

版权信息：本文档版权由 LDAPChina.com 所有，可随意传播、打印及用于任何用途，必须保留本文档的所有版权信息及版本信息，同时不可对本文档的任何部分进行任何修改。

版本信息

日期	版本	描述	作者
2004-04-08	v1.0	最初版本	LDAPChina.com

LDAPChina.com 保留随时对本文档的任何部分作出修改，而不事先通知使用者的权利。

A Summary of the X.500(96) User Schema for use with LDAPv3

LDAPv3 使用的 X.500(96)用户模式总结

1、本备忘录的状态（Status of this Memo）

本文档定义了一个用于 Internet 通讯的 Internet 标准跟踪协议，为了发展的需要讨论和建议。对于这个协议的状况和地位请参照 Internet 官方协议标准（"Internet Official Protocol Standards"（STD 1））的当前版。这个备忘录的传播是不受限制的。

版权提示（Copyright Notice）

版权 Internet 组织（The Internet Society (2000)）。所有权利保留。

IESG 提示（IESG Note）

本文档描述将一种同时提供读和更新访问的目录访问协议。更新访问需要安全认证，但这个文档并不强制实现任何安全认证机制。

与 RFC2026 的 4.4.1 节相同，本规范正在被 IESG 批准期间，作为被提议的标准，可能并不限于本文档所述内容。原因如下：

- a、鼓励在它们被发布前，实现和交互测试这些协议（带有或没有更新访问）；
- b、鼓励在只读的应用程序中配置和使用这些协议。（例如，在某些应用程序中，目录的更新访问使用某些其它安全的机制而不是 LDAP，而使用 LDAPv3 被作为对目录的查询语言）；
- c、避免阻碍别的 Internet 标准追踪协议的发展和发布。（这些协议需要 LDAPv3 的目录服务器的查询能力，而不是更新能力）

需要警告读者的是，直到强制的验证机制被标准化之前，根据本规范编写的客户端和服务端实现了更新功能的话，它们的互操作性可能是不可靠的，或者仅提供在认证需要极度弱化的时候的互操作性。

因此在具有强制认证的 LDAPv3 未成为一个 RFC 而被批准或发布之前，不鼓励实现者发布一个实现了更新功能的 LDAPv3 的客户端和服务端。

目 录

A Summary of the X.500(96) User Schema for use with LDAPv3 LDAPv3 使用的 X.500(96)用户模式总结.....	2
1、本备忘录的状态 (Status of this Memo)	2
版权提示 (Copyright Notice)	2
IESG 提示 (IESG Note)	2
2、摘要 (Abstract)	7
3、总论 (General Issues)	7
4、源 (Source)	7
5、属性类型 (Attribute Types)	8
5.1、对象类 (objectClass)	8
5.2、aliasedObjectName	8
5.3、knowledgeInformation	8
5.4、cn	8
5.5、sn	9
5.6、serialNumber	9
5.7、c	9
5.8、l	9
5.9、st	9
5.10、street	9
5.11、o	10
5.12、ou	10
5.13、title	10
5.14、description	10
5.15、searchGuide	10
5.16、businessCategory	10
5.17、postalAddress	11
5.18、postalCode	11
5.19、postOfficeBox	11
5.20、physicalDeliveryOfficeName	11
5.21、telephoneNumber	11
5.22、telexNumber	11
5.23、teletexTerminalIdentifier	12
5.24、facsimileTelephoneNumber	12
5.25、x121Address	12
5.26、internationaliSDNNumber	12
5.27、registeredAddress	12
5.28、destinationIndicator	12
5.29、preferredDeliveryMethod	13
5.30、presentationAddress	13
5.31、supportedApplicationContext	13
5.32、member	13
5.33、owner	13

