ICS 35.100.70
L 79

中华人民共和国国家标准

GB/T 16264.3—2008/ISO/IEC 9594-3:2005
代替 GB/T 16264.3—1996

信息技术　开放系统互连　目录　第3部分:抽象服务定义

Information technology—Open Systems Interconnection—The Directory—Part 3:Abstract service definition

(ISO/IEC 9594-3:2005 Information technology—Open Systems Interconnection—The Directory:Abstract service definition,IDT)

2008-08-06 发布　　2009-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

中华人民共和国
国家标准
信息技术 开放系统互连 目录
第3部分:抽象服务定义
GB/T 16264.3—2008/ISO/IEC 9594-3:2005
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 7 字数 204千字
2008年12月第一版 2008年12月第一次印刷
*
书号:155066·1-34753 定价 64.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68533533

GB/T 16264.3-2008

前　言

GB/T 16264《信息技术　开放系统互连　目录》包括以下10个部分：

——第1部分：概念、模型和服务的概述；

——第2部分：模型；

——第3部分：抽象服务定义；

——第4部分：分布式操作规程；

——第5部分：协议规范；

——第6部分：选定的属性类型；

——第7部分：选定的客体类；

——第8部分：公钥和属性证书框架；

——第9部分：复制(待发布)；

——第10部分：公用目录管理机构的系统管理用法(待发布)。

本部分是GB/T 16264的第3部分。

本部分等同采用ISO/IEC 9594-3:2005《信息技术　开放系统互连　目录　抽象服务定义》，仅有编辑性修改。

本部分代替GB/T 16264.3—1996。

本部分与GB/T 16264.3—1996的差异在于：

——增加13章搜索变元的分析；

——扩展了各章节的功能。

本部分的附录A是规范性附录，附录B和附录C是资料性附录。

本部分由中华人民共和国信息产业部提出。

本部分由全国信息技术标准化技术委员会归口。

本部分起草单位：中国电子技术标准化研究所。

本部分主要起草人：徐冬梅、冯惠、张翠、宋戚阳、胡顺。

本部分于1996年首次发布，本次为第一次修订。

引　言

GB/T 16264 的本部分连同本标准其他部分是为方便信息处理系统之间的互连以提供目录服务而制定的。所有这些系统的集合，连同它们所拥有的目录信息可被视为一个整体，被称为“目录”。目录所拥有的信息，总称为目录信息库(DIB)，典型地被用于方便客体之间的通信、与客体的通信或有关客体的通信等，这些客体如应用实体、个人、终端和分布列表等。

目录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。

本部分定义了目录为其用户提供的能力。

本部分提供了一些基础框架，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。在这些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。ISO/IEC 9594 的第 5 版是原有国际标准第 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符合第 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差错)。建议在系统实现时尽快符合第 5 版。

第 5 版详细定义了目录协议的第 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，如署名差错，只有包含在操作中的所有的目录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 GB/T 16264.5—2008 中定义的扩展规则调节。

本部分使用术语“第 1 版系统”来指遵循国际标准第 1 版的所有系统，即 ISO/IEC 9594:1990 版本；本部分使用术语“第 2 版系统”来指遵循国际标准第 2 版本的所有系统，即 ISO/IEC 9594:1995 版本；本部分使用术语“第 3 版系统”来指遵循国际标准第 3 版的所有系统，即 ISO/IEC 9594:1998 版本；本部分使用术语“第 4 版系统”来指遵循国际标准第 4 版的所有系统，即 ISO/IEC 9594:2001 版本的第 1 部分到第 10 部分；本部分使用术语“第 5 版系统”来指遵循国际标准第 5 版的所有系统，即 ISO/IEC 9594:2005 版本。

GB/T 16264—1996 是参照 ISO/IEC 9594:1990 而制定的。我国没有制定与国际标准第 2 版、第 3 版、第 4 版对应的国家标准。本部分提到的版本号是指国际标准的版本号。

附录 A 是规范性附录，提供了目录抽象服务的 ASN.1 模块。

附录 B 是资料性附录，提供了用于描述与基本访问控制相关的语义的图表，它适用于目录操作的处理。

附录 C 是资料性附录，给出了条目族使用的例子。

目　次

试读结束，需要全本PDF请购买 www.ertongbook.com

信息技术　开放系统互连　目录
第3部分:抽象服务定义

1　范围

GB/T 16264的本部分按抽象方法定义了目录所提供的外部可视服务。

本部分不规定具体实现或产品。

2　规范性引用文件

下列文件中的条款通过GB/T 16264的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 9387.1—1998　信息技术　开放系统互连　基本参考模型　第1部分:基本模型(idt ISO/IEC 7498-1:1994)

