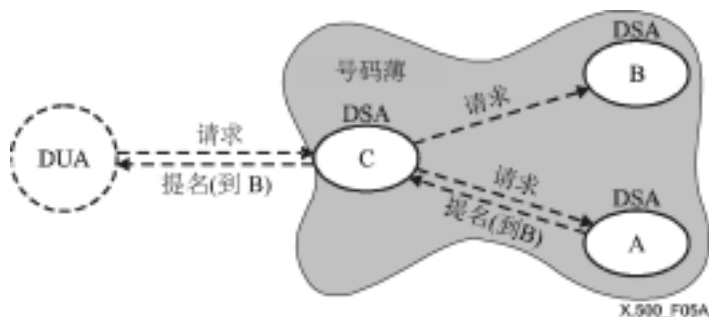


图 5a—提名

注 1 — 如果 DSA C 将提名返回给 DUA，则“提名（到 B）”将存在。同样，如果 DSA C 将请求转发到 DSA B，它将不会给 DUA 返回提名。

图 5b 中，DSA C 从 DSA A 获得了一个提名，它将负责或者将请求转发到 DSA B（在 DSA A 给出的提名中的 DSA 名称），或者将提名返回给发起请求的 LDAP 客户机。

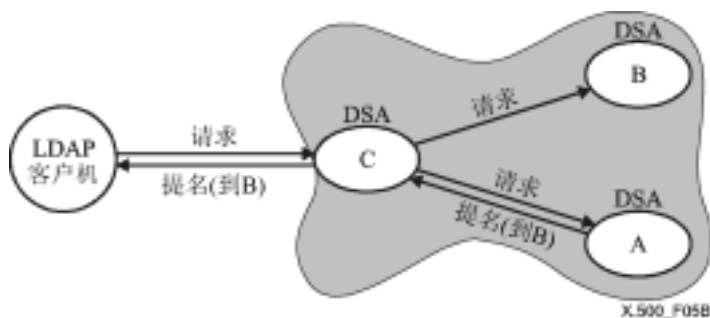


图 5b—提名

注 2 — 图 5b 中的 DSA C，除了可能要支持 X.500 中定义的其他协议外，还应当是一个 LDAP 响应者。

注 3 — 如果 DSA C 将提名返回给 LDAP 客户机，则“提名（到 B）”将存在。同样，如果 DSA C 将请求转发到 DSA B，它将不会给 LDAP 客户机返回提名。

注 4 — 如果 DSA C 将提名返回给 LDAP 客户机，提名应当以 LDAP 提名的形式存在。如果 DSA A 返回的提名是 LDAP 提名的形式，则 DSA C 可直接将该提名返回给 LDAP 客户机；否则，DSA C 应当或者将请求转发给 DSA B，或者将提名翻译为 LDAP 提名的形式。如果 DSA C 将提名返回给 LDAP 客户机，则客户机将直接与 DSA B 绑定，因此 DSA B 也应当是一个 LDAP 响应者。当 DSA A 返回一个 LDAP 提名，且 DSA C 将请求直接转发给 DSA B 时，DSA B 作为一个 LDAP 响应者也是必要的。