5.34、roleOccupant	13
5.35、seeAlso	13
5.36、userPassword	14
5.37、userCertificate	14
5.38、cACertificate	14
5.39、authorityRevocationList	14
5.40、certificateRevocationList	14
5.41、crossCertificatePair	14
5.42、name	15
5.43、givenName	15
5.44、initials	15
5.45、generationQualifier	15
5.46、x500UniqueIdentifier	15
5.47、dnQualifier	16
5.48、enhancedSearchGuide	16
5.49、protocolInformation	16
5.50、distinguishedName	16
5.51、uniqueMember	16
5.52、houseIdentifier	17
5.53、supportedAlgorithms	17
5.54、deltaRevocationList	17
5.55、dmdName	17
6、语法 (Syntaxes)	17
6.1、传递方法 (Delivery Method)	17
6.2、增强指南 (Enhanced Guide)	18
6.3、指南 (Guide)	18
6.4、八进制字符串 (Octet String)	19
6.5、Teletex Terminal Identifier	19
6.6、Telex Number	19
6.7、Supported Algorithm	20
7、对象类 (Object Classes)	20
7.1、top	20
7.2、alias	20
7.3、country	20
7.4、locality	20
7.5、organization	20
7.6、organizationalUnit	21
7.7、person	21
7.8、organizationalPerson	21
7.9、organizationalRole	21
7.10、groupOfNames	22
7.11、residentialPerson	22
7.12、applicationProcess	22

7.13、applicationEntity	22
7.14、dSA.....	22
7.15、device	22
7.16、strongAuthenticationUser	23
7.17、certificationAuthority.....	23
7.18、groupOfUniqueNames	23
7.19、userSecurityInformation.....	23
7.20、certificationAuthority-V2.....	23
7.21、cRLDistributionPoint.....	23
7.22、dmd.....	23
8、匹配规则（Matching Rules）	24
8.1、octetStringMatch.....	24
9、安全考虑（Security Considerations）	24
10、感谢（Acknowledgements）	24
11、参考书目（References）	24
12、作者地址（Authors' Addresses）	25
13、完整的版权声明（Full Copyright Statement）	25

2、摘要（Abstract）

本文档提供了 ISO 和 ITU-T 委员会在 X.500 文档中定义的属性类型和对象类的一个回顾，特别是专门面向目录用户使用的。这是被 LDAP/X.500 目录最为广泛使用的 schema（模式），许多其它 schema 定义白皮书将它们作为基础。本文档不覆盖由 X.500 目录服务器的管理所使用的属性，也不包括在其它 ISO/ITU-T 文档中定义的属性。

本文档中的关键字"**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**"和"**MAY**"的含意与 RFC 2119（参考文档[6]）中描述的相同。

3、总论（General Issues）

本文档参照的语法在本文档的第 6 节和参考文档[1]的第 6 节中描述。本文档参照的匹配规则在本文档的第 8 节和参考文档[1]的第 8 节中描述。

属性类型和对象类的定义使用在参考文档[1]中描述的 AttributeTypeDescription 和 ObjectClassDescription 的 BNF 格式进行书写，并已被拆分成易于读取的行。

4、源（Source）

本文档的 schema 定义基于 X.500 的参考文档[2]，[3]，[4]，[5]中的 schema 定义，并更新为这个文档，对照如下：

Sections	Source
=====	=====
5.1 - 5.2	X.501(93)
5.3 - 5.36	X.520(88)
5.37 - 5.41	X.509(93)
5.42 - 5.52	X.520(93)
5.53 - 5.54	X.509(96)
5.55	X.520(96)
6.1	RFC 1274
6.2	(new syntax)
6.3 - 6.6	RFC 1274
7.1 - 7.2	X.501(93)
7.3 - 7.18	X.521(93)
7.19 - 7.21	X.509(96)
7.22	X.521(96)

某些属性的名称与它在 X.520(93)中定义的名称不同。

三个新的属性 supportedAlgorithms, deltaRevocationList 和 dmdName 以及对象类 dmd, 在 X.500(96)的文档中定义。

5、属性类型 (Attribute Types)

一个 LDAP 服务器实现应该 (SHOULD) 可以识别在本节描述的属性类型。

5.1、对象类 (objectClass)

objectClass 属性的值 (译者注: objectClass 属性可能有多个值) 描述了一个条目代表的对象的类型。每个条目都拥有 objectClass 属性, 并且至少有两个值。其中一个值或者为 "top" 或者为 "alias"。

(2.5.4.0 NAME 'objectClass' EQUALITY objectIdentifierMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.38)

5.2、aliasedObjectName

如果包含该属性的条目是一个别名 (alias) 条目, 则目录服务将使用 aliasedObjectName 属性。

(2.5.4.1 NAME 'aliasedObjectName' EQUALITY distinguishedNameMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE)

5.3、knowledgeInformation

该属性不再被使用

(2.5.4.2 NAME 'knowledgeInformation' EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 {32768})

