ICS 35.240.80
C 07

中华人民共和国国家标准

GB/T 25513—2010/ISO/TS 21091:2005

健康信息学 安全、通信以及专业人员与患者标识的目录服务

Health informatics—Directory services for security, communications and identification of professionals and patients

(ISO/TS 21091:2005, IDT)

2010-12-01 发布　　2011-05-01 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

目　次

前　言

本标准等同采用ISO/TS 21091:2005《健康信息学　安全、通信以及专业人员与患者标识的目录服务》，其技术内容和结构与ISO/TS 21091一致。为便于使用，本标准与ISO/TS 21091:2005相比作了下列编辑性修改：

——正文、附录A和附录B中增加了表的编号和表题；

——正文、附录A和附录B中增加了提及表的文字。

本标准的附录A和附录B为资料性附录。

本标准由中国标准化研究院提出并归口。

本标准起草单位：中国标准化研究院。

本标准主要起草人：董连续、郭玉峰、石丽娟、陈煌、尹书蕊。

引　言

本标准旨在支持卫生保健专业人员在执行临床与管理功能时对通信及其安全性的需求。卫生保健服务在进行各种保密性健康信息的解密与传输时，对加密与访问控制有广泛需求。为支持卫生保健公钥基础设施，需完成与处理卫生保健事物相关的、包括企业与专业人员信息的许可证注册。这些信息应包含个体角色在卫生保健系统中的标识，而且只能由卫生保健组织各自来识别。同样，注册和管理功能应是可扩展的，而且能够分布到卫生保健的所有实体中。对这些附加的卫生保健安全需求的支持，也需要通过目录服务来提供。

目录正在成为越来越普遍的方法，能够提供单点登录能力。这个目标已使得目录模式得到扩展，包括了组织雇员管理信息、卫生保健具体的联系信息以及卫生保健标识符。本标准将评价卫生保健对目录的具体需求，并适当地将这些信息纳入卫生保健目录的标准规范。

健康信息学 安全、通信以及专业人员与患者标识的目录服务

1 范围

本标准给出了使用 X.500 框架的卫生保健目录服务的基本规范。本标准规定了用以支持在公共网络上安全地交换卫生保健信息所需的通用目录信息和服务。本标准从联合体的视角来编址健康目录，期待其能够用来支持企业间、管辖区域间以及国际间的卫生保健的通信。卫生保健数据通信不仅需要依赖主要在其他 ISO 标准中推出的安全技术措施，还需要一个可信赖的、可问责的“信任链”。为了在公钥基础设施中维护此信任链，用户（依赖方）应能够通过安全目录管理获得当前正确的证书和证书状态信息。

本标准除支持对访问控制、保密性等安全服务外，还给出了通信的其他方面的规范，如通信实体的地址与协议。

本标准还支持对卫生保健专业人员、健康组织和患者/消费者进行标识的目录服务，后面这些服务包括的内容有时被称为患者主索引。

本卫生保健目录将只支持标准的 LDAP（轻量目录访问协议）客户搜索。具体的实施指南、搜索标准和相关支持已超出本标准的范围。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。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标准，然而，鼓励根据本标准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标准。

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（ITU-T Recommendation X.500:2001，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（ITU-T Recommendation X.501:2001，ISO/IEC 9594-2:2005，IDT）

GB/T 16264.3—2008 信息技术 开放系统互连 目录 第 3 部分：抽象服务定义（ITU-T Recommendation X.511:2001，ISO/IEC 9594-3:2005，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（ITU-T Recommendation X.520:2001，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（ITU-T Recommendation X.521:2001，ISO/IEC 9594-7:2005，IDT）

IETF/RFC 3771:2004 轻量目录访问协议（LDAP）中间应答消息

IETF/RFC 3377:2002 轻量目录访问协议（v3）技术规范

IETF/RFC 3698:2004 轻量目录访问协议（LDAP）附加的匹配规则

3 术语和定义

下列术语和定义适用于本标准。

3.1

访问控制 access control

一种保证手段，即数据处理系统的资源只能由被授权实体按授权方式进行访问。

[GB/T 5271.8—2001,08.04.01]

3.2

可核查性 accountability

一种特性，即能保证某个实体的行动能唯一地追溯到该实体。

[GB/T 5271.8—2001,08.01.10]

3.3

属性机构 attribute authority;AA

通过发布属性证书来分配权限的机构。

[X.509]

3.4

属性证书 attribute certificate

由属性机构进行数字签名的数据结构，它将某些属性值与其持有者的标识绑定在一起。

[X.509]

3.5

鉴别 authentication

通过将标识符与其鉴别码进行安全关联来可靠识别安全主体的过程。

注：也可参见“数据原发鉴别”和“对等层实体鉴别”。

[GB/T 21716.1—2008,3.2.4]

3.6

授权 authorization

授予权限，包括允许基于访问权的访问。

[GB/T 9387.2—1995,3.3.10]

3.7

可用性 availability

根据授权实体的请求可被访问与使用。

[GB/T 9387.2—1995,3.3.11]

3.8

证书 certificate

公钥证书。

3.9

证书分发 certificate distribution

向安全主体发布和传输证书的行为。

3.10

证书发行方 certificate issuer

受到一个或多个依赖方所信任的、创建并分配证书的权威机构。

注：证书管理机构能够可选择地创建依赖方密钥。

[ISO/IEC 9594-8]

3.11

证书管理 certificate management

与证书相关的程序，即证书生成、证书分发、证书归档和撤销。

3.12

证书撤销 certificate revocation

即使证书没有过期，但由于证书不再可信，导致对证书与其持有方（或安全主体持有者）之间所有可靠链接进行删除的行为。

3.13

证书撤销列表 certificate revocation list;CRL

被中止和被废除的证书的公布列表（由 CA 数字签名）。

3.14

证书验证 certificate verification

验证证书是否可信。

3.15

认证机构 certification authority;CA

证书机构

证书认证机构

通过使用其私有签名密钥签署证书数据来发放证书的实体。

注：术语“CA”中的机构并不特指政府机构，它只是说明该机构是可信任的。“证书发行方”可能是一个更合适的术语，但广泛使用的是“CA”。

3.16

保密性 confidentiality

机密性

这一性质使信息不泄露给非授权的个人、实体或进程，不为其所用。

[GB/T 9387.2—1995，3.3.16]

3.17

数据完整性 data integrity

这一性质表明数据没有遭受以非授权方式所作的篡改或破坏。

[GB/T 9387.2—1995，3.3.21]

3.18

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换（见“密码学”），这种数据或变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人（例如接收者）进行伪造。

[GB/T 9387.2—1995，3.3.26]

3.19

标识 identification

以使数据处理系统能够识别实体的测试性能。

[ISO/IEC 2382-8]

3.20

标识符 identifier

在用相应的鉴别码进行进一步确证之前，用于说明身份的信息片段。

[ENV 13608-1]

3.21

完整性 integrity

证明在传输过程中没有以任何方式对消息内容进行有意或偶然的改变。

[GB/T 9387.2—1995,3.3.31]

3.22

密钥 key

控制加密和解密操作的一符号序列。

[GB/T 9387.2—1995,3.3.32]

3.23

密钥管理 key management

在一种安全策略指导下密钥的产生、存储、分配、删除、归档及应用。

[GB/T 9387.2—1995,3.3.33]

3.24

轻量目录访问协议 lightweight directory access protocol;LDAP

标准的目录访问协议,允许对公钥基础设施中所需的证书以及其他信息进行公开或受控的访问。

3.25

对象标识符 object identifier;OID

在 ISO 注册标准下注册,用于参照特定对象或对象类的唯一的字母数字/数字标识符。

3.26

患者 patient

消费者 consumer

健康相关服务的接受者和健康信息系统中的参与者。

注:健康相关服务的接受者不限于病人。

[GB/T 21716.1—2008,3.1.6]

3.27

隐私权 privacy

防止因不正当或非法收集和使用个人数据而对个人的私生活或私事进行侵犯。

[ISO/IEC 2382-8]

3.28

私有密钥 private key

私钥

在非对称密码算法中使用的并且其拥有者是受限制(通常只能由一个实体拥有)的密钥。

[GB/T 18794.1—2002,3.3.10]

3.29

公开密钥 public key

公钥

在非对称密码算法中使用的并且可以被公开的密钥。

[GB/T 18794.1—2002,3.3.11]

3.30

公钥证书 public key certificate;PKC

将身份与公钥绑定的 X.509 公钥证书。

注:在客户端证明它拥有 PKC 中公钥对应的私钥后,可以使用身份来支持基于身份的访问控制决策。

[IETF/RFC 3280]

3.31

公钥基础设施 public key infrastructure;PKI

由硬件、软件、人员、过程和策略所构成,它使用数字签名技术为依赖方提供非对称密钥对的公开组

件与特定主体之间的可验证关联。

3.32

依赖方 relying party

证书的接收方,它依靠证书和/或通过该证书验证的数字签名进行活动。

[IETF/RFC 3647]

3.33

角色 role

与一项任务相关的能力和/或行为的集合。

3.34

安全 security

可用性、保密性、完整性和可确认性的组合。

[ENV 13608-1]

3.35

安全策略 security policy

为保障计算机安全所采取的行动计划或方针。

[GB/T 5271.8—2001,08.01.06]

3.36

安全服务 security service

由参与通信的开放系统的层所提供的服务,它确保该系统或数据传送具有足够的安全性。

[GB/T 9387.2—1995,3.3.51]

3.37

主体 subject

所属公钥在证书中被证明的实体。

3.38

第三方 third party

数据发送方和数据接收方之外的另一参与方。它被要求实施通信协议部分的安全功能。

3.39

可信第三方 trusted third party;TTP

对于安全协议而言被认为是可信第三方。

注:本术语被用于许多 ISO/IEC 国际标准和其他主要描述 CA 服务的文献中。然而,该定义是比较宽泛的,它包括诸如时间戳和由第三方保存的契据之类的服务。

[ENV 13608-1]