在图 5c 中，DUA 从 DSA C 中获得了一个提名，它将负责重新将请求直接发给 DSA A（在 DSA C 给出的提名中的 DSA 名称）。

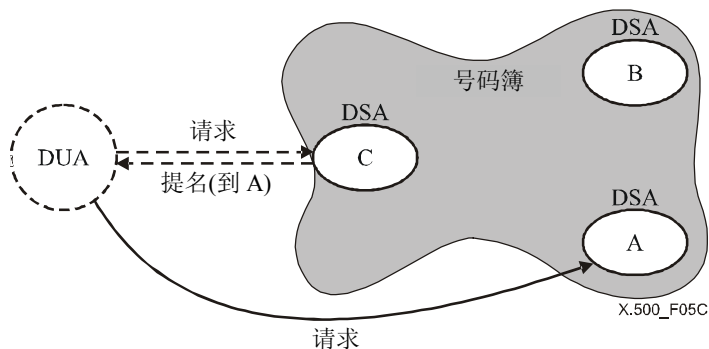


图 5c—提名

在图 5d 中，LDAP 客户机从 DSA C 中获得了一个提名，它将负责重新将请求直接发给 DSA A（在 DSA C 给出的提名中的 DSA 名称）。

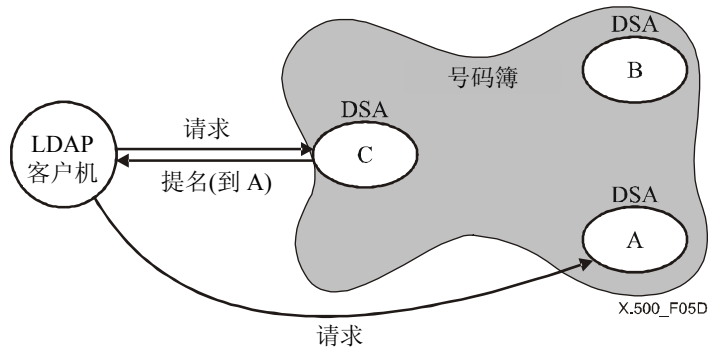


图 5d—提名

注 5 — 图 5d 中的 DSA A 和 DSA C 都应当是 LDAP 响应者。替代方案是这两个 DSA 中的任何一个可以是 LDAP 服务器。

注 6 — 返回给 LDAP 客户机的提名必须是 LDAP 提名的形式。

图 6a 到 6c 示出 DSA 的单一链接方式，这种方式下，在返回响应之前，请求能够通过多个 DSA。

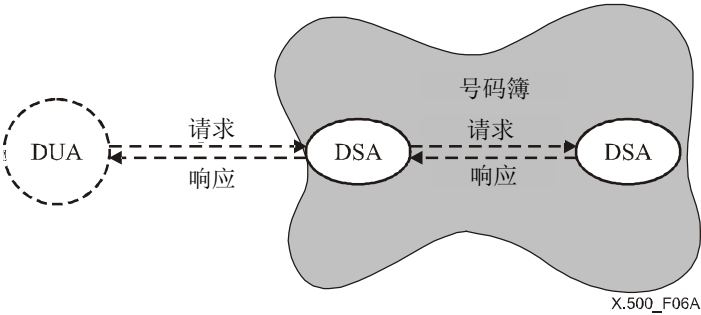


图 6a—单一链接

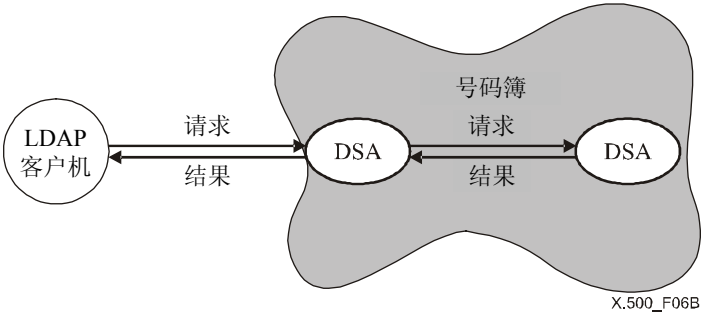


图 6b—单一链接

注 7 — 图 6b 左侧的 DSA，除了可能要支持 X.500 建议书的其他任何协议外，还必须是一个 LDAP 响应者。

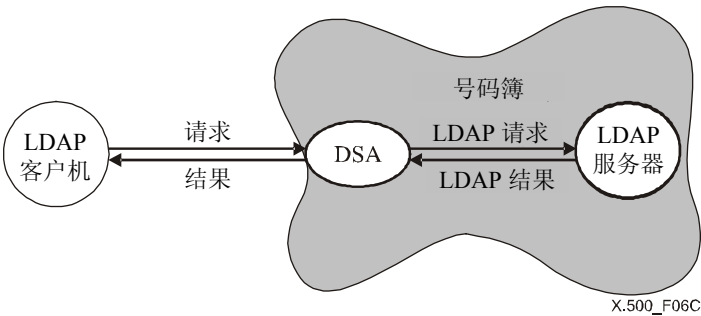


图 6c—单一链接

注 8 — 图 6c 中的 DSA，除了可能要支持 X.500 建议书的其他任何协议外，还必须既是一个 LDAP 响应者，又是一个 LDAP 请求者。

图 7a 到 7c 显示了多链接方式。在这种方式下，DSA 联合 DUA 和 LDAP 客户机将请求发送到两个或多个其他 DSA 和/或 LDAP 服务器上，发送到每个 DSA 或 LDAP 服务器上的请求是相同的。