GB/T 16262.1—2006　信息技术　抽象语法记法一(ASN.1)　第1部分:基本记法规范(ISO/IEC 8824-1:2002,IDT)

GB/T 16262.2—2006　信息技术　抽象语法记法一(ASN.1)　第2部分:信息客体规范(ISO/IEC 8824-2:2002,IDT)

GB/T 16262.3—2006　信息技术　抽象语法记法一(ASN.1)　第3部分:约束规范(ISO/IEC 8824-3:2002,IDT)

GB/T 16262.4—2006　信息技术　抽象语法记法一(ASN.1)　第4部分:ASN.1规范的参数化(ISO/IEC 8824-4:2002,IDT)

GB/T 16264.1—2008　信息技术　开放系统互连　目录　第1部分:概念、模型和服务的概述(ISO/IEC 9594-1:2005,IDT)

GB/T 16264.2—2008　信息技术　开放系统互连　目录　第2部分:模型(ISO/IEC 9594-2:2005,IDT)

GB/T 16264.4—2008　信息技术　开放系统互连　目录　第4部分:分布式操作规程(ISO/IEC 9594-4:2005,IDT)

GB/T 16264.5—2008　信息技术　开放系统互连　目录　第5部分:协议规范(ISO/IEC 9594-5:2005,IDT)

GB/T 16264.6—2008　信息技术　开放系统互连　目录　第6部分:选定的属性类型(ISO/IEC 9594-6:2005,IDT)

GB/T 16264.7—2008　信息技术　开放系统互连　目录　第7部分:选定的客体类(ISO/IEC 9594-7:2005,IDT)