5.4、cn

这是 X.500 的 commonName 属性, 它包含一个对象的名称。如果对象为一个人, 它就是该人的全名。

(2.5.4.3 NAME 'cn' SUP name)

5.5、sn

这是 X.500 的 surname 属性，它包含着一个人的姓。

(2.5.4.4 NAME 'sn' SUP name)

5.6、serialNumber

该属性包含一个设备的序列号。

(2.5.4.5 NAME 'serialNumber' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.44{64})

5.7、c

该属性包含双字符（two-letter）ISO 3166 国家代码（countryName）。

(2.5.4.6 NAME 'c' SUP name SINGLE-VALUE)

5.8、l

该属性包含地名，例如：一个城市、乡村或其它地理区域（localityName）。

(2.5.4.7 NAME 'l' SUP name)

5.9、st

该属性包含一个州或省的全名（stateOrProvinceName）

(2.5.4.8 NAME 'st' SUP name)

5.10、street

该属性包含这个条目关联的对象的物理地址（physical address），例如：送货的地址（streetAddress）。

(2.5.4.9 NAME 'street' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128})

5.11、o

该属性包含一个组织/机构的名称（organizationName）。

(2.5.4.10 NAME 'o' SUP name)

5.12、ou

该属性包含组织中一个部门的名称（organizationalUnitName）。

(2.5.4.11 NAME 'ou' SUP name)

5.13、title

该属性包含一个人在他的组织机构中的头衔，例如"Vice President"。"personalTitle"属性将被用于说明一个人独特的工作职能的头衔。

(2.5.4.12 NAME 'title' SUP name)

5.14、description

该属性包含对象的可读的（human-readable）描述。

(2.5.4.13 NAME 'description' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{1024})

5.15、searchGuide

该属性被 X.500 客户端在创建查询过滤器时使用。该属性已经被 enhancedSearchGuide 所取代，enhancedSearchGuide 将在 5.48 节描述。

(2.5.4.14 NAME 'searchGuide'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.25)

5.16、businessCategory

该属性描述某个组织所从事的商业业务类型。

(2.5.4.15 NAME 'businessCategory' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 {128})

5.17、postalAddress

(2.5.4.16 NAME 'postalAddress' EQUALITY caseIgnoreListMatch
SUBSTR caseIgnoreListSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.41)

5.18、postalCode

(2.5.4.17 NAME 'postalCode' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 {40})

5.19、postOfficeBox

(2.5.4.18 NAME 'postOfficeBox' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 {40})

5.20、physicalDeliveryOfficeName

(2.5.4.19 NAME 'physicalDeliveryOfficeName' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 {128})

5.21、telephoneNumber

(2.5.4.20 NAME 'telephoneNumber' EQUALITY telephoneNumberMatch
SUBSTR telephoneNumberSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.50 {32})

5.22、telexNumber

(2.5.4.21 NAME 'telexNumber'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.52)

5.23、teletexTerminalIdentifier

(2.5.4.22 NAME 'teletexTerminalIdentifier'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.51)

5.24、facsimileTelephoneNumber

(2.5.4.23 NAME 'facsimileTelephoneNumber'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.22)

5.25、x121Address

(2.5.4.24 NAME 'x121Address' EQUALITY numericStringMatch
SUBSTR numericStringSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.36{15})

5.26、internationaliSDNNumber

(2.5.4.25 NAME 'internationaliSDNNumber' EQUALITY numericStringMatch
SUBSTR numericStringSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.36{16})

5.27、registeredAddress

该属性拥有一个邮政地址，适用于电报或快递文档，它必须拥有可交付的接收者。

(2.5.4.26 NAME 'registeredAddress' SUP postalAddress
SYNTAX 1.3.6.1.4.1.1466.115.121.1.41)

5.28、destinationIndicator

该属性被有于电报服务。

(2.5.4.27 NAME 'destinationIndicator' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.44{128})

5.29、preferredDeliveryMethod

(2.5.4.28 NAME 'preferredDeliveryMethod'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.14
SINGLE-VALUE)

5.30、presentationAddress

该属性包含一个 OSI（Open System Interconnection：开放系统互连）表达地址。

(2.5.4.29 NAME 'presentationAddress'
EQUALITY presentationAddressMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.43
SINGLE-VALUE)

5.31、supportedApplicationContext

该属性包含 OSI 应用程序上下文的标识符。

(2.5.4.30 NAME 'supportedApplicationContext'
EQUALITY objectIdentifierMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.38)