3.40

X.509

针对证书和相应鉴别框架的国际电信联盟标准 X.509。

4 缩略语

下列缩略语适用于本标准。

CA	认证机构	Certification Authority
CRL	证书撤销列表	Certificate Revocation List
DAP	目录访问协议	Directory Access Protocol
DIT	目录信息树	Directory Information Tree

LDAP	轻量目录访问协议	Lightweight Directory Access Protocol
MPI	患者主索引	Master Patient Index
PDA	个人数字助理	Personal Data Assistant
PIDS	个人标识服务	Person Identification Service
PKC	公钥证书	Public Key Certificate
PKI	公钥基础设施	Public Key Infrastructure
RA	注册机构	Registration Authority
TTP	可信第三方	Trusted Third Party

5 卫生保健的相关环境

5.1 概述

为了适应对特定卫生保健项目的关切，卫生保健目录应加以扩展。健康信息的通信与管理工作日渐依赖网络，扩大了对卫生保健特定目录以及与之相关的大量信息与安全服务支持的需求。伴随对基于互联网与内联网的健康信息系统使用的增加，需要利用自动系统和基于人机交互的系统，使健康信息在内部多个实体间以及与外部实体间进行传递。实现这种分布式的健康信息管理和通信，需要一部涵盖通信数据、卫生保健专业目录以及消费者信息等内容的标准(见附录 A)。

相关组织越来越依赖于不断增强的信息技术基础设施，通过使用 LDAP 简化并加强用户管理功能，从而在组织内部的多个系统间管理与访问用户中心存储库。这些活动涉及到社团和公共机构目录、系统和服务的定义、合作方目录的定义等。不同于企业模式，在卫生保健领域需要更强的模式化的相关环境，以应对卫生保健规章信息、临床资格、卫生保健专业和组织层面上的多种隶属关系、卫生保健联合体的非组织成员、消费者和业务伙伴的表达需求。

另外，目录在用户鉴别与安全基础设施管理等方面的应用也在扩大，通过创建用于用户管理的单一信息来源，卫生保健组织能够增强用户标识识别与安全鉴别、退出过程的权限撤销、角色管理和访问控制。通过提供“单点登录”能力，可以支持更好的口令安全性。然而，当它作为提高安全性的强有力的工具时，目录本身以及目录间的需求也更为复杂了。

卫生保健目录的另外一种安全服务是支持卫生保健 PKI。此类服务利用目录进行公钥的存取及 PKI 服务支持(如 CRL 的存取)。对 PKI 和增强安全服务的支持，带来了对服务、应用组件和设备的额外对象的支持需求，从而增加了卫生保健目录的复杂性。

5.2 卫生保健人员

虽然 X.500 标准包括多个用以表达个人、雇员等人员信息的对象类，但这些对象类中缺乏支持行业通信与服务所需的、用于表达关键的卫生保健特定信息的标准属性。在目录中，卫生保健联合体需要表达诸如证书、卫生保健标识符、角色特定信息以及卫生保健特定联系信息等专业信息。由于卫生保健的联系信息具有多种从属关系的性质(见 5.3)，所以这类联系信息比典型业务环境中的联系信息要复杂得多。卫生保健人员包括：

——正规的卫生保健专业人员；

——非正规的卫生保健专业人员；

——卫生保健组织及其支持组织的雇员；

——卫生保健消费者。

卫生保健消费者所含内容要求保持核心目录信息、MPI 信息和保密性的平衡。

5.3 多种从属关系

在许多环境里，卫生保健人员可能与多个组织有关系，而且这些人在与他们有关系的每个组织中都

可能会行使不同的职责。卫生保健专业人员可以独立营业，也可以在一个或者多个组织内从业。同样，支撑服务也能够被提供给多个卫生保健组织。按照保健环境或其他因素，在卫生保健组织内部的个人可以担任不同角色。保健消费者通常向众多的卫生保健专家和组织寻求服务。为了尽量减少由于信息重复管理所致的不精确性，卫生保健模式中应备有与主要管理资源的链接，以支持多种从属关系。卫生保健工作人员也是卫生保健的消费者，但应该区分这两种身份。

5.4 卫生保健组织

虽然 X.500 标准提供了用于描述组织的对象类，但在这些构造中，缺乏支持卫生保健目录、用于表达卫生保健特定信息的足够属性。卫生保健特定信息包括：

——监管的标识符；

——所提供的服务类别；

——服务地址；

——密钥信息管理功能的联系信息。

卫生保健组织包括：

——正规的卫生保健组织(即：医院、药房、门诊部、机动部门、专业的护理所、专科单元)；

——付款方、支持组织(即：供应方、转录服务、编码服务、索赔处理服务)；

——监管/监控机构(即：疾病控制、药品控制、公共卫生)。

5.5 硬件/软件

当 X.500 为服务和应用提供对象类时，卫生保健设备和软件应服从监管和确认要求，因此上述对象类中应包括能够确切地表达卫生保健目录要求的额外属性。PDA 和其他设备也可以在卫生保健目录中与其他实体有特定关联。目录中硬件和软件的表达只限于它们的标识及其通信参数，以及它们与个体和组织的关联。目录可以用于资产标识，但不宜用于资产管理。

5.6 卫生保健安全服务

卫生保健认证机构、属性管理机构和注册机构需在目录中予以表达，这些机构应能发布有关密钥管理信息。对目录内卫生保健角色管理的支持应能够表达卫生保健的特定组成部分，包括与卫生保健人员相关的工作职能、工作特定的联系信息及其证书(包括职业证书和属性证书)，但不包括对功能角色表达的直接支持。

6 目录安全管理框架

卫生保健应由强安全管理策略的框架所支持，以确保通信数据和鉴别基础设施的完整性。国际标准已对此类强实践原则给出了定义。以下标准并非针对目录，但为保护目录基础设施也应遵守这些标准：

——ISO 22600-2[2]；

——ISO/IEC TR 13335-1[6]：信息技术安全 GMITS 的管理的指南；

——信息及相关技术的控制目标(COBIT)规范，由信息系统审计与控制基金会(Information Systems Audit and Control Foundation)制定。

特定安全措施和访问控制的规范虽不属于本标准范围，但由于目录服务支持的健康相关信息和隐私信息的敏感性，所以应能在有关分支、对象类和属性层面予以有效的控制。此框架应包含适当的进程和程序，以确保健康目录中所表达的可核查性和信息完整性。对卫生保健目录所有条目的读、写和修改最好都能在适当的访问控制管理下进行。

7 互操作性

7.1 要求

卫生保健目录应能与不同参与方目录联系和/或交换相关信息，所需技术包括目录之间的链接、复

制、引用和单边或双边信任。其中有些技术会因应用或服务的模式不一致而受到影响。以下层级注意事项适用于互操作模型。

a) 应能将卫生保健客户群/联合体物理上分离为一种受控的、高级的服务环境；
b) 应能提供复制和负载平衡的管理功能；
c) 应能将检索树限制在特定的地理或逻辑区域，以提供有效率的访问性能(如 80/20 法则)；
d) 应能通过分支点的引用来组织 DIT，以利于访问控制管理，保护存储在目录中的敏感信息(例如：患者证书应不能被公开访问)；
e) 应能组织 DIT，以实现卫生保健权限的分布式访问。

7.2 命名空间/树形结构

7.2.1 概述

为了以统一的方式落实这些要求，并依附现行的卫生保健监管辖区，应有 7.2.2～7.2.7 所描述的高层命名空间和树形结构。命名空间和树形结构的视图表示见图 1。

7.2.2 国家

在任何情况下，应有卫生保健专业权限的国家，并应将该国家置于树形结构的顶层。某组织在多个国家运营的情况下，应有一个视图，将该组织置于卫生保健监管辖区下。

C=必选的

7.2.3 地区

在地区代表监管辖区的国家(如美国各州)中，地区应被用来描绘卫生保健监管辖区的地域。

l=可选的

7.2.4 组织

组织应被用来指明卫生保健监管区域签发机构，目录中的卫生保健专业人员在此机构中被授权。组织也可以被用来表达卫生保健专业组织和机构。

O=签发机构，卫生保健专业组织

7.2.5 组织单元

对那些有多个专业授权分支的区域，应将签发机构进一步分类为组织单元。例如：在很多国家药剂师、内科医师、牙医可由单独的政府机构或部门分别管理。

OU=签发机构专业分支

7.2.6 结构化角色

在层级结构的每一层次，标准的结构化角色和本地定义的结构化角色都可并存。对结构化角色概念的进一步描述见 9.2.5。

7.2.7 个体的多实例化

在系统中每一个体的标识只能表达一次，除非某个体具有多个专业凭证，或与多个卫生保健组织相关，或其他有多个表达的情况。相关的区分和信息表达由对象类和目录信息树所支持，不过仅用对象类不能确保完成理想的区分。然而，通用名(Common Name)唯一性的结构确实能够经由每个健康标识中的个体的多实例的实例化来实现这种区分。

在卫生保健领域，需要通过不同监管主体启用和表达卫生保健标识的独立的“所有权”。在不同的监管主体下，个体相应具有不同的联系信息和管理信息。例如：由于这种多重监管机制，每种许可证类型和辖区的联系信息和基本通信信息可能存在冲突的属性内容。这种在同一目录中跨管辖区的实例应保持独立。

个体在目录中可以同时作为患者和保健服务提供者存在，在目录中应将个体的个人实例与职业实例分开，以保障适当的隐私管理。虽然 DIT(见图 1)可描述个人、组织、设备等参与者，但并不要求在同一个物理或逻辑信息空间之内完全包含这些参与者。可以根据体系机构设计和优化服务性能的需要，对它们进行分割。一个卫生保健目录中可以全部、部分采用或完全不采用上述参与者，并且可以采用集