ISO/IEC 9594-8:2005　信息技术　开放系统互连　目录:公钥和属性证书框架

ISO/IEC 9594-9:2005　信息技术　开放系统互连　目录:复制

ISO/IEC 9594-10:2005　信息技术　开放系统互连　目录:公用目录管理机构的系统管理用法

3　术语和定义

下列术语和定义适用于GB/T 16264的本部分。

3.1 基本目录定义

下列术语在 GB/T 16264.1—2008 中规定：

a) 目录 directory；

b) 目录信息库 directory information base；

c) (目录)用户 (directory) user。

3.2 目录模型定义

下列术语在 GB/T 16264.2—2008 中规定：

a) 目录系统代理 directory system agent；

b) 目录用户代理 directory user agent。

3.3 目录信息库定义

下列术语在 GB/T 16264.2—2008 中规定：

a) 别名条目 alias entry；

b) 目录信息树 directory information tree；

c) (目录)条目 (directory) entry；

d) 直接上级 immediate superior；

e) 直接上级条目/客体 immediately superior entry/object；

f) 客体 object；

g) 客体类 object class；

h) 客体条目 object entry；

i) 下级 subordinate；

j) 上级 superior；

k) 祖(条目) ancestor；

l) (条目的)家族 family(of entries)；

m) 复合条目 compound entry。

3.4 目录条目定义

下列术语在 GB/T 16264.2—2008 中规定：

a) 属性 attribute；

b) 属性类型 attribute type；

c) 属性值 attribute value；

d) 属性值断言 attribute value assertion；

e) 上下文 context；

f) 上下文类型 context type；

g) 上下文值 context value；

h) 操作属性 operational attribute；

i) 用户属性 user attribute；

j) 匹配规则 matching rule。

3.5 名(称)定义

以下术语在 GB/T 16264.2—2008 中规定：

a) 别名 alias,alias name；

b) 可辨别名 distinguished name；

c) (目录)名(称) (directory) name；

d) 声称名 purported name；

e) 相关可辨别名 relative distinguished name。

3.6 分布式操作定义

以下术语在 GB/T 16264.4—2008 中规定：

a) 绑定 DSA bound DSA；

b) 链接 chaining；

c) 初始执行者 initial performer；

d) 转向推荐 referral。

3.7 抽象服务定义

下列术语和定义适用于本部分。

3.7.1

附加搜索 additional search

指的是从 joinBaseObject 开始的一次搜索，由始发者在 search 请求中规定。

3.7.2

贡献成员 contributing member

复合条目中的一个家族成员，它或者对阅读、搜索或者对修改条目操作做出贡献。

3.7.3

明确未标记的条目 explicitly unmarked entry

依据管理搜索规则引用的控制属性中规定的规范，未包括在 SearchResult 中的一个条目或家族成员。

3.7.4

家族组合 family grouping

出于操作评估目的，将复合属性的成员组合在一起。

3.7.5

过滤器 filter

有关条目的某些属性存在与否或属性值的断言，以便限制搜索范围。

3.7.6

始发者 originator

始发操作的用户。

3.7.7

参与成员 participation member

一个家族成员，或者是一个贡献成员，或是一个家族组合成员，作为整体匹配一个 search 过滤器。

3.7.8

主搜索 primary search

从 baseObject 开始的搜索，按照始发者在 search 请求中规定。

3.7.9

张弛 relaxation

如果接收的太少，为获取更多地匹配条目；或者如果接收的太多，为得到较少的匹配条目，在搜索期间对过滤器行为所做的渐进修改。

3.7.10

服务控制 service controls

作为操作一部分传递的参数，用于约束其性能的不同方面。

3.7.11

束 strand

包括从叶子家族成员一直到祖(条目)路径上的全部成员的家族组合。家族成员将驻于各束中，束

的数量为其下叶家族成员的数量(直接或非直接下级)。

3.7.12

流结果 streamed result

包括在多个响应中的单个操作结果。

4 缩略语

下列缩略语适用于 GB/T 16264 的本部分。

AVA	属性值断言	(Attribute Value Assertion)
DIB	目录信息库	(Directory Information Base)
DIT	目录信息树	(Directory Information Tree)
DMD	目录管理域	(Directory Management Domain)
DSA	目录系统代理	(Directory System Agent)
DUA	目录用户代理	(Directory User Agent)
RDN	相关可辨别名	(Relative Distinguished Name)

5 约定

术语"目录规范(或本目录规范)"指的是 GB/T 16264.3。术语"系列目录规范"指的是GB/T 16264(或者 ISO/IEC 9594)的所有部分。

本目录规范使用术语"第 1 版系统"来指遵循系列目录规范第 1 版的所有系统,即 GB/T 16264—1996 版本。本目录规范使用术语"第 2 版系统"来指遵循系列目录规范第 2 版本的所有系统,即 ISO/IEC 9594:1995 版本。本目录规范使用术语"第 3 版系统"来指遵循系列目录规范第 3 版的所有系统,即 ISO/IEC 9594:1998 版本。本目录规范使用术语"第 4 版系统"来指遵循系列目录规范第 4 版的所有系统,即 ISO/IEC 9594:2001 年版本的第 1 部分到第 10 部分。

本目录规范使用术语"第 5 版系统"来指遵循系列目录规范第 5 版的所有系统,即 GB/T 16264—2008 版本的第 1 部分到第 7 部分以及 ISO/IEC 9594-8:2005、ISO/IEC 9594-9:2005 和 ISO/IEC 9594-10:2005。

本目录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 目录服务概述

如 GB/T 16264.2—2008 中所描述,通过 DUA 的访问点提供目录服务,每个访问动作代表一个用户。这些概念如图 1 描述。通过访问点,利用若干目录操作,目录为其用户提供服务。

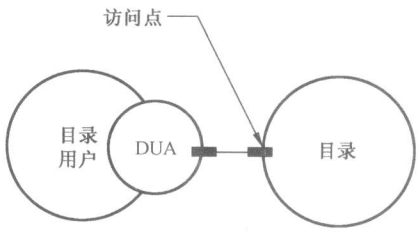

图 1 访问目录

有三种不同类型的目录操作:

a) 目录读操作,它查询单个目录条目;

b) 目录搜索操作,它查询若干潜在的目录条目;以及

c) 目录修改操作。

目录读操作、目录搜索操作和目录修改操作分别在第9章、第10章和第11章中规定。目录操作的一致性在GB/T 16264.5—2008中规定。

7 信息类型和公共规程

7.1 引言

本章标识(在某些情况下定义)后面的目录操作定义中使用的若干信息类型,这里所涉及的信息类型是那些用于多种操作,或在将来用于多种操作的通用信息类型;或者使用这些信息类型定义更复杂的或自包含的信息类型。

目录服务定义中使用的若干信息类型确实在其他地方进行了定义。7.2标识了这些类型,并指示了其定义的来源。7.3至7.10分别标识并定义了一种信息类型。

本章还规定了应用于多数或全部目录操作的若干公共规程元素。

7.2 在其他标准中定义的信息类型

以下信息类型在GB/T 16264.2—2008中规定:

a) Attribute;
b) AttributeType;
c) AttributeValue;
d) AttributeValueAssertion;
e) Context;
f) ContextAssertion;
g) DistinguishedName;
h) Name;
i) OPTIONALLY-PROTECTED;
j) OPTIONALLY-PROTECTED-SEQ;
k) RelativeDistinguishedName。