5.32、member

(2.5.4.31 NAME 'member' SUP distinguishedName)

5.33、owner

(2.5.4.32 NAME 'owner' SUP distinguishedName)

5.34、roleOccupant

(2.5.4.33 NAME 'roleOccupant' SUP distinguishedName)

5.35、seeAlso

(2.5.4.34 NAME 'seeAlso' SUP distinguishedName)

5.36、userPassword

(2.5.4.35 NAME 'userPassword' EQUALITY octetStringMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40{128})

密码使用 8 进制字符串语法存储，并不进行加密。当底层的传输服务不能保证保密性和密码可能泄漏给未授权方的情况下，明文密码的传输强烈建议不要使用。

5.37、userCertificate

该属性以二进制格式被存储和请求，以'userCertificate;binary'方式。

(2.5.4.36 NAME 'userCertificate'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.8)

5.38、cACertificate

该属性以二进制格式被存储和请求，以'cACertificate;binary'方式。

(2.5.4.37 NAME 'cACertificate'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.8)

5.39、authorityRevocationList

该属性以二进制格式被存储和请求，以'authorityRevocationList;binary'方式。

(2.5.4.38 NAME 'authorityRevocationList'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.9)

5.40、certificateRevocationList

该属性以二进制格式被存储和请求，以'certificateRevocationList;binary'方式。

(2.5.4.39 NAME 'certificateRevocationList'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.9)

5.41、crossCertificatePair

该属性以二进制格式被存储和请求，以'crossCertificatePair;binary'方式。

(2.5.4.40 NAME 'crossCertificatePair'

SYNTAX 1.3.6.1.4.1.1466.115.121.1.10)

5.42、name

name 属性类型是所有用来进行命名的属性类型的超类型 (supertype)。一般这个类型的值不出现在一个条目里。不支持属性子类型 (subtyping) 的 LDAP 服务器不需要在请求里识别这个类型。客户端实现**绝不** (MUST NOT) 能假设 LDAP 服务器具有执行属性子类型化的能力。

(2.5.4.41 NAME 'name' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 {32768})

5.43、givenName

givenName 属性用于保存一个人的名字中既不是姓和又不是中间名字 (middle name) 的部分。

(2.5.4.42 NAME 'givenName' SUP name)

5.44、initials

initials 属性包含着一些或所有独立名称的起始部分，除了姓。

(2.5.4.43 NAME 'initials' SUP name)

5.45、generationQualifier

generationQualifier 属性包含着名称的后缀部分，例如"IIIrd" (译者注：指：什么什么 三世)。

(2.5.4.44 NAME 'generationQualifier' SUP name)

5.46、x500UniqueIdentifier

x500UniqueIdentifier 属性被用于当一个分辨名被重用时，在两个对象之间进行区分。这是一个与"uid"和"uniqueIdentifier"不同的属性性类。

(2.5.4.45 NAME 'x500UniqueIdentifier' EQUALITY bitStringMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.6)

5.47、dnQualifier

dnQualifier 属性指定了添加到一个条目的 rdn（相对分辨名）的无歧义信息。它专用于从多个源合并数据时防止条目之间可能发生的同名。建议来自于同一个源的条目具有相同的 dnQualifier 值。

(2.5.4.46 NAME 'dnQualifier' EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.44)

5.48、enhancedSearchGuide

该属性由 X.500 客户端使用，用于构造查询过滤器。

(2.5.4.47 NAME 'enhancedSearchGuide'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.21)

5.49、protocolInformation

该属性与 presentationAddress 属性一同使用，向 OSI 网络服务提供额外的信息。

(2.5.4.48 NAME 'protocolInformation'
EQUALITY protocolInformationMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.42)

5.50、distinguishedName

该属性类型不用于对象自己的名称，但它是一个基本属性类型，允许具有 DN 语法的属性继承它。

一般情况下这个类型的值自身不出现在一个条目。不支持属性类型子类型化(subtyping)的 LDAP 服务器不需要在请求中识别该属性。客户端实现**绝不**(MUST NOT)能假定 LDAP 服务器具有执行属性子类型化的能力。

(2.5.4.49 NAME 'distinguishedName' EQUALITY distinguishedNameMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12)

5.51、uniqueMember

(2.5.4.50 NAME 'uniqueMember' EQUALITY uniqueMemberMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.34)