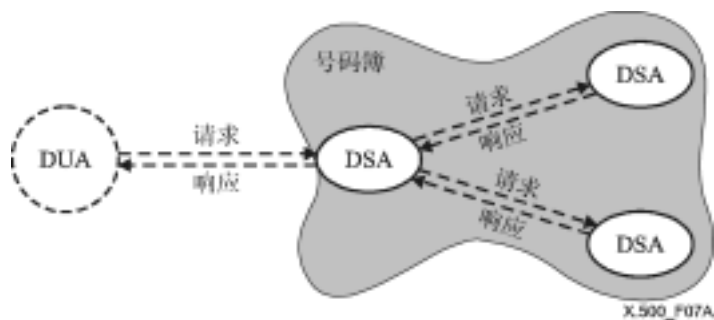


图 7a—多链接

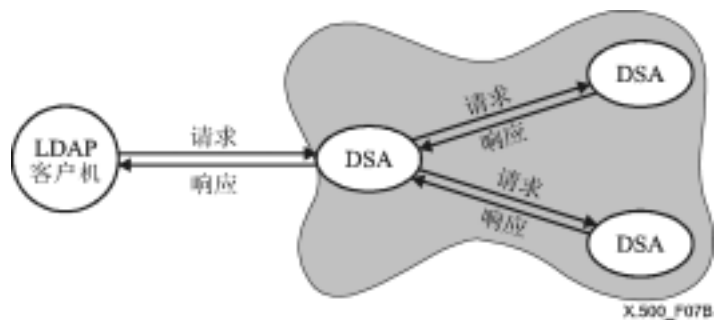


图 7b—多链接

注 9 — 图 7b 左侧的 DSA，除了可能要支持 X.500 建议书中的其他任何协议外，还必须是一个 LDAP 响应者。

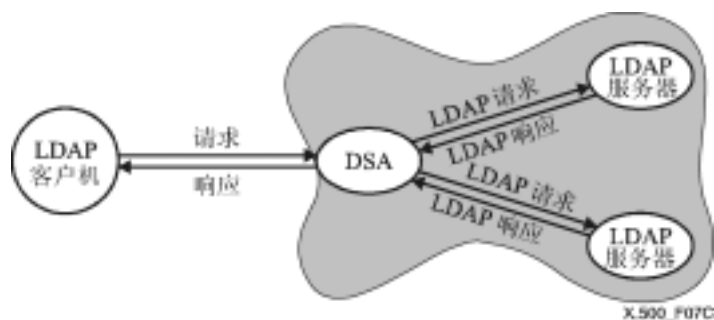


图 7c—多链接

注 10 — 图 7c 左侧的 DSA，除了可能要支持 X.500 建议书中的其他任何协议外，还必须既是一个 LDAP 响应者，又是一个 LDAP 请求者。

所有的方法都有其价值。例如，当希望降低本地 DSA 的负荷时，可能会采用图 5b 和 5d 中的方法。在其他环境下，可能会使用一种结合了多种功能交互集合的混合方法来满足发起者的请求，如图 8a 和 8b 显示的那样。

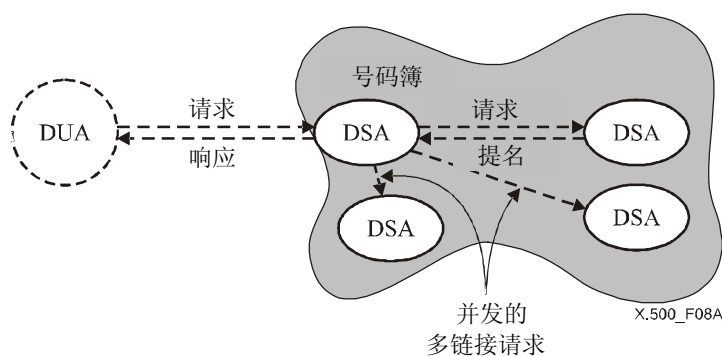


图 8a—混合模式混合途径

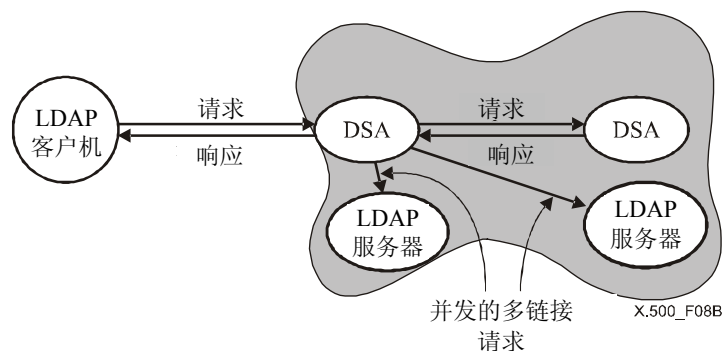


图 8b—混合模式混合途径

10 号码簿的访问控制

注一 号码簿访问控制模型在 ITU-T X.501 建议书 | ISO/IEC 9594-2 中定义。

对号码簿信息的访问由一些管理控制的安全策略来决定。对号码簿的访问有影响的两个安全策略的方面是认证过程和访问控制方案。

支持号码簿的认证过程和机制包括验证和传播身份的方法，在必要时，可使用这些方法对 DSA、号码簿用户、访问点所接收信息的发起者等的身份进行验证和传播。通用的认证过程在 ITU-T X.509 建议书 | ISO/IEC 9594-8 中定义。

支持号码簿的访问控制方案的定义包括这样一些方法：指定访问控制信息、执行该访问控制信息所定义的访问权限以及维护访问控制信息等。访问权限的执行指的是对 DIT 结构相关的号码簿信息、号码簿用户信息以及包括访问控制信息在内的号码簿操作信息等的访问做出控制。

ITU-T X.501 建议书 | ISO/IEC 9594-2 定义了一个特定的访问控制方案（或者潜在为多个），它被认为是号码簿的“基本访问控制”。主管当局在实现其安全策略时，可以使用该方案的全部或部分内容，或者可以根据他们的判断力自由地定义他们自己的方案。基本访问控制方案提供了一种方法来控制对 DIB 中的号码簿信息（潜在地，包括结构信息和访问控制信息）的访问。对信息的访问控制保护了信息不被非授权地检测、泄漏，或对信息进行修改等。

对信息的访问控制可用来防止非授权的检测、泄漏或对信息的修改等。ITU-T X.501 建议书 | ISO/IEC 9594-2 为号码簿定义了 3 种特定的访问控制方案，它们被称为“基本的访问控制”、“简化的访问控制”和“基于规则的访问控制”。主管当局在实现其安全策略时，可能会使用全部或部分方案，或者可能根据他们的决定自由地定义他们自己的方案。基本的访问控制方案提供了一种途径来控制对 DIB 中的号码簿信息（潜在地，包括结构信息和访问控制的信息）的访问。简化的访问控制方案提供的功能是基本访问控制方案的一个子集。基于规则的访问控制方案，提供了一些基于许可和标签的附加途径来控制对 DIB 内号码簿信息（潜在地，包括结构信息和访问控制信息）的访问。基于规则的访问控制方案能够与简化的或基本的访问控制方案共同使用，或者独自使用。