以下信息类型在GB/T 16264.6—2008中规定:

a) PresentationAddress。

以下信息类型在ISO/IEC 9594-8:2005中规定:

a) Certificate;
b) SIGNED;
c) CertificationPath。

以下信息类型在GB/T 16975.1中规定:

a) InvokeId。

以下信息类型在GB/T 16264.4—2008中规定:

a) OperationProgress;
b) ContinuationReference。

7.3 公共变元

CommonArguments信息可限定目录执行的每个操作的调用。

```
CommonArguments ::= SET {
        serviceControls         [30]    ServiceControls DEFAULT { },
        securityParameters      [29]    SecurityParameters OPTIONAL,
        requestor               [28]    DistinguishedName OPTIONAL,
        operationProgress       [27]    OperationProgress
```

```
                                DEFAULT { nameResolutionPhase notStarted },
    aliasedRDNs             [26]    INTEGER OPTIONAL,
    criticalExtensions      [25]    BIT STRING OPTIONAL,
    referenceType           [24]    ReferenceType OPTIONAL,
    entryOnly               [23]    BOOLEAN DEFAULT TRUE,
    nameResolveOnMaster     [21]    BOOLEAN DEFAULT FALSE,
    operationContexts       [20]    ContextSelection OPTIONAL,
    familyGrouping          [19]    FamilyGrouping DEFAULT entryOnly }
```

ServiceControls 组件在 7.5 中规定，不存在时表示控制为空集。

SecurityParameters 组件在 7.10 中规定。如果操作变元被请求方签名，那么SecurityParameters 组件应包括在变元中。SecurityParameters 组件缺省时表示为空集。

requestor 可辨别名标识某个抽象操作的始发者，它包含用户与目录建立绑定时使用的用户名。当要对请求签名(见 7.10)时，可以要求这个组件，并且包含发起请求的用户名。

注 1：当用户拥有一个由上下文区分的、可选的可辨别名时，用作requestor 值的名(称)应是所知的主可辨别名。否则，基于requestor 值的鉴别和访问控制可能无法按要求工作。

OperationProgress、referenceType、entryOnly、exclusions 和 nameResolveOnMaster 组件在 GB/T 16264.4—2008 中定义。它们在以下情况下由 DUA 提供：

a) 当按照 DSA 响应先前操作而返回的继续引用进行动作，并且其值由 DUA 从继续引用中复制；或

b) 当 DUA 代表管理 DSA 信息树的管理用户，并且manageDSAIT 选项在服务控制中设置。

aliasedRDNs 组件指示一个 DSA，在先前的操作中，其操作的客体组件通过别名解除引用进行创建，整数值指示客体中 RDN 的数量，它来自没有引用的别名(该值应在以前操作的转向推荐响应中设置)。

注 2：提供本组件是为了与目录第 1 版实现的兼容性。根据目录规范之后版本实现的 DUA(和 DSA)将总是从后续请求的CommonArguments 中省略该参数。这样，如果别名解除引用至进一步别名，目录将不发出差错信号。

operationContexts 组件提供了一组上下文断言，该组上下文断言适用与本操作生成的属性值断言和条目信息选择，否则对于相同的属性类型和上下文类型不包含上下文断言。如果operationContexts 不出现，或不描述某个特定的属性类型或上下文类型，那么 DSA 将使用缺省的上下文断言，如 GB/T 16264.2—2008 的 7.6.1、8.9.2.2 和 12.8 所述。如果选择了allContexts，那么所有属性类型的所有上下文都将是有效的，DSA 提供的各上下文缺省值都将被超越(ContextSelection 在 7.6 中定义)。

对于给定的操作处理，familyGrouping 用于描述应选择哪个家族成员，在 7.3.2 中对它有更为详细的描述。

7.3.1 临界扩展

criticalExtensions 组件提供了一种机制，以列出一组对目录抽象操作的执行来说是临界的扩展。如果扩展操作的始发者希望指示该操作必须和一个或多个扩展一起执行(即没有这些扩展的操作是不能接受的)这种执行是通过设置与该扩展相对应的criticalExtensions 位而进行的。如果目录和目录的某部分不能执行一个临界扩展，它返回一个unavailableCriticalExtension 指示(作为一个serviceError 或一个PartialOutcomeQualifier)。如果该目录不能报告一个非临界的扩展，则它忽略扩展的存在。