5.52、houseIdentifier

该属性用于在一个地址标识一座建筑。

(2.5.4.51 NAME 'houseIdentifier' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768})

5.53、supportedAlgorithms

该属性以二进制格式被存储和请求，以'supportedAlgorithms;binary'。

(2.5.4.52 NAME 'supportedAlgorithms'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.49)

5.54、deltaRevocationList

该属性以二进制格式被存储和请求，以'deltaRevocationList;binary'。

(2.5.4.53 NAME 'deltaRevocationList'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.9)

5.55、dmdName

该属性的值指定一个目录管理域（DMD: directory management domain），目录管理域是操作目录服务器管理中心。

(2.5.4.54 NAME 'dmdName' SUP name)

6、语法（Syntaxes）

服务器**应该**（SHOULD）识别在本节定义的语法。每个语法说明都以一个 ldapSyntaxes 属性值的范例开始，ldapSyntaxes 属性定义了语法的对象标识符（OBJECT IDENTIFIER）。语法名的描述不在协议中定义，并不保证是唯一的。

6.1、传递方法（Delivery Method）

(1.3.6.1.4.1.1466.115.121.1.14 DESC 'Delivery Method')

该语法的值按照下列 BNF 进行编码：

delivery-value = pdm / (pdm whsp "\$" whsp delivery-value)

pdm = "any" / "mhs" / "physical" / "telex" / "teletex" /
"g3fax" / "g4fax" / "ia5" / "videotex" / "telephone"

例如:

telephone

6.2、增强指南 (Enhanced Guide)

(1.3.6.1.4.1.1466.115.121.1.21 DESC 'Enhanced Guide')

该语法的值按照下列 BNF 进行编码:

EnhancedGuide = woid whsp "#" whsp criteria whsp "#" whsp subset

subset = "baseobject" / "oneLevel" / "wholeSubtree"

标准的产品在下面的 Guide 语法中定义。该语法已被增加到 RFC 1778 的后来版本中。

例如:

person#(sn)#oneLevel

6.3、指南 (Guide)

(1.3.6.1.4.1.1466.115.121.1.25 DESC 'Guide')

该语法的值按照下列 BNF 进行编码:

guide-value = [object-class "#"] criteria

object-class = woid

criteria = criteria-item / criteria-set / ("!" criteria)

criteria-set = (["("] criteria "&" criteria-set [")"]) /
(["("] criteria "|" criteria-set [")"])

criteria-item = ["("] attributetype "\$" match-type [")"]

match-type = "EQ" / "SUBSTR" / "GE" / "LE" / "APPROX"

该语法不应该被用于定义新属性。

6.4、八进制字符串（Octet String）

(1.3.6.1.4.1.1466.115.121.1.40 DESC 'Octet String')

该语法的值按照下列 BNF 进行编码：

例如：

secret

6.5、Teletex Terminal Identifier

(1.3.6.1.4.1.1466.115.121.1.51 DESC 'Teletex Terminal Identifier')

该语法的值按照下列 BNF 进行编码：

teletex-id = ttx-term 0*("\$" ttx-param)

ttx-term = printablestring

ttx-param = ttx-key ":" ttx-value

ttx-key = "graphic" / "control" / "misc" / "page" / "private"

ttx-value = octetstring

在上面，第一个可打印字符串（printablestring）是电报终端标识编码的第一部分，后面的 0 个或多个八进制字符（octetstrings）是电报终端标识的后续部分。

6.6、Telex Number

(1.3.6.1.4.1.1466.115.121.1.52 DESC 'Telex Number')

该语法的值按照下列 BNF 进行编码：

telex-number = actual-number "\$" country "\$" answerback

actual-number = printablestring

country = printablestring

answerback = printablestring

在上面，actual-number 是被编码的电报（TELEX）号码数字的数字部分的语法表示，country 是电报的国家代码，answerback 是电报（TELEX）终端的应答代码。

6.7、Supported Algorithm

(1.3.6.1.4.1.1466.115.121.1.49 DESC 'Supported Algorithm')

在本文档中没有定义 supportedAlgorithms 属性值的可打印形式。希望存储和检索这个属性的客户端必须（MUST）使用 "supportedAlgorithms;binary"，在属性 "supportedAlgorithms;binary" 中传输采用二进制编码。