中和分散的方法实现。

在任何给定的辖区中，正规的卫生保健专业人员仅能被实例化一次。通过采用以下所描述的HCOrganizationalRole中的RoleOccupant属性(包括专业人员的DN)，可以表达该实例在众多组织中的不同标识。使用这种结构，可以检索到工作特定的联系信息。

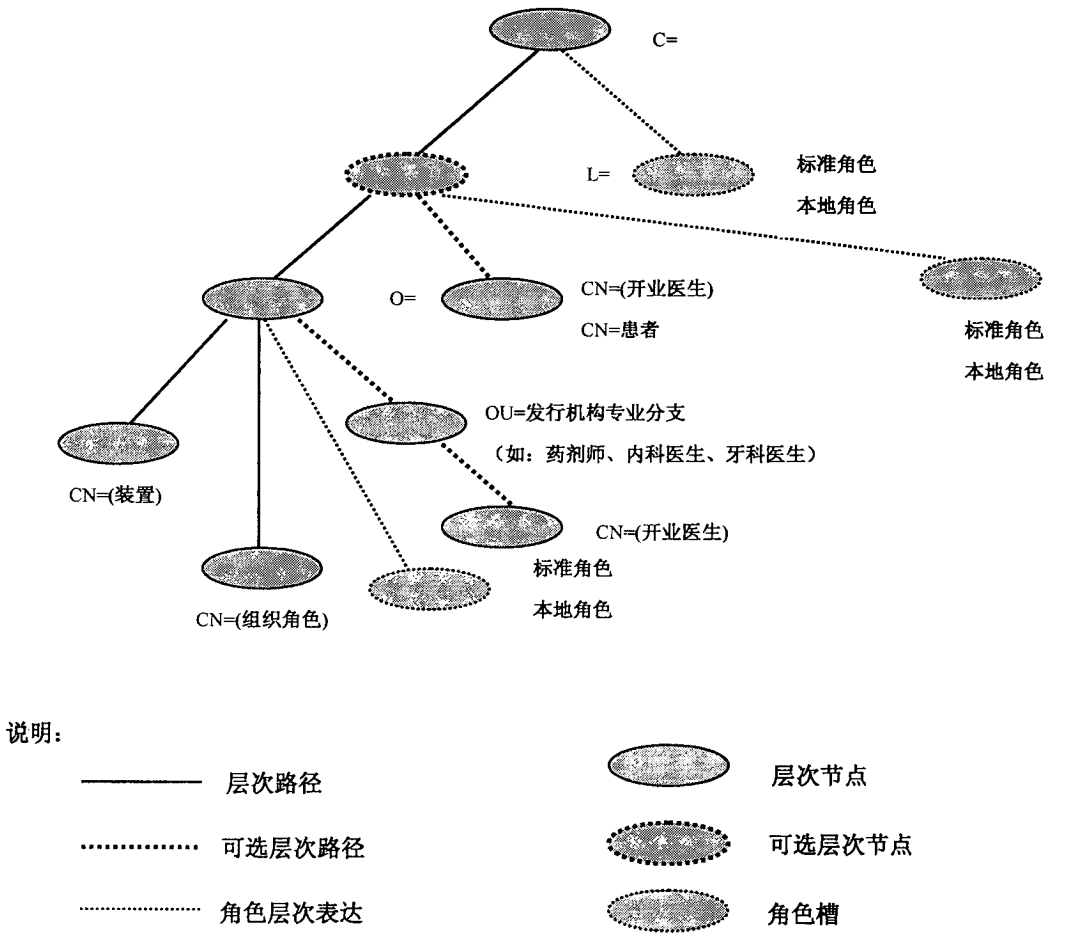

图 1 卫生保健的目录信息树(DIT)

8 卫生保健模式

8.1 卫生保健人员

8.1.1 概述

卫生保健目录中可表达个体的多种类型。除了在其他适合且必要的情况下，系统中每个个体的标识应该只被表达一次。例外的一个例子是，某个卫生保健专业人员在作为患者与卫生保健系统进行交互的情况下，该个体可以由两种对象类进行表达：一种包含专业特定信息，另一种包括患者特定信息。它们都具有“人员”的父类，并相应地进行特例化来表达如下个体类型：卫生保健消费者、卫生保健专业人员和卫生保健雇员。针对每个特例化类应在基本对象类上添加相应的信息属性(见附录B)。

包括扩展属性的对象类模式定义见表1。

表 1 对象类模式

属性	所支持的新属性名称
OID(对象标识符)	ISO/TC 215 设定的与新属性关联的对象标识符
描述	新属性的描述
语法	表达属性的 LDAP 支持的语法
匹配规则	当执行搜索和比较操作时,服务器对属性值与断言值进行比较所采用的匹配规则
多值	该属性是否支持表达多值

模式扩展规范内容还包括附加属性哪些是必选,哪些是可选的信息。

8.1.2 卫生保健消费者

对象类:HCConsumer

上级对象类:InetOrgPerson

对象标识符:1.0.21091.1.1

对象类的类型:结构化

必选属性:见表 2

表 2 HCConsumer 的必选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcConsumerID	1.0.21091.2.1.1	可以是一个可标识、匿名或假名写的标识符(发布机构:类型:ID)	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是

使用这种结构时,HcConsumerID 可用来表达任何标识符,包括但不限于安全号码、健康保险号码、医学记录号码和驾驶证号码。

可选属性:见表 3

表 3 HCConsumer 的可选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcIdentification Service	1.0.21091.2.0.2	提供生物测定或者其他标识验证服务的服务地址	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是
HcSigningCertificate	1.0.21091.2.0.3	针对用于健康交易的用户认可签名证书的公钥和证书	二进制	证书精确匹配和证书匹配	是
HcAttributeCertificate	1.0.21091.2.0.4	用于身份凭证、授权书、卫生保健决策者等,用 P7 格式证书填充	二进制	证书精确匹配和证书匹配	是
HcMPILocation	1.0.21091.2.1.2	可用于标识患者临床记录的患者主索引服务的定位	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是
HcSubstituteDecisionMaker	1.0.21091.2.1.3	可以签字或代表主体的人员的记录条目	可鉴别的名称	可区别的名称的匹配	是
HL7MothersMaidenName	1.0.21091.2.1.5	HL-7 定义的母亲的闺名	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是

表 3（续）

属性	对象标识符	描述	语法	匹配规则	多值
HL7DateTimeofBirth	1.0.21091.2.1.6	HL-7 定义的出生日期和时间	ISO 8601 日期	一般时间匹配 一般时间排序匹配	是
HL7Sex	1.0.21091.2.1.7	HL-7 定义的性别	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是
HL7PatientAlias	1.0.21091.2.1.8	HL-7 定义的患者别名	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是
HL7CountyCode	1.0.21091.2.1.11	HL-7 定义的国家代码	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是
HL7Religion	1.0.21091.2.1.16	HL-7 定义的宗教。该属性的应用会涉及到护理过程的患者信仰问题，因此应作为敏感的隐私信息严格保护	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是
HL7BirthPlace	1.0.21091.2.1.22	HL-7 定义的出生地点	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是
HL7PatientDeathDateandTime	1.0.21091.2.1.28	HL-7 定义的患者死亡日期和时间	日期	一般时间匹配 一般时间排序匹配	否

使用父类和扩展属性对 PIDS 属性的选择性表达：

下列 HL-7 PIDS 属性应采用参考模型属性填充，在引用 LDAP 属性的相应约束中使用所定义的 HL-7 进行格式化，见表 4。

表 4 HL-7 PIDS 属性

HL-7 PIDS 属性	inetOrgPerson/HcConsumer 属性
PatientName	包括 cn 里 XPN 格式化名称，作为第二个 cn 值
PhoneNumber _Home	homePhone(家庭电话)
PhoneNumber_Business	telephoneNumber(电话号码)
PrimaryLanguage	preferredLanguage(首选语言)
PatientAddress	homePostalAddress(家庭邮政地址)
PatientAccountNumber	如有需要，使用 HcConsumerID
SSNNumber	如有需要，使用 HcConsumerID
DriversLicenseNumber	如有需要，使用 HcConsumerID

8.1.3 卫生保健人员

对象类：HCProfessional

上级对象类：InetOrgPerson

对象标识符：1.0.21091.1.2

对象类的类型：结构化

必选属性：见表 5

可选属性：见表 6

表 5 HCProfessional 的必选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcIdentifier	1.0.21091.2.0.1	卫生保健标识符。在该标识符是指正式的卫生保健专业人员的情况下，该标识符应至少包含一项条目，用来指示该标识符由正规机构指定（发布机构：类型：ID：状态）	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是
HcProfession	1.0.21091.2.2.1	用户职业的文本表达（发布机构：代码系统：代码）	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是

表 6 HCProfessional 的可选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcIdentificationService	1.0.21091.2.0.2	提供生物测定或者其他标识验证服务的服务地址	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是
HcSigningCertificate	1.0.21091.2.0.3	针对用于健康交易的用户认可签名证书的公钥和证书	二进制	证书精确匹配和证书匹配	是
HcAttributeCertificate	1.0.21091.2.0.4	用于身份凭证、证书、受教育程度等。用 P7 格式化证书填充	二进制	证书精确匹配和证书匹配	是
HcRole	1.0.21091.2.0.5	（发布机构：代码系统：代码）用 HL-7 角色编码填充	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是
HcSpecialization	1.0.21091.2.0.6	（发布机构：代码系统：代码）用 HL-7 特化编码填充	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是
HcPrincipalPracticeLocation	1.0.21091.2.2.3	使用组织的标识名	标识名	标识名匹配	否
HcPracticeLocation	1.0.21091.2.2.4	使用组织的标识名	标识名	标识名匹配	是