本目录规范不建立有关执行 DSA 对其所接收的 PDU 进行解码和处理的次序的规则。收到一个未知临界扩展的 DSA 将返回一个带问题unavailableCriticalExtension 的ServiceError，以发出信号通知操作失败。

目录规范定义了若干扩展。各扩展采用以下形式，即 BIT STRING(比特束)中的额外编号位，或

试读结束，需要全本PDF请购买 www.ertongbook.com

者集合(SET)或序列(SEQUENCE)中的额外组件,第1版本系统忽视了这一点。每一种扩展被分配了一个可在criticalExtensions中设置成比特数的整数标识符。如果扩展的重要性设为临界,那么DUA将在criticalExtensions中设置相应的位。如果扩展的重要性设为非临界,那么DUA在criticalExtensions中可以或不可以设置相应的位。

扩展、扩展标识符、许可扩展的操作、推荐的临界性、定义扩展的章、相应的LDAP 控制(如果有的话),均示于如表1。

表1 扩展

扩　展	标识符	操　作	临界性	定义(条号)	LDAP控制
subentries	1	所有	非临界	7.5	1.3.6.1.4.1.4203.1.10.1
copyShallDo	2	读、比较、列表、搜索	非临界	7.5	
attribute size limit	3	读、搜索	非临界	7.5	
extraAttributes	4	读、搜索	非临界	7.6	
modifyRightsRequest	5	读	非临界	9.1	
pagedResultsRequest	6	列表、搜索	非临界	10.1	1.2.840.113556.1.4.319
matchedValuesOnly	7	搜索	非临界	10.2	1.2.826.0.1.3344810.2.3
extendedFilter	8	搜索	非临界	10.2	
targetSystem	9	增加条目	临界	11.1	
useAliasOnUpdate	10	增加条目、移除条目、修改条目	临界	11.1	
newSuperior	11	修改DN	临界	11.4	
manageDSAIT	12	所有	临界	7.5、7.13	2.16.840.1.113730.3.4.2
useContexts	13	读、比较、列表、搜索、增加条目、修改条目、修改DN	非临界	7.6、7.8	
partialNameResolution	14	读、搜索	非临界	7.5	
overspecFilter	15	搜索	非临界	10.1.3 f)	
selectionOnModify	16	修改条目	非临界	11.3.2	
安全参数—Response	17	所有	非临界	7.10	
安全参数—Operation code	18	所有	非临界	7.10	
安全参数—Attribute certification path	19	所有	非临界	7.10	
安全参数—Error Protection	20	所有	非临界	7.10	
SPKM Credentials	21	目录绑定	(注3)	8.1.1	
Bind token- Response	22	目录绑定	非临界	8.1.1	

表 1（续）

扩　展	标识符	操　作	临界性	定义（条号）	LDAP 控制
Bind token-Bind Int. Alg, Bind Int Key, Conf Alg and Conf Key Info	23	目录绑定	非临界	8.1.1	
Bind token-DIRQOP（obsolete）	24	目录绑定	非临界	8.1.1	
Service administration	25	读、搜索、修改条目	临界	10.2.2、第 13 章、GB/T 16264.2 第 16 章	
entryCount	26	搜索	非临界	10.1.3	
hierarchySelection	27	搜索	非临界	7.5	
relaxation	28	搜索	非临界	7.8	
familyGrouping	29	比较、搜索、移除条目	非临界 非临界 临界	7.3.2、7.8.3、9.2.2、10.2、11.2.2	
familyReturn	30	读、搜索、修改条目	非临界 非临界 非临界	7.6.4、7.7.1、9.1.3、10.2.3、11.3.3	
dnAttributes	31	搜索	非临界	10.2.2	
friend attributes	32	读、搜索	非临界	7.6、7.8.2	
Abandon of paged results	33	列表、搜索	临界	7.9	
Paged results on the DSP	34	列表、搜索	非临界	7.9	
replaceValues	35	修改条目	临界	11.3.1、11.3.2	

