版本信息

日期	版本	描述	作者
2004-02-08	v1.0	最初版本	LDAPChina.com
2004-05-21	v1.1	修正了格式，并改进了用词	LDAPChina.com

UTF-8 String Representation of Distinguished Names
分辨名的 UTF-8 字符串表示法

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）

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器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 的客户端和服务器。

摘要（Abstract）

X.500 目录使用分辨名（distinguished name）作为条目的主键（primary key）。在 X.500 目录协议中，分辨名使用 ASN.1 进行编码。在 LDAP 中，使用一种分辨名的字符串表示法。本规范定义了表示分辨名的字符串格式，该格式被设计用来给予普遍应用到的分辨名一个清晰的表达，该格式可以表达任何分辨名。

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 中描述的相同。

目 录

1、背景（Background）

本规范假定读者熟悉 X.500（参考文档[1]）和分辨名的概念。使用一种能够清晰表达分辨名的普通格式是非常重要的。本规范的主要目的是简化编码（encode）和解码（decode）。另一个目的是使分辨名可以让人读懂。我们并不希望某个 LDAP 客户端的用户界面直接把这些字符串显示给用户，而是使其尽可能地适合于翻译（例如，以一种本地语言来表达属性类型名）。

2、将分辨名从 ASN.1 转换为字符串（Converting DistinguishedName from ASN.1 to a String）

X.501（参考文档[2]）中，分辨名的定义如下：

```
DistinguishedName ::= RDNSequence

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET SIZE (1..MAX) OF
  AttributeTypeAndValue

AttributeTypeAndValue ::= SEQUENCE {
  type    AttributeType,
  value AttributeValue }
```

下面章节定义一种算法，该算法将分辨名从 ASN.1 结构表示法转换到 UTF-8 字符串表示法。

2.1、转换 RDNSequence（Converting the RDNSequence）

如果 RDNSequence 是一个空的序列（sequence），结果为空或长度为零的字符串。

否则，输出将由 RDNSequence（参照 2.2）中的每一个 RelativeDistinguishedName 的字符串编码组成，该输出从序列的最后一个元素开始，第一个元素移到最后。

连续多个 RelativeDistinguishedNames 的编码使用逗号（',' ASCII 44）字符分隔。

2.2 、 转 换 RelativeDistinguishedName （ Converting RelativeDistinguishedName）

当把 RelativeDistinguishedName 从 ASN.1 转换到一个字符串时，输出将由每个 AttributeTypeAndValue 的字符串编码组成（参照 2.3），与顺序无关。

若存在多值的 RDN，连续多个 AttributeTypeAndValues 的输出使用加号（'+' ASCII 43）字符分隔。

2.3 、 转 换 AttributeTypeAndValue （ Converting AttributeTypeAndValue）

AttributeTypeAndValue 被编码为 AttributeType 的字符串表示，后面跟一个等号字符（'=' ASCII 61），然后是代表 AttributeValue 的字符串。AttributeValue 的编码在 2.4 节中介绍。

如果 AttributeType 是 LDAP（参考文档[4]）相关属性类型公布表中的属性类型，那么使用该表中的类型名称字符串，否则使用 AttributeType 对象标识符（OBJECT IDENTIFIER）的点-数符号进行编码。点-数符号在参考文档[3]中描述。作为一个例子，下面列出了一些频繁地在 RDN 中出现的属性类型的字符串：

String	X.500 AttributeType
CN	commonName
L	localityName
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName
C	countryName
STREET	streetAddress
DC	domainComponent
UID	userid

2.4、将 AttributeValue 从 ASN.1 转换为字符串（Converting an AttributeValue from ASN.1 to a String）

如果 AttributeValue 是一种没有已定义的字符串表示的类型，则简单地使用井字符（'#' ASCII 35），后面跟 X.500 AttributeValue 的每个 BER 编码字节的 16 进制表示。如果

AttributeType 是点-数形式，则**应该**（SHOULD）使用上述编码方式。

否则，如果 AttributeValue 是一种具有字符串表示的类型，那么首先根据该值的语法定义，将它转换为 UTF-8 字符串。（参照参考文档[4]中的第 6 节的例子）。