8.1.4 雇员

对象类：HCEmployee

上级对象类：InetOrgPerson

对象标识符：1.0.21091.1.3

对象类类型：结构化

必选属性：见表 7

可选属性：见表 8

表 7 HCEmployee 的必选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcIdentifier	1.0.21091.2.0.1	卫生保健标识符。其发布机构允许为雇主(发布机构:ID)	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是

表 8 HCEmployee 的可选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcIdentificationService	1.0.21091.2.0.2	提供生物测定或者其他标识验证服务的服务地址	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是
HcSigningCertificate	1.0.21091.2.0.3	针对用于健康交易的用户认可签名证书的公钥和证书	二进制	证书精确匹配和证书匹配	是
HcAttributeCertificate	1.0.21091.2.0.4	用于身份凭证、证书、受教育程度等,用 P7 格式化证书填充	二进制	证书精确匹配和证书匹配	是
HcRole	1.0.21091.2.0.5	(发布机构:代码系统:代码)用 HL-7 角色编码填充	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是
HcOrganization	1.0.21091.2.3.1	用于指明组织的组织标识名	标识名	标识名匹配	是

对属于非正规卫生保健专业人员的雇员,将会为每个雇佣该个体的卫生保健组织提供示例。正规的卫生保健专业人员则采用 8.3.1 中提到的 HCOrganizationalRole 表达。

8.2 组织标识

8.2.1 概述

各种组织应该被一个包含组织特定信息的对象类所表达。这种特定信息应包括执行卫生保健管理和临床功能所要的全部变量。下列组织的类型应在目录内表达:

a) 正规卫生保健组织;

b) 付款方;

c) 支持组织;

d) 管理机构。

为适应行业伙伴对卫生保健的特定需求的,上述每种组织类型都可能需要进一步特例化定。例如,对付款方可能规定包含国家付款方标识号码;雇主可能包括国家雇主标识号码;小型的内科医师诊所应被视作正规卫生保健组织,以便于容纳相关办公室职员。

8.2.2 正规的卫生保健组织

对象类:HCRegulatedOrganization

上级对象类:Organization

对象标识符:1.0.21091.1.4

对象类类型:结构化

必选属性:见表 9

可选属性:见表 10

表 9 HCRegulatedOrganization 的必选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcIdentifier	1.0.21091.2.0.1	卫生保健标识符。发布机构可以是雇主(发布机构:ID)	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是

表 10 HCRegulatedOrganization 的可选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcSigningCertificate	1.0.21091.2.0.3	针对用于健康交易的用户认可签名证书的公钥和证书	二进制	证书精确匹配和证书匹配	是
HcAttributeCertificate	1.0.21091.2.0.4	用于身份凭证、证书等。采用 P7 格式化的证书填充	二进制	证书精确匹配和证书匹配	是
HcSpecialisation	1.0.21091.2.0.6	(发布机构:代码系统:代码)	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是
EdiAdministrativeContact	1.0.21091.2.0.7	负责 EDI 管理的个体条目	标识名	标识名匹配	是
ClinicalInformationContact	1.0.21091.2.0.8	联系临床问题的个体条目	标识名	标识名匹配	是
HcOrganizationCertificates	1.0.21091.2.0.9	用于卫生保健组织证书的存储	二进制	证书精确匹配和证书匹配	是
HcClosureDate	1.0.21091.2.0.10	组织关闭的日期或组织变更名称/从属关系的日期	日期	广义时间匹配,广义时间序列匹配	否
HcSuccessorName	1.0.21091.2.0.11	继任者的标识名条目	标识名	标识名匹配	是
HcRegisteredName	1.0.21091.2.4.1	实体向卫生保健管理机构注册的合法名称	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是
HcRegisteredAddr	1.0.21091.2.4.2	在监管机构注册的地址,该地址应与 PostalAddress 的结构相同	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是
HcServiceLocations	1.0.21091.2.4.3	提供卫生保健服务的卫生保健组织	标识名	标识名匹配	是

8.2.3 付款方组织

对象类:HCPayer

上级对象类:Organization

对象标识符:1.0.21091.1.5

对象类类型:结构化

必选属性:见表 11

可选属性:见表 12

表 11 HCPayer 的必选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcIdentifier	1.0.21091.2.0.1	卫生保健标识符 发布机构可以是雇主(发布机构:ID)	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是

表 12 HCPayer 的可选属性

属性	对象标识符	描述	句法	匹配规则	多值
HcSigningCertificate	1.0.21091.2.0.3	针对用于健康交易的用户认可签名证书的公钥和证书	二进制	证书精确匹配和证书匹配	是
HcAttributeCertificate	1.0.21091.2.0.4	用于身份凭证、证书等。采用 P7 格式化证书填充	二进制	证书精确匹配和证书匹配	是
EdiAdministrativeContact	1.0.21091.2.0.7	负责 EDI 管理的个体的条目	标识名	标识名匹配	是
ClinicalInformationContact	1.0.21091.2.0.8	联系临床问题的个体的条目	标识名	标识名匹配	是
HcOrganizationCertificates	1.0.21091.2.0.9	用于存储卫生保健组织证书。这些证书将用于与组织或组织部门的安全通信,而不是与组织内的具体个体的通信	二进制	证书精确匹配和证书匹配	是
HcClosureDate	1.0.21091.2.0.10	组织关闭的日期或组织变更名称/从属关系的日期	日期	广义时间匹配 广义时间序列匹配	否
HcSuccessorName	1.0.21091.2.0.11	接任者进入的标识名	标识名	标识名匹配	是
HcPayerProductID	1.0.21091.2.5.1	分配机构的名称:付款方计划:ID	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是

8.2.4 支持性组织

对象类:HCSupportingOrganization

上级对象类:Organization

对象标识符:1.0.21091.1.6

对象类类型:结构化

必选属性:见表 13

可选属性:见表 14

表 13 HCSupportingOrganization 的必选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcIdentifier	1.0.21091.2.0.1	卫生保健标识符。发布机构可以是雇主(发布机构:ID)	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是

表 14 HCSupportingOrganization 的可选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcSigningCertificate	1.0.21091.2.0.3	用于健康交易的在身份凭证上签字的用户的抗抵赖的公钥和证书	二进制	证书精确匹配和证书匹配	是
HcAttributeCertificate	1.0.21091.2.0.4	用于身份凭证、证书等。采用 P7 格式化证书填充	二进制	证书精确匹配和证书匹配	是
EdiAdministrativeContact	1.0.21091.2.0.7	负责 EDI 管理的个体的条目	标识名	标识名匹配	是
ClinicalInformationContact	1.0.21091.2.0.8	联系临床问题的个体的条目	标识名	标识名匹配	是
HcOrganizationCertificates	1.0.21091.2.0.9	用于存储卫生保健组织证书	二进制	证书精确匹配和证书匹配	是
HcClosureDate	1.0.21091.2.0.10	组织关闭的日期或组织变更名称/从属关系的日期	日期	广义时间匹配 广义时间序列匹配	否
HcSuccessorName	1.0.21091.2.0.11	接任者进入的标识名	标识名	标识名匹配	是

8.3 角色、工作职责和分组

8.3.1 组织化角色个体

这是个体雇员或订约人的组织定义的工作职责。在一个组织内部,一个个体可以承担一项或多项工作职责。例如,医院内的一名医师既可以作为临床工作者同时也可以作为管理工作者,针对每项工作职责可能会有不同的联系信息。因此在此例中,将临床通信指向不同于管理通信的存储单元是较为适合的。为了使一个单一标识能够在一个或多个组织中占据多项工作职责,其模式应包括一个不带唯一标识符(UID)的对象类,含有一个标识名类型为角色乘员(Role Occupant)的属性。

应注意到此模式对象与 Role(角色)不同,为其命名如此,目的在于保持与概念 OrganizationalRole(组织化角色)中表达的对象类的一致性。

对象类:HCOrganizationalRole

上级对象类:OrganizationalRole

对象标识符:1.0.21091.1.7

对象类类型:结构化

必选属性:没有附加的必选属性被指定

可选属性:见表 15

表 15 HCOrganizationalRole 的可选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcAttributeCertificate	1.0.21091.2.0.4	用于身份凭证、证书、教育程度等。采用 P7 格式化证书填充	二进制	证书精确匹配和证书匹配	是
HcRole	1.0.21091.2.0.5	(发布机构:代码系统:代码)工作特定角色。采用 HL-7 定义的角色填充	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是
mail	0.9.2342.19200300.100.1.3	在此角色下用于通信的电子邮箱地址	IA5String	字符串忽略 IA5String 或 caseExactIA5 字符串	是
HcResponsibleParty	1.0.21091.2.7.1	人员或对此条目负责的 HCOrganizationalRole(医务工作者、法律审查、合约雇员、雇员)的标识名	标识名	标识名匹配	是

8.3.2 卫生保健标准角色

Role 是 Group(组)的一种特殊类型,旨在表达卫生保健中的多种角色类型,这些角色应当被限定为经过标准定义的。这些角色的成员用组织化角色个体的 DN 来标识。这些角色是涉及 SSL 基于证书鉴别的目录服务的应用的访问控制定义的基础。这些角色也可被临床应用所引用,从而这些临床应用可以基于用户的角色来限制某些功能。

对象类:HCStandardRole

上级对象类:GroupOfNames

对象标识符:1.0.21091.1.8

对象类类型:结构化

必选属性:没有附加的必选属性被指定

可选属性:见表 16

表 16 HCStandardRole 的可选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcRole	1.0.21091.2.0.5	(发布机构:代码系统:代码)	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是
HcRoleValidTime	1.0.21091.2.0.12	用户能够以这个角行动的 GMT 格式时间	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是
HcRoleLocationRestriction	1.0.21091.2.0.13	定位限制,角色仅在这个位置是有效(即仅从急诊、从 IP 地址等)	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是