注 1：为首个扩展提供了标识符 1，对应 BIT STRING 的位 1。BIT STRING 的第 0 位没有使用。

注 2：对增加条目、移除条目、修改条目、修改 DN 使用加密的或签名的和加密安全转换或者对任何差错或结果使用保护，要求第 2 版或更高版本的协议。

注 3：SPKM 证书扩展至关重要，除非用在利用第 2 版或更高版本建立的关联中。

7.3.2　家族组合

家族组合允许将复合条目的单个家族成员、若干个家族成员或所有的家族成员结合在一起，以便在操作评估之前做综合考虑。这些语义可以用于以下操作（如下列描述所述）：比较（定义比较属性可能处于的范围）、搜索（定义可能进行过滤的组）、移除条目（定义移除组）。下列 ASN.1 用于选择家族成员。

```
FamilyGrouping ::= ENUMERATED {
        entryOnly               (1),
        compoundEntry           (2),
```

```
    strands                 (3),
    multiStrand             (4) }
```

entryOnly 含义是将在组中对操作选择的特定家族成员进行考虑。这是缺省值，确保向后兼容于目录规范的先前版本。

compoundEntry 含义是将把操作选择的、完整的复合条目看作是一个结合了所有属性的单元。对移除条目操作，只有当规定的客体名(称)是复合条目祖(条目)的客体名(称)时才适用，这将造成全部家族成员被相同操作移除(依据访问控制)。

strands 含义是操作将选择所有与家族成员关联的束。该选项对移除条目操作无效。对搜索操作，认为单个束是用于过滤器目的。如果一个或多个束的复合属性集匹配与过滤器匹配，那么认为复合条目与过滤器匹配。如果基本客体是一个孩子成员，那么只考虑那些通过基本客体的束。对比较操作，条目所属的所有束中所有家族成员的所有属性将会在比较中用到。

multiStrand 只适用于搜索操作，对家族信息限定过滤器的匹配规则。其他操作被忽略。它规定每次只考虑来自复合条目中每个组的一个束，但所有结合在一起考虑。如果基本客体是一个孩子家族成员，那么multiStrand 不适用，在这种情况下，multiStrand 将被忽略，entryOnly 将被替换。

7.4 公共结果

CommonResults 或CommonResultsSeq 信息用于限定目录能执行的各检索操作的结果。另外，它出现在任何返回的差错中。

```
CommonResults ::=SET {
    securityParameters      [30]  SecurityParameters                    OPTIONAL,
    performer               [29]  DistinguishedName                     OPTIONAL,
    aliasDereferenced       [28]  BOOLEAN                               DEFAULT FALSE,
    notification            [27]  SEQUENCE SIZE (1..MAX) OF Attribute   OPTIONAL }
    CommonResultsSeq ::=SEQUENCE {
    securityParameters      [30]  SecurityParameters                    OPTIONAL,
    performer               [29]  DistinguishedName                     OPTIONAL,
    aliasDereferenced       [28]  BOOLEAN                               DEFAULT FALSE,
    notification            [27]  SEQUENCE SIZE (1..MAX) OF Attribute   OPTIONAL }
```

注：CommonResults 和CommonResultsSeq 由相同的组件组成。当被COMPONENT 类型包含在集合类型中时，使用前者，而后者类似地用在序列类型中。

SecurityParameters 组件在 7.10 中规定。如果目录对结果进行签名，那么SecurityParameters 组件将包括在结果中。SecurityParameters 组件不出现将被认为相当于一个空集。

performer 可辨别名用于确定某个特定操作的执行者。当对结果进行签名时可能需要它(见 7.10)，并将持有签名结果的 DSA 的名(称)。

当作为操作目标的客体或基本客体的假设名(称)包括任何已解除引用的别名时，aliasDereferenced 组件将被设为TRUE。

notification 组件将用于限定返回结果和差错 APDU，例如用于提供更加精确的差错信息。标准通告属性在 GB/T 16264.6—2008 的 5.12 中定义。此类通告属性不必储存在目录条目中。

7.5 服务控制

ServiceControls 参数包含指导或限制提供服务的控制信息。

```
ServiceControls ::=SET {
    options                 [0] ServiceControlOptions DEFAULT { },
    priority                [1] INTEGER { low (0),medium (1),high (2) } DEFAULT medium,
    timeLimit               [2] INTEGER OPTIONAL,
```

```
    sizeLimit                [3] INTEGER OPTIONAL,
    scopeOfReferral          [4] INTEGER { dmd(0),country(1) } OPTIONAL,
    attributeSizeLimit       [5] INTEGER OPTIONAL,
    manageDSAITPlaneRef      [6] SEQUENCE {
        dsaName Name,
        agreementID AgreementID } OPTIONAL,
    serviceType              [7] OBJECT IDENTIFIER OPTIONAL,
    userClass                [8] INTEGER OPTIONAL }
ServiceControlOptions ::=BIT STRING {
        preferChaining          (0),
        chainingProhibited      (1),
        localScope              (2),
        dontUseCopy             (3),
        dontDereferenceAliases  (4),
        subentries              (5),
        copyShallDo             (6),
        partialNameResolution   (7),
        manageDSAIT             (8),
        noSubtypeMatch          (9),
        noSubtypeSelection      (10),
        countFamily             (11),
        dontSelectFriends       (12),
        dontMatchFriends        (13),
        allowWriteableCopy      (14) }
```