号码簿的基本访问控制模型为每个操作都定义了一个或多个点，在这些点上可能会执行访问控制决定。每个访问控制决定包括：

- 在号码簿中正在被访问的组件，可能是一个完整的复合条目；
- 发起操作请求的用户；
- 组成操作完整部分的必要的特定权限；以及
- 控制对该条目访问的安全策略。

号码簿的基于规则的访问控制模型为每个操作都定义了一个或多个点，在这些点上可能会执行访问控制决定。每个访问控制决定包括：

- 与用户访问请求相关的一个许可；
- 与被访问的信息相关的安全标签；
- 控制该访问的安全策略规则，这些规则定义了根据给定的许可和安全标签之间的关系，访问是否应当被拒绝。

11 服务管理

ITU-T X.501 建议书 | ISO/IEC 9594-2 中定义的号码簿抽象服务，向用户提供了浏览和阅读号码簿信息的有效的方法。

这些系列号码簿规范提供了广泛的服务管理能力，允许主管当局能够管理和限制向用户提供的业务。主管当局需要限制和调整提供给用户的业务，可能有如下一些原因：

- 主管当局知道它所拥有的信息的质量。为了提高号码簿搜索成功的速度，并且确保只返回高质量的信息，主管当局应能够限制在一个搜索过滤器中允许出现的属性类型，以及什么样的信息可以返回等。
- 为了保护在检测和清除信息方面的投资，主管当局可能会根据采用信息的用户类型，以及所提供的特定类型的服务等，对可返回的信息执行非常严格的限制。
- 一个主管当局可能会想要保护信息不被非法使用，例如为了大规模的市场目的，提取某个特定街道上的所有人员信息，或者提取某个特定职业的所有人员信息等。
- 比使用访问控制还要更大可能地保护个人数据。这种情况包括返回假的邮政地址，不允许在搜索时使用非常短的字符串，不允许在搜索时使用某些属性的组合，或者不允许搜索某些组合，等等。
- 对于所提供的服务使用什么样的限制以及如何进行适应等，取决于服务的用户群。

12 号码簿复制

注 — 号码簿复制在 ITU-T X.525 建议书 | ISO/IEC 9594-9 中定义。

12.1 介绍

号码簿的复制指的是除了对信息创建和修改负有责任的 DSA 外，在其他 DSA 内也存在对号码簿条目信息和操作信息的拷贝。包含原始信息的 DSA 被称为主 DSA。

在构建号码簿系统时可以定义其不使用复制的信息。

号码簿信息的复制服务是为了满足两类通用需求，一类与号码簿所提供的服务质量相关，另一类与号码簿系统的管理相关。

对号码簿条目信息部署额外的拷贝，可用于提高号码簿所提供的服务质量，体现在以下方面：

- a) 通过将号码簿信息移到与特定的号码簿用户“更近的”地点，来提高号码簿系统的性能；
- b) 通过引入冗余的号码簿信息和号码簿组件，使得一个单独组件的失效不会影响到对 DIT 中同一部分信息的所有访问，这样可以提高号码簿服务的可用性。

对号码簿条目信息部署额外的拷贝，可用于对号码簿信息的管理，体现在以下方面：

- a) 方便某些操作信息（如知识）的分布；以及
- b) 可通过拷贝号码簿的某个组件中拥有的信息来重建另一个组件中的信息，这样就为从严重的系统故障中进行恢复提供了一种机会。

12.2 号码簿复制的形式

号码簿组件所拥有的复制的条目信息有 3 种形式：高速缓冲拷贝、镜像信息和多主实现。

高速缓冲拷贝是号码簿的一个组件获取的条目信息的拷贝，其使用方法不在本系列号码簿规范中定义。

镜像拷贝是号码簿的一个组件获取的号码簿信息的拷贝，其使用方法在 ITU-T X.525 建议书 | ISO/IEC 9594-9 中定义。

多主实现是在一个给定的号码簿条目集中，为每一个条目都维护了多于一个的可写实例。每一个可写的号码簿条目的拷贝是完整的（即它拥有所有的用户属性和 DSA 共享的操作属性）。其中，有且仅有一个实例可被定义为允许号码簿将其标识为最基本的主实例，以便支持一种场景的部署，在这种场景中，有必要执行对单一 DSA 的修改（例如当增大某个用做计数器的属性值时）。号码簿组件获取某个条目的可写拷贝的方式以及在修改后这些可写拷贝如何保持一致性的方式，不在本建议书|国际标准的范围之内。

只有在信息最初提供时所达成的策略或合约中允许时，DSA 才可能会保持从其他 DSA 中获取到的信息。一个保持了这些信息的 DSA 只有在与信息的访问控制策略相符合的情况下，才可能会将这些信息提供给 DUA 和/或 LDAP 客户机。如果已知对某信息没有阅读方面的访问控制，则在信息提供时可认为是允许阅读的。

一个拥有高速缓冲信息或镜像信息的 DSA，会将所有可能修改拷贝信息的请求传送到拥有该信息的主 DSA。一个拥有拷贝信息的 DSA 会将所有指示了不能使用该拷贝信息的请求传送到拥有该信息的主 DSA。