8.3.3 本地角色

本地角色服务于标准中未定义的组织定义的群。大多数访问控制需求应基于标准的角色。如果角色不足以满足访问控制的需求时，群组应当是有效的，以满足这些特定需求。

对象类：HCLocalRole

上级对象类：GroupOfName

对象标识符：1.0.21091.1.9

对象类类型：结构化

必选属性：没有附加的必选属性被指定。

可选属性：见表 17

表 17 HCLocalRole 的可选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcRole	1.0.21091.2.0.5	（发布机构：代码系统：代码）	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是
HcRoleValidTime	1.0.21091.2.0.12	用户能够以这个角色行动的 GMT 格式时间	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是
HcRoleLocationRestriction	1.0.21091.2.0.13	定位限制，角色仅在这个位置是有效（即仅从急诊、从 IP 地址等）	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是

8.3.4 编码型参考

卫生保健需利用许多编码型参考文件。目录技术能够使健康信息管理应用所使用的这种信息的通信变得更加容易。编码型参考信息本身被存储为编码的连接值和 HcReferenceDescription 属性中的相关描述。以下属性构成了一种新的卫生保健特定对象类：

对象类：HCCodedReference

上级对象类：Top

对象标识符：1.0.21091.1.10

对象类类型：辅助

必选属性：见表 18

可选属性：见表 19

表 18 HCCodedReference 的必选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcIssuingAuthority	1.0.21091.2.10.1	对编码场景负责的机构	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是
HcReferenceEffectiveDate	1.0.21091.2.10.2	参考词汇有效或曾经有效的日期	日期	广义时间匹配 广义时间序列匹配	否

表 18（续）

属性	对象标识符	描述	语法	匹配规则	多值
HcReferenceDescription	1.0.21091.2.10.3	连接值:参考编码:描述	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是

表 19 HCCodedReference 的可选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcVocabularyOID	1.0.21091.2.10.4	被使用的卫生保健词汇的对象标识符	对象标识符	对象标识符匹配	否
HcReferenceDateOfIssue	1.0.21091.2.10.5	参考词汇被发布的日期	日期	广义时间匹配 广义时间序列匹配	否
HcReferenceInvalidDate	1.0.21091.2.10.6	参考词汇有效或曾经有效的日期	日期	广义时间匹配 广义时间序列匹配	否
HcReferenceVersion	1.0.21091.2.10.7	编码型参考文件的版本号码	目录字符串	字符串大小写忽略匹配,子字符串大小写忽略匹配	是

8.3.5 设备特征管理

设备支持应依据 DICOM 附录 67[1]和 ISO 有关设备规范中的描述,并结合下述附加内容以支持特征管理。

对象类:HCDevice

上级对象类:Top

对象标识符:1.0.21091.1.11

对象类类型:辅助

必选属性:这些属性都不是强制性的。

可选属性:见表 20

表 20 HCDevice 的可选属性

属性	对象标识符	描述	语法	匹配规则	多值
HcDeviceIssuedTo	1.0.21091.2.11.1	已被分发到设备的个体的标识名	标识名	标识名匹配	否
HcDeviceDateOfIssue	1.0.21091.2.11.2	设备被分发给接受者的日期	日期	广义时间匹配 广义时间序列匹配	否
HcDeviceDateRecalled	1.0.21091.2.11.3	设备被召回的日期	日期	广义时间匹配 广义时间序列匹配	否
HcDeviceDateRetrieved	1.0.21091.2.11.4	设备被恢复的日期	日期	广义时间匹配 广义时间序列匹配	否
HcDeviceCertificate	1.0.21091.2.11.5	所发行的设备证书	二进制	证书精确匹配和证书匹配	是

表 20（续）

属性	对象标识符	描述	语法	匹配规则	多值
HcDeviceTracking Number	1.0.21091.2.11.6	（发行者：号码）分配到设备的跟踪号码	目录字符串	字符串大小写忽略匹配，子字符串大小写忽略匹配	是
HcDevicePhone	1.0.21091.2.11.7	分配给设备电话号码（如：PDA）	电话号码	电话号码匹配和电话字号码匹配	是

9 标识名

9.1 概述

标识名是条目的名称，由该条目的 RDN 序列及其各上层条目构成。相对标识名（RDN）是一个或多个属性及值配对的集合，每个配对都匹配该条目一个不同的显著属性值。

根据标识名所用属性搜索目录这种误解很常见。由于标识名仅是目录的一个唯一标识符，不能以此为依据进行检索；相反，应根据条目本身的属性类型和值配对搜索条目。

9.2 相对标识名

9.2.1 概述

相对标识名（RDN）经常是 UID 或通用名。由于我们希望在目录内表达多种概念，故在卫生保健领域内建立起通用的唯一命名约定尤为重要。这种唯一的 RDN 应由发布机构名称和标识符连接组成，根据 WG3 对名称间隔的规定，采用“:”作为分隔符，例如：

ID=issuing_authority_name:ID

对卫生保健专业人员来讲，发布机构被认为是拥有管理卫生保健专业人员资格证书的正规机构。这就需要每个国家或管辖区域对代表国家、州/省和临床管辖范围（如医师、牙医、药剂师）的认证机构都有一个标识名，这些机构都应维护其唯一标识系统。链接时，如需要分隔符，则用“.”为分隔符。

9.2.2 卫生保健专业人员

9.2.2.1 目录标识符

对于卫生保健专业人员，目录标识符应能表明专业人员的：

a） 多种职业执照；

b） 多个从业场所。

9.2.2.2 发布机构标识符（UID）

为表明多个正规职业和从业场所可能会与同一个卫生保健专业人员有所关联，UID 组成应是：

UID=发布机构标识符：国家/地区专业标识符

这确实可能会在健康目录内造成同一个体多种实例的情况，但是由于健康标识是卫生保健提供中用户交互不可缺少的部分，因此将个体表述为在任何时间由特定监管机构管理并依照该机构管理条例而行为活动是适当的。

9.2.2.3 通用名称

通用名称（CN）应维持个体或组织依法登记的名称。为确保通用名称的唯一性及个体查询的易用性，卫生保健专业人员的通用名称应由如下组成：

姓、名、UID

其中 UID 的组成见 9.2.2.2。

针对具有多姓的情况，通用名称应首先列出被选择的姓。如果由政府发布的个体标识中名称表达存在差异，则所用名称应与医疗管理机构所列名称相同。

在通用名称的表达中不应带有头衔(例如：医学博士、兽医学博士)。但是如小(Jr.)、老(Sr.)、二世(II)等区分同一家族名(或家族内名字相似)个体的称谓应予以保留。

9.2.2.4 多值的通用名称的使用

附加的通用名称值可用来表达所代表个体的首选名称和常用名称。

9.2.3 健康消费者

9.2.3.1 表达

健康消费者可以被包括匿名标识在内的众多标识系统表达。这些标识符可以包括区域标识符，MPI 以及区域管理系统。个体可以在大量的目录对象实例中所表达。对消费者搜索的条件应该包括 PIDS 标识属性列表。

9.2.3.2 UID

多个组织和实体需要在各自区域与地点内表达消费者，UID 的组成应是：

UID=发布机构标识符：国家/地区/组织/患者/人员标识符

这确实可能会造成健康目录中同一个体多种实例的情况，但是由于健康标识是在卫生保健接受中用户交互不可缺少的部分，所以按照其在特定的标识发放机构下的活动来表达个体是适当的。这就必然(或必定)要求支持患者标识符定位服务，就这点而言，对象类中应含有支持此类搜索性能的变量。在消费者匿名的情况下，这些变量和标识符可以是是可逆的或不可逆的假名和编码值。为能够通过家庭地址进行辨别，ID 编号的住所标识符可以用作通用名称的组成部分或作为 HCConsumer 对象类中的可选变量。

9.2.3.3 通用名称

通用名称应保留个体或组织的合法名称。为了保证通用名称的唯一性并便于进行个体查询，通用名称的组成应该是：

姓、名，UID

UID 的组成见 9.2.3.2。

在通用名称的表达中不应带有头衔(例如，医学博士、兽医学博士)。然而，为了区分同一家族内有相同名字的个体的称号，如小(Jr.)、老(Sr.)、二世(II)等应保留。

9.2.3.4 多值的通用名称的使用

附加的通用名称值可用来表达所代表个体的首选名称和常用名称。

9.2.4 组织

9.2.4.1 UID

组织 UID 的组成应该是：

UID=发布机构标识符：国家/地区标识符

这确实可能会在健康目录内造成同一组织多种实例的情况，但是由于健康标识是在卫生保健接受中用户交互不可缺少的部分，因此将组织表述为在特定的标识发放机构管理下行为活动是适当的。

9.2.4.2 通用名称

通用名称应保留组织当前的合法名称。

9.2.4.3 组织合法名称的保存

在发生业务从属关系变更、名称变更和其他继承实例的情况下，接任者应通过新实体条目的通用名称与目前组织合法名称被标明。在停业的情况下，关闭日期应由 HcClosureDate 表达。

9.2.5 角色/工作

9.2.5.1 概述

由于一个 UID 在卫生保健社团内可以有多个工作或从属关系，我们应考虑将此种类型的对象类作为通用名称的键控，从而使用通用名称作为此概念内任何对象类的相对标识名。角色的相对标识名就成为通用名称。此名称应基于 HCStandardRole 案例的标准化结构角色进行构建。

9.2.5.2 HCOrganizationalRole(卫生保健组织角色)

对象类 HC 用以表达代表关系的结构化角色和工作头衔。对象类 HC 不用于支持优先权管理，而是用于工作特定的联系信息和属性，它的命名格式是：

mailto:CN. job_function@organization_domain_name

此处的 CN 是个体的 CN，organization_domain_name 为该组织的域名，采用对象类 OrganizationalRole。Job_function 基于组织结构和职位，不被视为国际标准化候选，但不排除使用基于标准的名称。工作特定属性证书可填充在此对象类中。