如果在该 UTF-8 字符串中，没有任何下列需要转意的字符串，则该字符串可以被用作值的字符串表达。

- 在字符串开头的空格或 "#" 字符；
- 在字符串结尾的空格字符；
- 下列字符之一：","，"+"，"""，"\"，"<"，">" 或 ";"

不同的实现**可以**（MAY）对其它字符进行转意。

如果一个字符是上方列表中的某个字符，则在转意时，使用反斜线（'\' ASCII 92）字符作为前缀。

否则该字符在转意时，替换为一个反斜线和和两个 16 进制数字，这是一个字符的单字节编码。

转意机制的例子在第 5 节中介绍。

3、将字符串解析回分辨名（Parsing a String back to a Distinguished Name）

字符串的结构在 BNF 语法中指定，BNF 语法基于 RFC 822（参考文档[5]）的语法。如果服务器实现可以解析来自 LDAPv2 客户端的 DN 字符串，则它**必须**（MUST）也接受（和忽略）在本文档第 4 节给出的变量。

```
distinguishedName = [name]                    ; 可以为空字符串

name              = name-component *("," name-component)

name-component = attributeTypeAndValue *("+" attributeTypeAndValue)

attributeTypeAndValue = attributeType "=" attributeValue

attributeType = (ALPHA 1*keychar) / oid
keychar       = ALPHA / DIGIT / "-"

oid               = 1*DIGIT *("." 1*DIGIT)
```

```
attributeValue = string

string        = *( stringchar / pair )
                / "#" hexstring
                / QUOTATION *( quotechar / pair ) QUOTATION ; only from v2

quotechar     = <any character except "\" or QUOTATION >

special       = "," / "=" / "+" / "<" /    ">" / "#" / ";"

pair          = "\" ( special / "\" / QUOTATION / hexpair )
stringchar = <any character except one of special, "\" or QUOTATION >

hexstring     = 1*hexpair
hexpair       = hexchar hexchar

hexchar       = DIGIT / "A" / "B" / "C" / "D" / "E" / "F"
                / "a" / "b" / "c" / "d" / "e" / "f"

ALPHA         =   <any ASCII alphabetic character>
                                                ; (decimal 65-90 and 97-122)
DIGIT         =   <any ASCII decimal digit>    ; (decimal 48-57)
QUOTATION     =   <the ASCII double quotation mark character "" decimal 34>
```

4、与 RFC1779 和 LDAPv2 的关系（Relationship with RFC 1779 and LDAPv2）

本文档中给出的语法比 RFC 1779 中的语法更为严格。能够解析来自 LDAPv2 客户端字符串的服务器实现**必须**（MUST）接受 RFC 1779 定义的语法。然而该实现**绝不**（MUST NOT）可以产生任何未在第 2 节中提到的 RFC 1779 的编码。

服务器的具体实现**必须**（MUST）允许用一个分号字符来取代逗号来分隔分辨名（DN）中的 RDN，并且也**必须**（MUST）允许在逗号或分号的任何一边出现空格字符。空格字符被忽略，分号替换为逗号。

服务器的具体实现**必须**（MUST）允许属性类型中的 oid 带有"oid" 或 "OID"的前缀。

服务器的具体实现**必须**（MUST）允许在名称元素（name-component：译者注：指 DN 或 RDN）和 ',' 之间存在空格（' ' ASCII 32）字符，在 attributeTypeAndValue 和 '+' 之间存在空格，在 attributeType 和 '=' 之间存在空格，在 '=' 和 attributeValue 之间存在空格。这些空格字符在解析时被忽略。

实现**必须**（MUST）允许一个值被双引号（"" ASCII 34）字符包围，该双引号不是值的一部分。在双引号内的值，下列字符可以存在，而不需要任何转意：

","，"="，"+"，"<"，">"，"#" 和 ";"