在使用高速缓冲信息或镜像拷贝信息响应查询请求时，拥有该信息的 DSA 会指示此拷贝信息曾经用来满足过此请求。

分别负责两个 DSA 的主管当局间可能会建立一个镜像合约，根据合约，一个镜像提供者 DSA 将向另一个镜像使用者 DSA 提供约定的 DIT 中某部分的镜像信息。如果在镜像信息获取的镜像合约中允许的话，镜像使用者本身还可以作为一个镜像提供者，与其他 DSA 之间再建立信息镜像合约。

除了对镜像使用者所拥有的条目信息的拷贝提供修改外，镜像提供者也可能会提供一些操作信息（如知识）给镜像使用者。

在任何镜像合约中，典型的要被复制的信息包括下面 3 个元素：

- 从 DIT 的一棵子树中复制的条目信息；
- 要对复制信息提供完全的阅读访问，需要一些相关的操作信息，包括访问控制信息；
- 一些从属的知识信息（可选项）。

复制信息可能会组成子树内完整信息的一个子集，在该子集内：

- 可通过仅仅指定对象类的某些条件来选择条目；

- 在每个条目内，可根据属性的详细说明来选择属性；
- 在每个属性内，可基于属性值的上下文来选择属性值。

12.3 号码簿信息的复制和一致性

当一个特定属性的所有拷贝都相同时，则称号码簿具有一致性。有时，一致性可能是需要妥协的，因为在号码簿内，镜像信息可能会存在临时的不一致性，而高速缓冲信息可能会存在永久的一致不一致性。

高速缓冲的条目信息可能与号码簿中直接对信息进行修改的组件所存储的信息是不一致的，并且这种不一致可能是不确定的。与之相反，镜像使用者所拥有的镜像信息，可以根据镜像合约中已约定好的时间表与镜像提供者所拥有的相应信息达成一致。

基本的要素是包含在一个单独对象条目实例中的信息在内部应当是一致的。任何复制机制都应当与维护复制信息内部一致性以及服务可靠性的机制共同实现。号码簿定义了模式过程来确保一个条目信息的内部一致性。

另外一个基本的要素是允许 DIT 在 DSA 间分布的知识信息应当是正确的。任何复制机制都应当与维护知识信息正确性以及服务可靠性的机制共同实现。号码簿定义了如何使用 DSA 所需的最少的知识信息的过程来确保每个 DIT 视图的一致。

在号码簿信息被复制的环境下，号码簿对获得一致性没有特别的时间限制。镜像信息的使用者应当高度信任其一致性，因为：

- 镜像信息在内部是一致的；
- 将镜像信息与 DIT 视图相关联起来的知识是正确的；以及
- 被镜像的条目最终将变得与主 DSA 中的条目一致起来。

12.4 复制视点

本小节描述了一些不同的方法，利用这些方法，当前存在的号码簿复制信息将提供给如下方面：

- a) 号码簿用户；
- b) 主管部门用户；以及
- c) 号码簿（DSA）的操作组件。

12.4.1 号码簿用户视点

由于号码簿操作的自然特性，一般来说，复制的信息将与主 DSA 中所拥有的信息保持一致。因此，在一般情况下，返回给最终用户的信息拥有可接受的自然特性，而该信息是否是一个拷贝并不重要。

应当总是通知号码簿用户条目的拷贝信息是否能够满足用户的请求。在用户有特别严格的需求或者用户能够检测到不一致性时，用户可以选择请求访问主 DSA 所拥有的信息。

因此，可向号码簿的用户提供两种选择，一种是性能和可用性提高，代价是偶然会收到过时的信息；另一种是具有最大程度的信息时效性，但代价是性能和可用性会潜在地降低。

12.4.2 主管部门用户视点

主管部门用户负责对 DSA 所拥有的信息和所提供的服务进行管理。为了执行这种管理功能，主管部门用户需要相应的工具来进行监视、控制并对 DSA 的服务进行优化等。

DSA 支持复制的标准能力（本地能力）是主管部门用户可用的一种主要工具，用来优化 DSA 提供的服务。

12.4.3 DSA视点

尽管 DSA 能够检测出复制信息与主 DSA 所拥有的信息的不同，但一般来说，它用同样的方法来使用这两种信息，即它选择使用两种信息中的哪种信息来满足用户的查询请求，取决于哪个信息最为方便使用。

在这种主信息与复制信息的同等性上，有两个例外：DSA 将仅使用条目信息来满足修改 DIB 的请求；当查询请求明确表示复制信息不可接受时，将仅使用条目信息来满足查询请求。

另外，由于可能知道本地所拥有的信息是部分的（见第 12.2 节），因此一个 DSA 可将请求转到另一个能更好提供所需信息的 DSA 上。

注 — 一个 DSA 可能包含从多个源获得的复制信息，这些复制信息之间可能会存在交叉。在这种情况下，DSA 必须分别维护每个信息，如同复制时提供的一样。

12.5 复制和访问控制

访问控制模型允许对 DIT 的一个域定义访问控制信息。这个域可能会跨越 DSA 的边界。如果一个域包含了多个 DSA，则每个 DSA 都将拥有相应的访问控制信息。