9.2.5.3 HCstandardRole(卫生保健标准角色)

此角色是基于标准的卫生保健结构化角色，可用于基于目录的特权组的管理。其命名格式是：

standardRole@organization_domain_name

其中，standardRole 是结构化角色的标准名称，organization_domain_name 是组织的域名，那些基于标准的角色都隶属于该组织。其命名也可以是：

standardRole@Locality

如果适用于地区(如州)，那么此处 standardRole 为结构化角色的标准名称。

9.2.5.4 HClocalRole(卫生保健本地角色)

此角色是非基于标准的 GroupOfNames 规范，用于新的、非标准的、区域或本地定义的角色。这其命名格式应该是：

localRole@organization_domain_name

其中 localRole 为结构角色的名称，organization_domain_name 是组织的域名，那些非基于标准的角色都隶属于该组织。其命名也可以是：

localRole@Locality

如果适用于地区(如州)，那么此处 localRole 为结构化角色的标准名称。

附 录 A
（资料性附录）
卫生保健目录场景

A.1 引言

本附录介绍了一系列代表目录服务的核心业务和技术需求的高层卫生保健案例或场景，其目录服务支持卫生保健行业大范围的跨区域服务。

本附录首先介绍了通用要求，说明了基本的保密和安全规则以及卫生保健行业的基本需求。而后，本附录详细说明了如下场景：

a) 对场景的描述，或需要卫生保健目录服务的情形；

b) 目录服务应满足的、产生业务和技术需求的方案。

A.2 场景的解释

A.4 所描述的场景表明了目录服务在卫生保健中是如何被应用的。每个场景均意在描述卫生保健目录服务潜在和可能的应用，以便提供临床、管理和安全方面的支持，从而确保电子健康信息共享的安全。由于卫生保健遍及世界的分布性质，加之需要不同人员和组织都能积极合作来提供无缝的卫生保健，任何目录服务均能够进行交叉操作并支持不同的卫生保健设置就显得尤为重要，这些设置包括基于保健的医院和社区的设置以及公立和私立医院的设置。

A.3 在卫生保健场景中举例说明的服务

表 A.1 卫生保健场景与服务

服 务	场景编号															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
专业人员关注的临床护理支持		X	X	X	X	X	X	X				X	X	X	X	X
健康信息管理与行政支持	X	X	X			X	X				X	X	X			
健康信息安全支持	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X
消费者健康支持		X			X			X				X	X			X
个人联系卫生保健信息	X	X	X	X	X	X		X			X	X	X	X	X	X
系统联系卫生保健信息	X	X					X					X	X			
组织联系卫生保健信息			X	X		X		X			X	X	X			
检索用于加密的公钥	X	X	X	X	X	X	X	X			X	X	X			
签名验证			X	X	X	X	X					X	X		X	
CRL 检查			X	X	X	X	X	X			X	X	X	X	X	X
鉴定								X				X	X	X		X
生物测定参考								X								
证明/发布支持									X	X	X					

所列举的场景

1 声明处理	9 CA 证书处理支持
2 实验室医嘱和结果处理	10 属性证书处理支持
3 电子处方	11 身份凭证处理支持
4 临床实践指南的群播	12 在其他国家进行的患者医护
5 疾病状态管理指南的群播	13 来自另一个国家的转诊证明
6 患者转诊	14 远程访问临床应用
7 患者纵向病史(MPI)	15 特权委托
8 例行疾病状态管理通信	16 移动用户鉴别

A.4 场景描述

A.4.1 声明处理

A.4.1.1 场景描述

卫生保健专业人员的计费系统处理一批声明并按照电子数据交换规范中的适当条款生成声明文件。该系统执行目录查找动作来识别接收系统的通信信息和接收者的公钥,相关信息被加密并发送给接收者等待处理。系统生成一个供追加跟踪的错误报告。声明处理系统在目录中查找卫生保健专业机构的 EdiAdministrativeContact 联系信息,并在电子邮件系统中检索联系和公共证书信息。一封加密的电子邮件消息将被发送给卫生保健专业联系组,请求卫生保健专业人员回馈识别和支持文档。卫生保健专业人员将包括患者信息的适当文档附在加密的电子邮件中作为对付款方的答复,同时,在目录中查找付款方的联系信息和加密证书。

A.4.1.2 运用的目录服务

本场景运用了个人和系统联系信息、群组间电子邮件以及检索加密所用公钥等目录服务。

A.4.2 实验室医嘱和结果处理

A.4.2.1 场景描述

卫生保健专业人员发送一封带有实验室服务医嘱并加密后的电子邮件给另一位卫生保健专业人员,需要在目录中查找实验室联系和通信信息的公钥。临床医师使用其个人的私钥签署上述请求,实验室为患者执行该请求的试验,并通过电子邮件或直接报告给提出请求的卫生保健专业人员,要使用目录查找正确的联系信息和加密所需的公钥。试验结果由实验室人员和/或系统酌情签署。卫生保健专业人员发送一封含有试验结果、签名并加密的电子邮件给患者,需要依据目录来标识联系信息和加密密钥。

A.4.2.2 运用的目录服务

本场景运用了个人和系统联系信息、加密所用公钥检索等目录服务。

A.4.3 电子处方

A.4.3.1 场景描述

临床医师开具处方并用其私人签名密钥签署。为避免潜在的专业人员困窘,在应用证书之前需要首先在 CRL 中核查该医生证书的撤销情况。经签名并加密后的处方被发送给药房,组织的联系信息和密码证书信息通过 LDAP 查找而获得。本地环境中药剂师的鉴别使本地系统可将解密的消息提交给用户,并通过 LDAP 查找利用公钥验证签名与数据内容。比对目录检查签名证书的撤销情况,并保障

证书是通过一个可信的CA发布的。如果过程中使用了在线证书状态协议的服务，其联系信息的标识是通过目录来鉴定的。

A.4.3.2 运用的目录服务

本场景运用了个人和组织联系信息、加密和签名鉴别的公钥检索以及CRL查验等目录服务。

A.4.4 临床实践指南的群播

A.4.4.1 场景描述

儿童期免疫临床实践指南的修订版被作为广播消息发布给每个儿科医师。此处，目录被用来标识包括所有儿科医师的群。此消息是经过签名的，目录被接收方用来验证签名的真实性和签名者证书的有效状态。

A.4.4.2 运用的目录服务

本场景运用了个人联系信息、加密和签名验证公钥检索、组织查找及CRL查验等目录服务。

A.4.5 疾病状态管理指南的群播

A.4.5.1 场景描述

疾病状态管理指南的修订版已被公布。临床资源识别需参考该指南的患者，使用目录来确定患者联系信息和公钥，从而对同意接收此类消息的患者启动消息广播。发送给患者的电子邮件消息是被签名和加密过的。患者的电子邮件系统会按照目录来验证签名人的证书，并确认此签名。

A.4.5.2 运用的目录服务

本场景运用了个人联系信息、加密和签名鉴别的公钥检索以及CRL查验等目录服务。

A.4.6 患者转诊

A.4.6.1 场景描述

患者转诊应用与目录进行交互，用于鉴别获得患者转诊信息的卫生保健专业人员。在接受组织的卫生保健专业人员既作为管理人员同时也是临床医生。当电子邮件中出现objectClass=HcOrganizationalRole，和开业医生的标识名为roleOccupant以及通用名称包含job_function@organization等情况时，需要查询健康目录。另外也可以执行一个双路查询，首先检索开业医生在该组织内的全部工作职能，其次获取那些工作职能的联系信息。通信信息和加密证书经LDAP查询和具体应用来鉴定，此处应用包括发送签名过的通知和护理说明给患者转诊的接收方。接收患者转诊的组织通过目录和CRL来验证签名和证书的有效性。

A.4.6.2 运用的目录服务

本场景运用了个人联系信息、加密和签名验证公钥检索、组织查找及CRL查验等目录服务。

A.4.7 患者纵向病史(MPI)

A.4.7.1 场景描述

患者求诊并要求得到初级、非卧床或紧急护理。由患者签署同意查阅医疗记录的授权。相关签名和数据内容是通过LDAP查找对照公钥进行验证的，证书需要经过撤销检验。

患者纵向病史应用从目录中标识MPI数据来源，同时也从可获得的资源记录中的细节进行标识。通信信息和加密证书通过应用的LDAP查询被标识，对细节的请求被发送至ClinicalInformationContact。

此外，当没有数字身份凭证的患者来求诊时，通过对已知的PIDS数据进行目录查询可识别患者的MPI定位符，从而可标示其MPI资源。在征得患者同意后，可从患者的MPI资源中检索所需信息。

A.4.7.2 运用的目录服务

本场景运用了 MPI 定位信息目录服务，并使用目录比较目录中 CRL 的签名验证对患者同意的身份凭证进行验证。目录还用于检索加密公钥和通信信息。

A.4.8 例行疾病状态管理通信

A.4.8.1 场景描述

患者预定疾病状态管理计划。患者使用用户 ID 和密码或者数字证书进行验证使用定期程序来登录例行程序度量，CRL 被用于确证目的。次级生物测定也可被提供以保障患者标识。提醒患者即将/已错过预约或其他类似的警报，由自动化系统或执行案例考察的个体生成，加密后发送给患者。通信信息和加密证书由应用通过 LDAP 查询所鉴定。

A.4.8.2 运用的目录服务

本场景运用了个人联系信息、用户鉴别、生物测定服务参照、加密所需公钥的检索和 CRL 检验等目录服务。

A.4.9 CA 证书处理支持

A.4.9.1 场景描述

卫生保健认证机构所使用的目录包含 CA 层级和 CA 联系信息。由认证机构向卫生保健个人颁发证书。证书的主体及其所携带的属性和卫生保健模式信息一同被输入目录。CA 将公钥/证书登入目录，用来签名、鉴别和加密密钥。由 CA 负责更新目录中所存储的 CRL。