7、对象类（Object Classes）

LDAP 服务器必须（MUST）识别对象类 "top" 和 "subschema"。LDAP 服务器应该（SHOULD）识别本节列出的，作为 objectClass 属性的值的，所有其它对象类。

7.1、top

(2.5.6.0 NAME 'top' ABSTRACT MUST objectClass)

7.2、alias

(2.5.6.1 NAME 'alias' SUP top STRUCTURAL MUST aliasedObjectName)

7.3、country

(2.5.6.2 NAME 'country' SUP top STRUCTURAL MUST c
MAY (searchGuide \$ description))

7.4、locality

(2.5.6.3 NAME 'locality' SUP top STRUCTURAL
MAY (street \$ seeAlso \$ searchGuide \$ st \$ l \$ description))

7.5、organization

(2.5.6.4 NAME 'organization' SUP top STRUCTURAL MUST o
MAY (userPassword \$ searchGuide \$ seeAlso \$ businessCategory \$
x121Address \$ registeredAddress \$ destinationIndicator \$
preferredDeliveryMethod \$ telexNumber \$ teletexTerminalIdentifier \$
telephoneNumber \$ internationalISDNNumber \$

facsimileTelephoneNumber \$
street \$ postOfficeBox \$ postalCode \$ postalAddress \$
physicalDeliveryOfficeName \$ st \$ l \$ description))

7.6、 organizationalUnit

(2.5.6.5 NAME 'organizationalUnit' SUP top STRUCTURAL MUST ou
MAY (userPassword \$ searchGuide \$ seeAlso \$ businessCategory \$
x121Address \$ registeredAddress \$ destinationIndicator \$
preferredDeliveryMethod \$ telexNumber \$ teletexTerminalIdentifier \$
telephoneNumber \$ internationaliSDNNumber \$
facsimileTelephoneNumber \$
street \$ postOfficeBox \$ postalCode \$ postalAddress \$
physicalDeliveryOfficeName \$ st \$ l \$ description))

7.7、 person

(2.5.6.6 NAME 'person' SUP top STRUCTURAL MUST (sn \$ cn)
MAY (userPassword \$ telephoneNumber \$ seeAlso \$ description))

7.8、 organizationalPerson

(2.5.6.7 NAME 'organizationalPerson' SUP person STRUCTURAL
MAY (title \$ x121Address \$ registeredAddress \$
destinationIndicator \$
preferredDeliveryMethod \$ telexNumber \$ teletexTerminalIdentifier \$
telephoneNumber \$ internationaliSDNNumber \$
facsimileTelephoneNumber \$
street \$ postOfficeBox \$ postalCode \$ postalAddress \$
physicalDeliveryOfficeName \$ ou \$ st \$ l))

7.9、 organizationalRole

(2.5.6.8 NAME 'organizationalRole' SUP top STRUCTURAL MUST cn
MAY (x121Address \$ registeredAddress \$ destinationIndicator \$
preferredDeliveryMethod \$ telexNumber \$ teletexTerminalIdentifier \$
telephoneNumber \$ internationaliSDNNumber \$
facsimileTelephoneNumber \$
seeAlso \$ roleOccupant \$ preferredDeliveryMethod \$ street \$
postOfficeBox \$ postalCode \$ postalAddress \$
physicalDeliveryOfficeName \$ ou \$ st \$ l \$ description))

7.10、groupOfNames

(2.5.6.9 NAME 'groupOfNames' SUP top STRUCTURAL MUST (member \$ cn)
MAY (businessCategory \$ seeAlso \$ owner \$ ou \$ o \$ description))

7.11、residentialPerson

(2.5.6.10 NAME 'residentialPerson' SUP person STRUCTURAL MUST 1
MAY (businessCategory \$ x121Address \$ registeredAddress \$
destinationIndicator \$ preferredDeliveryMethod \$ telexNumber \$
teletexTerminalIdentifier \$ telephoneNumber \$
internationaliSDNNumber \$
facsimileTelephoneNumber \$ preferredDeliveryMethod \$ street \$
postOfficeBox \$ postalCode \$ postalAddress \$
physicalDeliveryOfficeName \$ st \$ l))

7.12、applicationProcess

(2.5.6.11 NAME 'applicationProcess' SUP top STRUCTURAL MUST cn
MAY (seeAlso \$ ou \$ l \$ description))