5、范例（Examples）

本符号集被设计用于方便将名称命名为普通形式。本节将给出一些使用本符号集书写的分辨名的示例。第一个例子包含三个相对分辨名（RDN）：

CN=Steve Kille,O=Isode Limited,C=GB

这是一个包含三个 RDN 的例子，第一个 RDN 是多值的：

OU=Sales+CN=J. Smith,O=Widget Inc.,C=US

下面的范例展示了如果一个机构名称里有一个逗号，应该如何书写：（译者注：即在 DN 的属性值中存在有需要转意的字符）

CN=L. Eagle,O=Sue\, Grabbit and Runn,C=GB

下面的范例中，名称的一个属性值中包含一个回车字符：

CN=Before\0DAfter,O=Test,C=GB

下面的范例中，名称中的一个 RDN 包含不可识别的类型。值是一个八进制字符串（OCTET STRING）的 BER 编码，该编码包含 0x48 和 0x69 两个字节。

1.3.6.1.4.1.1466.0=#04024869,O=Test,C=GB

在最后这个范例中，RDN 的值由五个字符组成：

Unicode Letter Description	10646 code	UTF-8	Quoted
LATIN CAPITAL LETTER L	U0000004C	0x4C	L
LATIN SMALL LETTER U	U00000075	0x75	u
LATIN SMALL LETTER C WITH CARON	U0000010D	0xC48D	\C4\8D
LATIN SMALL LETTER I	U00000069	0x69	i
LATIN SMALL LETTER C WITH ACUTE	U00000107	0xC487	\C4\87

能够使用可打印的 ASCII 字符书写（对于 debug 有帮助）：

SN=Lu\C4\8Di\C4\87

6、参考书目（References）

[1] The Directory -- overview of concepts, models and services. ITU-T Rec.

X.500(1993).

[2] The Directory -- Models. ITU-T Rec. X.501(1993).

[3] Wahl, M., Howes, T., and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

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

[5] Crocker, D., "Standard of the Format of ARPA-Internet Text Messages", STD 11, RFC 822, August 1982.

[6] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119.

7、安全考虑（Security Considerations）

7.1、泄密（Disclosure）

分辨名典型地由关于条目的描述性信息组成，可以是人、组织、设备、或其它现实世界中的对象。这经常包括一些下列的各类信息：

- 该对象的公共名称（common name，译者注：就是 DN 中经常用到的 cn 的全称）（例如：某个的全名）

- 电子邮件地址或 TCP/IP 地址

- 它的物理方位（国家、省、市、街道地址）

- 机构的属性（例如：部门的名称或上下级关系）

绝大多数国家都有针对关于人的信息公开的隐私法。

7.2、在安全应用程序中分辨名的使用（Use of Distinguished Names in Security Applications）

AttributeValue 从 X.501 格式转换到 LDAP 字符串表示的过程并不总是可逆的，也就是说不总是能够逆向转换为同样的 BER 或 DER 形式。在验证一个 X.509 证书时，需要分辨名的 DER 格式，这是这种情况的一个例子。

例如，由带有一个 AVA 的 RDN 组成的分辨名，在该分辨名中，属性类型是 commonName，值是 TeletexString 类型的字符'Sam'，它在 LDAP 中表示为字符串 CN=Sam。另一个分辨名

值仍然是'Sam'，但是值是 PrintableString 类型，它将具有相同的表示 CN=Sam。

需要重构值的 DER 形式的应用程序，在将一个分辨名转换成 LDAP 格式时**不应该**（SHOULD NOT）使用字符串表达的属性语法。相应的，它们**应该**（SHOULD）使用在 2.4 节第一段描述的以（'#'）为前缀的 16 进制形式。

8、作者地址（Authors' Addresses）

Mark Wahl
Critical Angle Inc.
4815 W. Braker Lane #502-385
Austin, TX 78759
USA
EMail: mailto:M.Wahl@critical-angle.com

Steve Kille
Isode Ltd.
The Dome
The Square
Richmond, Surrey
TW9 1DT
England
Phone: +44-181-332-9091
EMail: mailto:S.Kille@ISODE.COM

Tim Howes
Netscape Communications Corp.
501 E. Middlefield Rd, MS MV068
Mountain View, CA 94043
USA
Phone: +1 650 937-3419
EMail: mailto:howes@netscape.com

9、完整的版权声明（Full Copyright Statement）