任何时候，当条目被复制给其他 DSA 时，访问控制信息也必须被复制。

13 号码簿协议

注 — 允许处于不同开放系统中的 DUA 和 DSA 间协作的号码簿协议在 ITU-T X.519 建议书 | ISO/IEC 9594-5 中定义。

有 4 种号码簿协议：

- 号码簿访问协议（DAP），该协议定义了一个 DUA 与一个 DSA 间对请求和结果的交互；
- 号码簿系统协议（DSP），该协议定义了两个 DSA 间对请求和结果的交互；
- 号码簿信息镜像协议（DISP），该协议定义了两个建立了镜像合约的 DSA 间对复制信息的交互；
- 号码簿操作绑定管理协议（DOP），该协议定义了两个 DSA 间为管理它们之间的操作绑定而对管理信息的交互。

每个协议都被定义为一个协议元素集。例如，DAP 包括与查询和修改号码簿相关的协议元素。

14 号码簿系统管理

注 — 号码簿系统管理在 ITU-T X.530 建议书 | ISO/IEC 9594-10 中定义。

14.1 介绍

号码簿管理的目的是确保所需的、正确的号码簿信息能够在预定的期望的响应时间内提供给用户，并具有完整性、安全性和某种程度的一致性。此外，系统管理的实现还应当对平台和通信系统带来最小的处理时间负荷和内存负荷。

号码簿的管理可分为如下 4 个主要部分：

- a) 对 DIT 域的管理：管理号码簿信息；
- b) 对单个 DSA 操作的管理；
- c) 对单个 DUA 的管理；以及
- d) 对 DMD 的管理 — 号码簿功能组件的集中管理。

系统管理规范定义了前 3 部分。号码簿管理域（DMD）的管理有待进一步研究。

14.2 DIT域的管理

号码簿中的用户属性由号码簿访问协议（DAP）进行管理。操作属性也可能由 DAP 进行管理。这些属性包括信息框架中的属性、子模式（subschema）属性、访问控制属性以及 DSA 信息树中的属性、知识等。知识的管理还可能使用号码簿操作绑定管理协议（DOP）、号码簿信息镜像协议（DISP）以及号码簿系统协议（DSP）等。

14.3 号码簿组件的管理

系统管理规范定义了号码簿域内用于管理号码簿组件（DUA 和 DSA）的 OSI 系统管理的被管对象。对这些号码簿组件的管理可使用公共管理信息服务和协议来实现。

一些号码簿或管理服务没有实现的管理需求，可以通过本地定义的服务来实现。

附 件 A

号码簿的应用

(本附件是本建议书|国际标准的组成部分)

A.1 号码簿环境

注 — 本节中提到的术语“网络”指的是它的通用含义，即表示与任何电信业务相关的一系列相连的系统和进程，而不仅仅是指与 OSI 网络层相关的系统和进程。

号码簿所处的环境（并且在这种环境下提供服务）如下：

- a) 许多电信网络规模都很大，并且在不断地发生着变化，如：
 - 1) 各种类型的对象会在没有任何通告的情况下进入或离开网络，而且可能是单独的，也可能是成组地进入或离开；
 - 2) 由于对象（尤其是网络节点）之间的路径被增加或删除，因此它们之间的连接性会发生变化；
 - 3) 对象的各种特性，如它们的地址、可用性、物理位置等，在任何时间都可能发生变化。
- b) 尽管发生变化的整体频率比较高，但任何一个特定对象的有用的生命周期并不短。一个对象被典型地包含在通信中的频率将远高于它变化的频率，如地址、可用性、物理位置的变化等。
- c) 当前通信服务中所包含的对象，典型地被表示为数量类型或其他符号的字符串类型，这些类型的选择是从便于定位和处理的角度出发，而不是从便于人使用的角度出发的。

A.2 号码簿服务特性

对号码簿能力的要求在增长，体现在：

- a) 要求尽可能将网络用户从频繁改变的网络中分离出来。这可通过在用户和他们所处理的对象之间放置一个“间接级别”来实现，包括用户在引用对象时通过名字来引用，而不是通过地址来引用等。号码簿提供必要的映射服务。
- b) 要求提供一个更“用户友好的”网络视图，例如使用别名、指配黄页（见 A.3.5）等，可以在查找和使用网络信息时帮助减轻负担。

号码簿允许用户获取关于网络的各种各样的信息，并且提供对信息的维护、分布和安全性。

A.3 号码簿的使用方式

注 — 本节仅关注号码簿查询，假设号码簿修改服务仅仅是应用程序在必要时用来维护 DIB 的。

A.3.1 介绍

在系列号码簿规范中，对号码簿服务是这样定义的：DUA 能够发出的特定请求以及请求中的参数。但对于一个应用设计者来说，当考虑到该应用对号码簿信息查询的需求时，希望能有一种更加面向目标的术语。本节相应地描述了一些号码簿服务的高层使用方式，这些号码簿服务可能与许多应用是相关的。

A.3.2 查找

直接的号码簿查找包括提供了对象的识别名以及一个属性类型的 DUA。号码簿将返回与该属性类型相应的任何值。这是传统的号码簿功能的一般化定义，当所要求的属性类型与某个特定的地址类型相符合时将获得信息。各种类型地址的属性类型已被标准化，包括 OSI-PSAP 地址、消息处理 O/R 地址以及电话和电报号码等。