7.13、applicationEntity

(2.5.6.12 NAME 'applicationEntity' SUP top STRUCTURAL
MUST (presentationAddress \$ cn)
MAY (supportedApplicationContext \$ seeAlso \$ ou \$ o \$ l \$
description))

7.14、dSA

(2.5.6.13 NAME 'dSA' SUP applicationEntity STRUCTURAL
MAY knowledgeInformation)

7.15、device

(2.5.6.14 NAME 'device' SUP top STRUCTURAL MUST cn
MAY (serialNumber \$ seeAlso \$ owner \$ ou \$ o \$ l \$ description))

7.16、strongAuthenticationUser

(2.5.6.15 NAME 'strongAuthenticationUser' SUP top AUXILIARY
MUST userCertificate)

7.17、certificationAuthority

(2.5.6.16 NAME 'certificationAuthority' SUP top AUXILIARY
MUST (authorityRevocationList \$ certificateRevocationList \$
cACertificate) MAY crossCertificatePair)

7.18、groupOfUniqueNames

(2.5.6.17 NAME 'groupOfUniqueNames' SUP top STRUCTURAL
MUST (uniqueMember \$ cn)
MAY (businessCategory \$ seeAlso \$ owner \$ ou \$ o \$ description))

7.19、userSecurityInformation

(2.5.6.18 NAME 'userSecurityInformation' SUP top AUXILIARY
MAY (supportedAlgorithms))

7.20、certificationAuthority-V2

(2.5.6.16.2 NAME 'certificationAuthority-V2' SUP
certificationAuthority
AUXILIARY MAY (deltaRevocationList))

7.21、cRLDistributionPoint

(2.5.6.19 NAME 'cRLDistributionPoint' SUP top STRUCTURAL
MUST (cn) MAY (certificateRevocationList \$
authorityRevocationList \$
deltaRevocationList))

7.22、dmd

(2.5.6.20 NAME 'dmd' SUP top STRUCTURAL MUST (dmdName)
MAY (userPassword \$ searchGuide \$ seeAlso \$ businessCategory \$

x121Address \$ registeredAddress \$ destinationIndicator \$
preferredDeliveryMethod \$ telexNumber \$ teletexTerminalIdentifier \$
telephoneNumber \$ internationalISDNNumber \$
facsimileTelephoneNumber \$
street \$ postOfficeBox \$ postalCode \$ postalAddress \$
physicalDeliveryOfficeName \$ st \$ l \$ description))

8、匹配规则（Matching Rules）

服务器可以（MAY）实现附加的匹配规则。

8.1、octetStringMatch

实现 extensibleMatch 过滤器的服务器**应该**（SHOULD）允许在本节列出的匹配规则在 extensibleMatch 中使用。总的来说，当匹配规则的判定语法与属性的值语法相同时，这些服务器**应该**（SHOULD）允许匹配规则与服务器所知道的所有属性类型一同使用。

(2.5.13.17 NAME 'octetStringMatch'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40)

9、安全考虑（Security Considerations）

目录条目的属性用于提供它们所代表的现实世界对象的描述性信息，它能是人、组织或设备等。绝大多数国家都有针对关于人的信息公开的隐私法。

当底层传输服务不能保证机密性并且可能导致密码泄漏给未授权的一方时，强烈建议不要采用明文密码的传输。

10、感谢（Acknowledgements）

本文档中的定义已经被电信和国际标准委员会开发。没有新的属性被增加。本语法定义基于 X.500 的 ISODE "QUIPU"实现。

11、参考书目（References）

[1] Wahl, M., Coulbeck, A., Howes, T., and S. Kille, "Lightweight X.500 Directory Access Protocol (v3): Attribute Syntax Definitions", RFC 2252, December 1997.

[2] The Directory: Models. ITU-T Recommendation X.501, 1996.

- [3] The Directory: Authentication Framework. ITU-T Recommendation X.509, 1996.
- [4] The Directory: Selected Attribute Types. ITU-T Recommendation X.520, 1996.
- [5] The Directory: Selected Object Classes. ITU-T Recommendation X.521, 1996.
- [6] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

12、作者地址（Authors' Addresses）

Mark Wahl
Critical Angle Inc.
4815 West Braker Lane #502-385
Austin, TX 78759
USA
Phone: +1 512 372 3160
EMail: M.Wahl@critical-angle.com

13、完整的版权声明（Full Copyright Statement）

略