A.4.9.2 运用的目录服务

本场景中，目录用于存储证书持有者标识和联系信息。也用于存储和维护签名用户的证书、CA 联系信息和 CRL。

A.4.10 属性证书处理支持

A.4.10.1 场景描述

该目录用于包含 AA 层级和 AA 联系信息的卫生保健属性机构。由属性机构对卫生保健个人颁发属性证书。在目录中用证书所保存的属性对证书的主体进行更新。AA 将属性证书登入签署人条目或签署人 OrganizationalRole 所属的目录。AA 负责更新存储在目录中的 CRL。

A.4.10.2 运用的目录服务

该目录用于存储和维护签署人证书、AA 联系信息和 CRL。

A.4.11 身份凭证处理支持

A.4.11.1 场景描述

从事认可工作的卫生保健组织或管理机构从目录中查找教育信息和联系信息。将具有属性证书信息形式的认证登入。

A.4.11.2 运用的目录服务

该目录用于存储和维护与卫生教育相关的教育凭证。

A.4.12 在其他国家进行的患者医护

A.4.12.1 场景描述

患者在国外逗留期间患病。患者联系到一位当地的医师。医师使用比较本地目录服务验证的本地证书凭证和比较 CRL 所检查撤消状况向本地医疗机构进行认证。医师通过加密的消息向患者祖国的初级医护医师查询患者的病史信息，并向该国目录提供证书凭证。相关凭证和 CRL 通过源目录进行检验。

A.4.12.2 运用的目录服务

本场景运用了个人联系信息、加密和签名认证所需公钥的检索、组织查找和 CRL 检验等目录服务。

A.4.13 来自另一个国家的转诊证明

A.4.13.1 场景描述

正在国外逗留的患者要求本国的初级保健医师提供转诊证明。初级保健医生向本地目录进行认证，请求服务于患者所在地的外国目录的专业信息。一旦一名临床医生被标识，转诊医师使用由本地目录验证的凭证向消息应用进行认证。这些凭证用于向指定的临床医生生成转诊消息，用他/她的签名证书证实信息的内容。接收方的凭证通过 CRL 进行验证，发送医师的凭证通过 CRL 检查进行验证。

A.4.13.2 运用的目录服务

本场景运用了个人联系信息、加密和签名认证所需公钥的检索、组织查找和 CRL 检验等目录服务。

A.4.14 远程访问临床应用

A.4.14.1 场景描述

某应用被配置为，需要来自被信任的 CA 的 SSL3 客户端认证证书。用户为进入应用环境的认证提供令牌存储证书。证书映射将所提供的证书链接至用户目录条目，完成用户标识。通过 LDAP 查询对所认证用户的角色进行标识。通过作为适当的群成员的个体或证书属性断言，基于角色访问控制的决策根据在目录中所注册的角色制定。证书的撤消状态被检查，用户被允许依照在信赖应用中被指定的特权进行访问。

A.4.14.2 运用的目录服务

本场景中，目录用于鉴别基于角色的访问控制的角色信息，也用于对 CRL 的检查。

A.4.15 特权委托

A.4.15.1 场景描述

在特定条件下经由属性证书，卫生保健专业人员托付机构来代表他们的利益。通过查询目录可以验证特权路径和身份凭证撤消状态。

A.4.15.2 运用的目录服务

本场景中，目录用于验证授权身份凭证，并经由 CRL 验证撤消状态。

A.4.16 移动用户鉴别

A.4.16.1 场景描述

用户为移动环境的应用提供用于鉴别的软件证书。证书的撤消状态被检查。该应用请求对照目录进行第二次口令验证。

A.4.16.2 运用的目录服务

本场景中，目录用于用户鉴别、CRL 检查和口令验证。

附 录 B
（资料性附录）
引用的对象类

B.1 inetOrgPerson

对象类:inetOrgPerson

上级对象类:organizationalPerson

对象标识符:2.16.840.1.113730.3.2.2

对象类的类型:结构化

必选属性:见表 B.1

可选属性:见表 B.2

表 B.1 inetOrgPerson 的必选属性

属性	对象标识符	描述	语法	匹配规则	多值
SN	2.5.4.4	姓	目录字符串	字符串大小写忽略匹配	是
CN	2.5.4.3	通用名:RFC2256:名称属性的通用父型	目录字符串	字符串大小写忽略匹配	是

表 B.2 inetOrgPerson 的可选属性

属性	对象标识符	描述	语法	匹配规则	多值
description	2.5.4.13	描述性的信息	目录字符串	字符串大小写忽略匹配	是
seeAlso	2.5.4.34	RFC2256: 标识名属性的通用父型	标识名	标识名匹配	是
telephoneNumber	2.5.4.20	RFC2256:电话号码	电话号码	电话号码匹配	是
userPassword	2.5.4.35	RFC2256/2307:用户的口令	八位字节串	八位字节串匹配	是
title	2.5.4.12	工作头衔(与人员头衔相对。)	目录字符串	字符串大小写忽略匹配	是
ou	2.5.4.11	主要联合组织的标识名	目录字符串	字符串大小写忽略匹配	是
preferredDelivery-Method	2.5.4.28	RFC2256:首选交付模式	1.3.6.1.4.1.1466.115.121.1.14		否
st	2.5.4.8	州或省	目录字符串	字符串大小写忽略匹配	是
telexNumber	2.5.4.21	电报号码	电报号码		是
l	2.5.4.7	所在地名称	目录字符串	字符串大小写忽略匹配	是

表 B.2（续）

属性	对象标识符	描述	语法	匹配规则	多值
physicalDelivery OfficeName	2.5.4.19	实际交付办事处的名称	目录字符串	字符串大小写忽略匹配	是
postalCode	2.5.4.17	邮政编码	目录字符串	字符串大小写忽略匹配	是
internationalISDNNumber	2.5.4.25	RFC2256：国际综合业务数字网(ISDN)编码	数字串	数字串匹配	是
x121Address	2.5.4.24	RFC2256：X.121 地址	数字串	数字串匹配	是
registered Address	2.5.4.26	RFC2256：邮政地址	邮政地址	字符串大小写列表忽略匹配	是
street	2.5.4.9	RFC2256：对象的街道地址	目录字符串	字符串大小写忽略匹配	是
postalAddress	2.5.4.16	RFC2256：邮政地址	邮政地址	字符串大小写列表忽略匹配	是
facsimileTelephone Number	2.5.4.23	RFC2256：传真电话号码	传真电话号码		是
teletexTerminal Identifier	2.5.4.22	RFC2256：电报终端标识符	1.3.6.1.4.1.1466.115.121.1.51		是
postOfficeBox	2.5.4.18	RFC2256：邮政信箱	目录字符串	字符串大小写忽略匹配	是
destinationIndicator	2.5.4.27	RFC2256：目标指示符	可印刷字符串	字符串大小写忽略匹配	是
userCertificate	2.5.4.36	RFC2256：X.509 用户证书使用；二进制的	证书		是
uid	0.9.2342.19200300.100.1.1	RFC1274：用户标识符	目录字符串	字符串大小写忽略匹配	是
homePostalAddress	0.9.2342.19200300.100.1.39	RFC1274：家庭邮政地址	邮政地址	字符串大小写列表忽略匹配	是
employeeType	2.16.840.1.113730.3.1.4	RFC2798：个人受雇佣类型	目录字符串	字符串大小写忽略匹配	是
preferredLanguage	2.16.840.1.113730.3.1.39	RFC2798：个人擅长的书面或口头语言	目录字符串	字符串大小写忽略匹配	否
mail	0.9.2342.19200300.100.1.3	RFC1274：RFC822 邮箱	IA5 字符串	字符串大小写忽略 IA5 匹配	是

表 B.2（续）

属性	对象标识符	描述	语法	匹配规则	多值
homePhone	0.9.2342.19200300.100.1.20	RFC1274:家庭电话号码	电话号码	电话号码匹配	是
roomNumber	0.9.2342.19200300.100.1.6	RFC1274:房间号码	目录字符串		是
x500UniqueIdentifier	2.5.4.45	RFC2256:X500 唯一性标识符	位串	位串匹配	是
employeeNumber	2.16.840.1.113730.3.1.3	RFC2798:数字化标识某组织内的某个雇员	目录字符串	字符串大小写忽略匹配	否
photo	0.9.2342.19200300.100.1.7	RFC1274:照片（G3 传真）	1.3.6.1.4.1.1466.115.121.1.23		是
businessCategory	2.5.4.15	RFC2256:商业类别	目录字符串	字符串大小写忽略匹配	是
pager	0.9.2342.19200300.100.1.42	RFC1274:寻呼电话号码	电话号码	电话号码匹配	是
o	2.5.4.10	组织名称:RFC2256:名称属性的通用父型	目录字符串	字符串大小写忽略匹配	是
jpegPhoto	0.9.2342.19200300.100.1.60	RFC2798:JPEG 格式的图像	JPEG		是
secretary	0.9.2342.19200300.100.1.21	RFC1274:秘书的标识名	标识名	标识名匹配	是
audio	0.9.2342.19200300.100.1.55	RFC1274:音频（u-law）	音频		是
userPKCS12	2.16.840.1.113730.3.1.216	RFC2798: PKCS # 12 PFX PDU 用于个人识别信息交换	二进制的		是
displayName	2.16.840.1.113730.3.1.241	RFC2798:显示输入时所用的首选名称	目录字符串	字符串大小写忽略匹配	否
mobile	0.9.2342.19200300.100.1.41	RFC1274:移动电话号码	电话号码	电话号码匹配	是
labeledURI	1.3.6.1.4.1.250.1.57	RFC2079:带有可选标记的统一资源标识符	目录字符串	字符串大小写精确匹配	是
carLicense	2.16.840.1.113730.3.1.1	RFC2798:RFC2798:汽车牌照	目录字符串	字符串大小写忽略匹配	是
givenName	2.5.4.42	RFC2256:名称属性的通用父型	目录字符串	字符串大小写忽略匹配	是