查找由阅读服务支持，该服务还提供如下更进一步的一般化服务：

- 查找可基于对象的识别名之外的对象名字，如别名等。

- 在一个请求内，可以请求多个属性类型的值，极端的情况是一个条目内的所有属性值都被返回。
- 可基于上下文（如某个组织名称的法语值）请求一个属性的某个特定的值。

A.3.3 用户友好的命名

给对象赋予的名字最好是能够让人类能够预知到（或可能记住）的名字。具有这种特性的名字一般来说可以由对象本身所特有的、内在的属性来组成，而不是专门为了起名而虚构一个。对象的名字在所有引用该对象的应用中是相同的。

A.3.4 浏览

在许多面向人的号码簿使用中，对用户（或 DUA）来说，直接提供包含要查询信息的对象名称有时是不可能的，而不管名字是用户友好的还是不友好的。然而，有可能是这种情况，即用户“如果看到它就知道是它”。这时，就需要浏览能力来允许用户在 DIB 中浏览查找合适的条目。

浏览应用可以通过联合列表和查询服务，同时也可能联合阅读服务（尽管搜索业务已经包含了阅读能力）来完成。

A.3.5 黄页

有多种途径可以提供黄页类型的能力。最简单的一种是基于过滤的，即使用关于某些特定属性的断言，这些属性的值是有分类的（如 ITU-T X. 520 建议书 | ISO/IEC 9594-6 中定义的“商务类别”属性类型）。这种方法除了要确保存在一些必要的属性外，不会要求在 DIT 中建立任何特别的信息。然而，在一般情况下，当人数众多时，这种搜索可能是昂贵的，因为过滤可能要求对全集进行过滤。

一个可能替代的方法是建立一棵特定的子树，这棵子树的命名结构是特别为黄页类型的搜索而设计的。图 A.1 中示出一个黄页子树的例子，这棵子树仅具有别名条目。在具体实现时，黄页子树中的条目可能是混合了对象和别名条目的条目，只要对每个存储在号码簿中的对象而言仅存在一个对象条目即可。

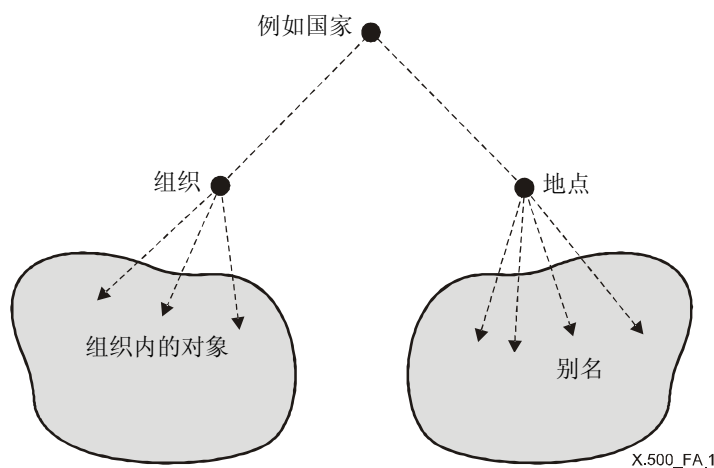


图 A.1—一种黄页的方法

A.3.6 搜索限制和放宽

在许多搜索请求中，信息搜索的最初尝试结果将返回太少或者太多的信息。号码簿包括了这样一些指配功能，可以允许将搜索“放宽”以便获得更多的成功机会（如自动执行语音匹配的第二轮搜索，而不是严格的字符串匹配），或者将搜索“收紧”以便减少“命中”的数量。号码簿还允许使用本地的、更适合的匹配规则来替代可能会应用的标准的匹配规则。

例如，利用地理信息来匹配某地点和所存储地点的匹配规则，可能会替代一个字符串匹配规则来使用。这两种方法也可以组合使用。如果一个严格的地理匹配不会产生任何结果（如匹配“Warfield”和

“Bracknell”可能会失败，没有任何结果），则基于一个放宽的地理匹配可能会成功（如匹配“Warfield”与“Bracknell”时，将其放宽为包含 Bracknell 以及周围相邻的村庄，包括 Warfield，则匹配就会成功）。

放宽还可用于扩展黄页搜索的能力，即使用更通用的类别来替代特定的类别。例如，“餐馆”作为一个字符串不能与“中国餐馆”相匹配，但是可通过匹配规则的替换或放宽来达到匹配目的。

A.3.7 分组

分组是这样一个集合，该集合内的成员可通过显式地增加和删除而发生变化。分组是一个对象，它的成员也都是对象。能够请求号码簿提供如下功能：

- 指示一个特定的对象是否为一个分组内的成员；
- 列出一个分组内的所有成员。

对分组的支持可以通过在条目中包含一个具有多个值的“成员”属性（这样的属性类型在 ITU-T X.520 建议书|ISO/IEC 9594-6 中定义）来实现。上述提到的两个功能可以分别通过对该属性的比较和阅读功能来实现。