options 组件包含若干指示，若设置，则每个指示断言所建议的条件。因此：

a) preferChaining 指示优先选择是链接而不是转向推荐提供服务，不强迫目录依从该优先选择。

b) chainingProhibited 指示禁止链接以及其他有关目录的请求分发方法。

c) localScope 指示操作限于本地范围。该选项的定义本身是一个本地问题，例如，在一个单个 DSA 或一个单个 DMD 内。

d) dontUseCopy 指示拷贝的信息(如 GB/T 16264.4—2008 中定义)不会用于提供服务。

e) dontDereferenceAliases 指示不解除引用任何用于标识受操作影响的条目的别名。

注 1：允许引用别名条目本身而不是使用别名的条目，例如为了读别名条目。

f) subentries 指示搜索或列表操作仅用于访问子条目；常规条目变得不可访问，即目录行为如同常规条目不存在。如果不设置该服务控制，那么操作只访问常规条目，子条目变得不可访问。对搜索或列表之外的各操作忽略服务控制。

注 2：即使子条目是不可访问的，仍观察对访问控制、模式和联合属性的子条目影响。

注 3：如果设定该服务控制，那么可以继续将常规条目规定为操作的基本客体。

g) copyShallDo 指示如果目录能够部分地而不是全部地满足对条目拷贝的查询要求，那么它将不链接查询。只有当不设置dontUseCopy 时它才有意义。如果不设置copyShallDo，那么只有当它完整得足以允许操作彻底满足拷贝要求时，目录才使用影像数据。由于在影像拷贝中丢失某些请求的属性，一个查询可能只能部分地满足要求，由于 DSA 不持有它没有的属性值的所有上下文信息，或者由于持有影像数据的 DSA 不支持有关该数据的请求匹配规则，在影像拷贝中会丢失给定属性的某些属性值。如果设置了copyShallDo，并且目录无法彻底满足一个

查询的要求，那么它将在返回的条目信息中设置incompleteEntry。

h) partialNameResolution 指示如果目录只能解析读或搜索操作中的部分声称名，即它将返回一个nameError，那么名(称)包括所有已解析 RDN 的条目将被认为是操作的目标，并且在结果中将partialName 设为TRUE。对读或搜索之外的各操作忽略该服务控制。

注 4：如果设定该服务控制，那么声称名将是一个上下文前缀条目，拒绝对其进行访问，请求方需要访问上级条目，而后将存在上下文前缀条目这一情况间接地泄露给请求方，即使拒绝条目的*DiscloseOnError* 许可。

i) manageDSAIT 指示管理用户已请求操作，因此对 DSA 信息树进行管理。如果在 DSA 有多个复制平面需要管理，并且manageDSAITPlaneRef 服务控制未包括在操作中，那么 DSA 为操作选择一个合适的复制平面。

j) noSubtypeMatch 指示不会尝试进行属性子类型匹配。除了比较和搜索操作，对其他操作将忽略该服务控制。

k) noSubtypeSelection 指示不进行子类型选择。

l) countFamily 指示将把复合条目的每个成员当作一个单独的条目，例如出于大小和管理限制以及张弛控制目的。如果未设置该控制，那么将把复合属性的成员当作一个单个条目。

m) dontSelectFriends 指示条目信息选择中锚属性的规定不自动包括选择中的友人属性。

n) dontMatchFriends 指示过滤器项中锚属性的规定只能满足锚属性值的要求，不能满足友人属性的要求。

o) allowWriteableCopy 指示，在提供查询服务请求中，类型writeableCopy 的 DSE 是可接受的。

注 5：allowWriteableCopy 服务控制不同于copyShallDo，该服务控制用于指示需要一个完整的拷贝，但它不必来自主源，而copyShallDo 用于指示任何拷贝，不论是完整的还是不完整的，都可接受。

如果忽略该组件，那么假设以下内容：对链接没有优选权，但不禁止链接；对操作范围没有限制；许可使用拷贝；将解除引用别名(除非对修改操作，对它不支持别名解除引用)；子条目不可访问；对不能完全满足影像数据要求的操作需做进一步链接。不过，对这些缺省，在服务特定管理区域内可以通过搜索规则进行重写。