表 B.2（续）

属性	对象标识符	描述	语法	匹配规则	多值
manager	0.9.2342.19200300.100.1.10	RFC1274:经理的标识名	标识名	标识名匹配	是
userSMIMECertificate	2.16.840.1.113730.3.1.40	RFC2798:PKCS#7 用于支持 S/MIME 的已标记数据	二进制的		是
initials	2.5.4.43	RFC2256:名称属性的通用父型	目录字符串	字符串大小写忽略匹配	是
departmentNumber	2.16.840.1.113730.3.1.2	RFC2798:识别组织内部的部门	目录字符串	字符串大小写忽略匹配	是

B.2 Organization

对象类:organization

上级对象类:Top

对象标识符:2.5.6.4

对象类的类型:结构化

必选属性:见表 B.3

可选属性:见表 B.4

表 B.3 Organization 的必选属性

属性	对象标识符	描述	语法	匹配规则	多值
o	2.5.4.10	组织名称:RFC2256:名称属性的通用父型	目录字符串	字符串大小写忽略匹配	是

表 B.4 Organization 的可选属性

属性	对象标识符	描述	语法	匹配规则	多值
description	2.5.4.13	描述性的信息	目录字符串	字符串大小写忽略匹配	是
preferredDeliveryMethod	2.5.4.28	RFC2256:首选交付模式	1.3.6.1.4.1.1466.115.121.1.14		否
searchGuide	2.5.4.14	RFC2256:已被增强型搜索向导取代了的搜索向导	1.3.6.1.4.1.1466.115.121.1.25		是
st	2.5.4.8	RFC2256:名称属性的通用父型	目录字符串	字符串大小写忽略匹配	是
businessCategory	2.5.4.15	RFC2256:商业类别	目录字符串	字符串大小写忽略匹配	是
telexNumber	2.5.4.21	电报号码	电报号码		是
l	2.5.4.7	所在地名称	目录字符串	字符串大小写忽略匹配	是

表 B.4（续）

属性	对象标识符	描述	语法	匹配规则	多值
seeAlso	2.5.4.34	RFC2256:标识名属性的通用父型	标识名	标识名匹配	是
telephoneNumber	2.5.4.20	RFC2256:电话号码	电话号码	电话号码匹配	是
physicalDeliveryOffice-Name	2.5.4.19	实际交付办事处名称	目录字符串	字符串大小写忽略匹配	是
postalCode	2.5.4.17	邮政编码	目录字符串	字符串大小写忽略匹配	是
internationalISDNNumber	2.5.4.25	RFC2256:国际综合业务数字网(ISDN)编码	数字串	数字串匹配	是
x121Address	2.5.4.24	RFC2256:X.121 地址	数字串	数字串匹配	是
userPassword	2.5.4.35	RFC2256/2307:用户的口令	八位字符串	八位字符串匹配	是
registeredAddress	2.5.4.26	RFC2256:邮政地址	邮政地址	字符串大小写列表忽略匹配	是
street	2.5.4.9	RFC2256:对象的街道地址	目录字符串	字符串大小写忽略匹配	是
postalAddress	2.5.4.16	RFC2256:邮政地址	邮政地址	字符串大小写列表忽略匹配	是
facsimileTelephoneNumber	2.5.4.23	RFC2256:传真电话号码	传真电话号码		是
teletexTerminalIdentifier	2.5.4.22	RFC2256:电报终端标识符	1.3.6.1.4.1.1466.115.121.1.51		是
postOfficeBox	2.5.4.18	RFC2256:邮政信箱	目录字符串	字符串大小写忽略匹配	是
destinationIndicator	2.5.4.27	RFC2256:对象指示符	可印刷字符串	字符串大小写忽略匹配	是

B.3 OrganizationalRole

对象类:organizationalRole

上级对象类:Top

对象标识符:2.5.6.8

对象类的类型:结构化

必选属性包括:见表 B.5

可选属性包括:见表 B.6

表 B.5 organizationalRole 的必选属性

属性	对象标识符	描述	语法	匹配规则	多值
CN	2.5.4.3	通用名:RFC2256:名称属性的通用父型	目录字符串	字符串大小写忽略匹配	是

表 B.6 organizationalRole 的可选属性

属性	对象标识符	描述	语法	匹配规则	多值
description	2.5.4.13	描述性的信息	目录字符串	字符串大小写忽略匹配	是
ou	2.5.4.11	主要联合组织的标识名	目录字符串	字符串大小写忽略匹配	是
preferredDelivery-Method	2.5.4.28	RFC2256:首选交付模式	1.3.6.1.4.1.1466.115.121.1.14		否
st	2.5.4.8	RFC2256:名称属性的通用父型	目录字符串	字符串大小写忽略匹配	是
telexNumber	2.5.4.21	电报号码	电报号码		是
l	2.5.4.7	所在地名称	目录字符串	字符串大小写忽略匹配	是
seeAlso	2.5.4.34	RFC2256:标识名属性的通用父型	标识名	标识名匹配	是
telephoneNumber	2.5.4.20	RFC2256:电话号码	电话号码	电话号码匹配	是
physicalDeliveryOffice-Name	2.5.4.19	实际交付办事处名称	目录字符串	字符串大小写忽略匹配	是
postalCode	2.5.4.17	邮政编码	目录字符串	字符串大小写忽略匹配	是
roleOccupant	2.5.4.33	RFC2256:标识名属性的通用父型	标识名	标识名匹配	是
internationalISDN-Number	2.5.4.25	RFC2256:国际综合业务数字网(ISDN)编码	数字串	数字串匹配	是
x121Address	2.5.4.24	RFC2256:X.121 地址	数字串	数字串匹配	是
registeredAddress	2.5.4.26	RFC2256:邮政地址	邮政地址	字符串大小写列表忽略匹配	是
street	2.5.4.9	RFC2256:对象的街道地址	目录字符串	字符串大小写忽略匹配	是
postalAddress	2.5.4.16	RFC2256:邮政地址	邮政地址	字符串大小写列表忽略匹配	是
facsimileTelephoneN-umber	2.5.4.23	RFC2256:传真电话号码	传真电话号码		是
teletexTerminalIdenti-fier	2.5.4.22	RFC2256:电报终端标识符	1.3.6.1.4.1.1466.115.121.1.51		是
postOfficeBox	2.5.4.18	RFC2256:邮政信箱	目录字符串	字符串大小写忽略匹配	是
destinationIndicator	2.5.4.27	RFC2256:目标指示符	可印刷字符串	字符串大小写忽略匹配	是

B.4 GroupOfNames

对象类:groupOfNames

上层对象类:Top

对象标识符:2.5.6.9

对象类的类型:结构化

必选属性:见表 B.7

可选属性:见表 B.8

表 B.7 groupOfNames 的必选属性

属性	对象标识符	描述	语法	匹配规则	多值
CN	2.5.4.3	通用名:RFC2256:名称属性的通用父型	目录字符串	字符串大小写忽略匹配	是
member	2.5.4.31	RFC2256:标识名属性的通用父型	标识名	标识名匹配	是

表 B.8 groupOfNames 的可选属性

属性	对象标识符	描述	语法	匹配规则	多值
description	2.5.4.13	描述性的信息	目录字符串	字符串大小写忽略匹配	是
ou	2.5.4.11	主要联合组织的标识名	目录字符串	字符串大小写忽略匹配	是
businessCategory	2.5.4.15	RFC2256:商业类别	目录字符串	字符串大小写忽略匹配	是
owner	2.5.4.32	RFC2256:标识名属性的通用父型	标识名	标识名匹配	是
seeAlso	2.5.4.34	RFC2256:标识名属性的通用父型	标识名	标识名匹配	是
o	2.5.4.10	组织名称:RFC2256:名称属性的通用父型	目录字符串	字符串大小写忽略匹配	是

参 考 文 献

[1] GB/T 5271.8—2001 信息技术 词汇 第8部分:安全(ISO/IEC 2382-8:1998,IDT)

[2] GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分:安全体系结构(ISO 7498-2:1989,IDT)

[3] GB/T 18794.1—2002 信息技术 开放系统互连 开放系统安全框架 第1部分:概述(ISO/IEC 10181-1:1996,IDT)

[4] ISO 22600-2 Health informatics—Privilege management and access control—Part 2: Formal models

[5] ISO/IEC 9594-8 Information technology—Open Systems Interconnection—The Directory: Publickey and attribute certificate frameworks—Part 8

[6] ISO/IEC TR 13335-1:1996 Information technology—Guidelines for the management of IT Security—Part 1: Concepts and models for IT security

[7] ISO/IEC 14516:2002 Information technology—Security techniques—Guidelines for the use and management of Trusted Third Party services

[8] ISO/IEC 15945:2002 Information technology—Security techniques—Specification of TTP services to support the application of digital signatures

[9] ISO 17090 (all parts) Health informatics—Public key Infrastructure

[10] DICOM Supplement 67:2003 Configuration Management

[11] ENV 13608-1 Health informatics—Security for healthcare communication—Part 1: Concepts and terminology

[12] HL7 V3 RIM Reference Information Model

[13] IETF/RFC 3280: 2002 Internet X.509 Public Key Infrastructure Certificate and CRL Profile

[14] IETF/RFC 3647:2003 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[15] ITU-T Recommendation X.509:2000 | ISO/IEC 9594-8:2001 ITU-T Information technology—Open systems Interconnection—The Directory—Public-Key and Attribute Certificate Frameworks

中 华 人 民 共 和 国
国 家 标 准
健康信息学
安全、通信以及专业人员与
患者标识的目录服务
GB/T 25513—2010/ISO/TS 21091:2005
*
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 2.5 字数 74 千字
2011年4月第一版 2011年4月第一次印刷
*
书号:155066·1-42410 定价 36.00元

打印日期:2011年5月12日 F009A