如果对应用程序来说是有意义的，则分组内的成员本身还可以是一个分组。然而，除了所提供的非递归版本外，DUA 还必须创建一个必要的递归证明和扩展服务。

A.3.8 认证

许多应用程序要求对象在被允许执行某些动作之前，还需要提供一些证明来验证它们的身份。号码簿提供了对该认证过程的支持（作为一个分离的事务，号码簿本身也会要求对它的用户进行认证，以便支持访问控制）。

一种被称为“简单认证”的更直接的认证方式，是基于这样一种情况 — 号码簿在条目中为每个希望认证自己的用户拥有一个“用户口令”属性。在服务请求中，号码簿将证实或否认用户所提供的特定值是用户真正的口令。这就避免了用户为每一个服务都需要一个不同的口令。在使用简单认证的本地环境中，对口令进行交互被认为是不适当的，在这种情况下，号码簿可以可选地提供方法来保护这些口令不被某个单向功能重放或错误地使用。

一种被称为“强认证”的更复杂的认证方式，是基于公钥密码系统的。在这种方式中，号码簿存储了用户的公共密钥，并防止被篡改。用户从号码簿中获取彼此的公共密钥并使用密钥来相互认证的步骤，在 ITU-T X.509 建议书 | ISO/IEC 9594-8 中详细描述。

A.3.9 基于属性的定位

许多应用程序都要求能够快速检测到拥有特定属性值的条目是否存在；如果检测到有这样的条目存在，则要求快速查找并返回这些条目。在一个包含单个 DSA 的号码簿中，这种能力是直接的。然而，在一个分布式的号码簿中，基于属性的查询可能会有问题，主要问题在于对查询执行时间的上限很难控制。

对上述需求的一个相对简单的解决方法可以应用在 DSA 集已知且被合作管理的环境下。为了支持对某个特定属性的快速搜索，一个单独的 DSA（或者特定的 DSA 集合）能够被配置为拥有一个过滤后的包含这些感兴趣的属性在内的复制域。这样搜索操作可被限定在一个单独的 DSA 上，该 DSA 将快速提供“有”或“没有”的答案，如果条目存在，还将提供该条目的主 DSA 的相关知识。复制在 ITU-T X.525 建议书 | ISO/IEC 9594-9 中详细讨论。

A.4 通用应用

A.4.1 介绍

有许多通用的应用可被假设为是号码簿隐含支持的，这些应用不是专门应用于某一个特定的电信服务的。这里描述了两个这样的应用：个人间通信号码簿和系统间通信号码簿（OSI）。

注 — 在 A.3.8 中描述的作为一种访问方式的认证，也可以被认为是一种通用的号码簿应用。

A.4.2 个人间通信

本应用的目的是为个人或其代理提供如何与其他人员或分组内人员进行通信的信息。

本应用包含下述对象类：个人、组织角色和分组。其他类（如国家、组织、组织单元等）也可能被包含，但可能不是直接包含。

除了那些用在命名中的属性类型外，这里涉及的属性类型主要是地址类属性。典型地，某个特定个人的条目中将拥有与每种通信方式相适应的地址，通过这些地址可访问到该人员，其中至少应包括电话、电子邮件、电报、ISDN、物理投递（如邮政系统）、传真等的号码（地址）。在某些情况下，如电子邮件地址，条目中还应当具有一些附加的信息，如用户设备可以处理的信息类型等。如果支持认证，则需要用户口令和/或证书。

用于各种对象类的命名方案应当是用户友好的，适当时候还可建立别名以提供一个替代名称，在名字改变后别名不变以保持连贯性等。

本应用中可出现下述访问模式：查找、用户友好命名、浏览、黄页和分组。为了使级别多样化，也可以使用认证。

A.4.3 系统间通信（为OSI定义）

根据 OSI 参考模型，在 OSI 中要求有两个号码簿功能，一个在应用层，将应用实体名映射到表示层地址；另一个在网络层，将 NSAP 地址映射到 SNPA 地址（SNPA：子网附着点）。

注一 本小节中后续部分，仅描述应用层功能。

该功能的执行是通过向号码簿确认，为完成此映射功能所需的信息通过其他方法是否是不方便获得的。

该服务的用户是应用实体，所感兴趣的对象类或子类也是应用实体。

除了那些用在命名中的属性类型外，这里涉及到的属性类型主要是表示层地址。其他对本号码簿功能来说不是必需的属性类型，能够支持验证或查找应用实体类型，或者所支持的应用上下文列表、抽象语法列表等。认证相关的属性类型也可能是相关的。

附 件 B

修正案和勘误

(本附件不是本建议书|国际标准的组成部分)

本号码簿规范的这一版本包括如下对前一版本的修正案草案内容，该草案经 ISO/IEC 投票批准：

— X.500 和 LDAP 间最大一致化的修正案 3。

本号码簿规范的这一版本不包括任何技术上的勘误，因为没有收到关于本号码簿规范前一版本的错误报告。

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	视听和多媒体系统
I系列	综合业务数字网
J系列	有线网和电视、声音节目和其他多媒体信号的传输
K系列	干扰的防护
L系列	线缆的构成、安装和保护及外部设备的其他组件
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	测量设备技术规程
P系列	电话传输质量、电话装置和本地线路网络
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	数据网和开放系统通信及安全
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
Z系列	用于电信系统的语言和一般软件问题