以priority (low、medium 或high)优先级提供服务。注意，在目录中这不是一个保证的服务，整体上不进行排队。在低层上使用优先级并不隐含任何关系。

timeLimit 指示服务提供中的最大耗费时间，以秒计。如果约束无法满足，那么报告一个差错。如果忽略该组件，那么不暗指任何时间限制。当在列表或搜索中时间限制超出时，结果是任选一个积累的结果。

注 6：该组件不显示流逝时间中的请求处理时间长度：在处理流逝时间中的请求时可能涉及任何数量的 DSA。

sizeLimit 仅适用于列表和搜索操作。它指示当不返回分页结果时的最大返回条目数。在超出了大小限制的情况下，列表或搜索操作的结果可以是任选一个积累的结果，数量上等于大小限制。将抛弃任何更多的结果。当返回分页结果时，执行分页的 DSA 将忽略 sizeLimit 的值，详见 7.9。

scopeOfReferral 指示 DSA 返回之转向推荐将关联的范围。依据选择的值是dmd 还是country，将只返回选定范围内的其他 DSA 转向推荐。这适用于referral 差错以及list 和search 结果unexplored 参数中的转向推荐。

attributeSizeLimit 指示任何属性的最大大小(即类型及其所有值)，它包括在返回的条目信息中。如果一个属性超出了该限制，那么从返回的条目信息中删去其所有值，并在返回的条目信息中设置incompleteEntry。采用的属性大小为其在持有数据的本地具体语法中的大小，以八位字计。由于所用的不同数据保存方法，限制是不精确的。如果未规定该参数，那么不暗指任何限制。

注 7：作为条目可辨别名一部分返回的属性值不受该限制所限。

priority、timeLimit 和sizeLimit 的某些结合可能产生冲突。例如，短时间限制可能与低优先级产生

冲突;高大小限制可能与低时间限制产生冲突;等等。

manageDSAITPlaneRef 指示,管理用户已请求操作,因此对 DSA 信息树的某个特定复制平面进行管理。如果未设置manageDSAIT 选项,那么忽略manageDSAITPlaneRef 服务控制。平面由dsaName 组件(它是提供 DSA 的名(称))和agreementID 组件(它包含影像协议标识符)确定。

serviceType 服务控制只与search 请求相关,它在一个服务特定管理区域内开始其最初的评估阶段;否则将忽略之。如果提供,那么它增加获得有用通告信息的可能性,当差错表达search 请求时返回通告信息。

userClass 服务控制只与search 请求相关,它在一个服务特定管理区域内开始其最初的评估阶段;否则将忽略之。它确定一个用户类别。它允许请求方规定另一个用户类别,否则将应用目录。如果提供,那么它还会增加获得有用通告信息的可能性,当差错表达 search 请求时返回通告信息。

7.6 条目信息选择

EntryInformationSelection 参数用于指示在检索服务中条目所请求的哪些信息。

```
EntryInformationSelection ::= SET {
    attributes                  CHOICE {
      allUserAttributes             [0]     NULL,
      select                        [1]     SET OF AttributeType
      --empty set implies no attributes are requested--} DEFAULT allUserAttributes: NULL,
    infoTypes                   [2]     INTEGER {
      attributeTypesOnly                (0),
      attributeTypesAndValues           (1) } DEFAULT attributeTypesAndValues,
    extraAttributes                   CHOICE {
      allOperationalAttributes      [3] NULL,
      select                        [4] SET SIZE (1..MAX) OF AttributeType } OPTIONAL,
    contextSelection ContextSelection OPTIONAL,
    returnContexts BOOLEAN DEFAULT FALSE,
    familyReturn FamilyReturn DEFAULT
                                  { memberSelect contributingEntriesOnly } }
ContextSelection ::= CHOICE {
    allContexts                 NULL,
    selectedContexts            SET SIZE (1..MAX) OF TypeAndContextAssertion }
TypeAndContextAssertion ::= SEQUENCE {
    type                        AttributeType,
    contextAssertions           CHOICE {
        preference                      SEQUENCE OF ContextAssertion,
        all                             SET OF ContextAssertion } }
FamilyReturn ::= SEQUENCE {
    memberSelect   ENUMERATED {
        contributingEntriesOnly         (1),
        participatingEntriesOnly        (2),
        compoundEntry                   (3) },
    familySelect SEQUENCE SIZE (1..MAX) OF OBJECT-CLASS.&id OPTIONAL }
```

attributes 组件用于规定有关请求信息的用户和操作属性。

a) 如果选择select 选项,则列出所包含的属性;如果列表为空,则不返回属性;如果属性存在,则

试读结束,需要全本PDF请购买 www.ertongbook.com