ICS 35.100.01
L 79

中华人民共和国国家标准

GB/T 17969.8—2010/ISO/IEC 9834-8:2005

信息技术　开放系统互连 OSI登记机构操作规程 第8部分:通用唯一标识符(UUID)的生成和登记及其用作ASN.1客体标识符部件

Information technology—Open systems interconnection—Procedures for the operation of OSI registrartion authorities—Part 8:Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 object identifier components

(ISO/IEC 9834-8:2005,IDT)

2011-01-14 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

GB/T 17969 在《信息技术　开放系统互连　OSI 登记机构操作规程》总标题下，分为以下几个部分：

——第 1 部分：一般规程；

——第 3 部分：ISO 和 ITU-T 联合管理的顶级弧下的客体标识符弧的登记；

——第 5 部分：VT 控制客体定义的登记表；

——第 6 部分：应用进程和应用实体；

——第 8 部分：通用唯一标识符(UUID)的生成和登记及其用作 ASN.1 客体标识符部件。

本部分是 GB/T 17969 的第 8 部分。

本部分等同采用国际标准 ISO/IEC 9834-8:2005《信息技术　开放系统互连 OSI 登记机构操作规程　第 8 部分：通用唯一标识符(UUID)的生成和登记及其用作 ASN.1 客体标识符部件》。与 ISO/IEC 9834-8 的等同文本为 ITU-T 建议 X.667。

本部分的附录 A、附录 B、附录 C 和附录 D 为资料性附录。

本部分由全国信息技术标准化技术委员会提出并归口。

本部分起草单位：中国电子技术标准化研究所，北京易华世纪科技发展中心。

本部分主要起草人：徐冬梅、王茜、董挺。

引　言

GB/T 17969 的本部分规定了通用唯一标识符(UUID)的生成和可选登记。

UUID 是一个 16 个八位位组(128 比特)的位组串。16 个八位位组能被解释为一个无符号整数编码,并且所涉及到的整数值能被用作在弧{joint-iso-itu-t uuid(25)}下的 OID 树的弧。这使用户能生成 OID,而无需任何登记规程。

UUID 也被称作全球唯一标识符(GUID),但是该术语在本部分中,不予使用。UUID 最初被用于网络计算系统(NCS)[1],后来被用于开放软件基金会的分布式计算环境(DCE)[2]。ISO/IEC 11578[3]包含了在本部分中规定的某些(但并非全部)UUID 格式的简短定义,在本部分中的规范与所有这些早期规范相一致。

形成 OID 部件的 UUID 都是用 ASN.1 值记法被表示为其整数值的十进制,但是对于所有其他显示目的来说,更常见的是以十六进制数来表示它们,以一个连字符分隔 16 个八位位组 UUID 范围内的不同字段。该表示在本部分中予以定义。

如果按照在本部分中定义的机制之一来生成,或者保证 UUID 不同于公元 3603 年前生成的所有其他 UUID,或者保证 UUID 可能极为不同(取决于所选择的机制)。

不要求集中式机构来管理 UUID,但是要求自我生成的 UUID 的集中登记,并且提供了对 UUID 的自动生成(使用在本部分中定义的算法)和登记。集中生成的 UUID 被保证不同于集中生成的所有其他 UUID。已登记的 UUID 被保证不同于所有其他登记的 UUID。

UUID 能用于多用途,从触发具有极短生命周期的客体,到可靠地标识出跨越网络的每个持久客体,特别是(但不必是)作为 ASN.1 客体标识符(OID)值的或统一资源名称(URN)的一部分。

在本部分中规定的 UUID 生成算法支持很高的分配速率:每机器每秒 10 兆(如果有必要),所以,UUID 也能用作事务 ID。一个资料性附录提供了用 C 语言表示的程序,它将按照本部分来生成 UUID。

为了生成唯一 UUID 规定了三种算法,以使用不同机制来确保唯一性。它们产生了不同版的 UUID。

第 1 个(和最普通)机制产生了所谓的基于时间的版本。这些 UUID 在单台机器中能够以每秒 10 兆的速率来生成。对于在单个计算机系统内生成的 UUID,带有 100 ns 的粒度的,基于协调世界时(UTC)的 60 比特时戳(用作时钟值)被用来保证在约 1600 年周期内的唯一性。对于以同一时戳通过不同系统生成的 UUID,唯一性是通过使用在 GB/T 15629.3 中规定的 48 比特媒体访问控制(MAC)地址来获得的(这是被用作结点值)。(这些地址在大多数已联网的系统上通常早已用到,否则从 IEEE 的 MAC 地址登记机构可获得——见[4]。如果在某一系统上不能用到 UTC 时间,或如果没有 MAC 地址可用,则对于基于时间的版本,规定了生成时钟和结点值的可替换方法。

第 2 个机制产生了基于名称的版本的单个 UUID,其中,密码散列技术被用于根据全球无二义文档(文本)名称来产生 128 比特 UUID 值。

第 3 个机制使用伪随机或真随机数生成来产生在 128 比特值中的大多比特。

第 5 章规定了用于八位位组次序和比特次序命名的和用于规范传输次序的记法。

第 6 章规定 UUID 的结构以及用二进制、十六进制或作为单个整数值对它的表示。

第 7 章和第 8 章规定了分别在 OID 或 URN 中使用 UUID。

第 9 章规定了比较 UUID 的规则,以测试相等性或提供在两个 UUID 之间的排序关系。

第 10 章讨论了检验 UUID 有效性的可能性。一般来说,UUID 具有小的冗余度,并且有检验其有

效性的小范围。然而，如果接受了登记的 UUID，则该 UUID 被保证不同于所有其他登记的 UUID。

第 11 章描述了在 UUID 中历史上使用的某些比特，以定义 UUID 格式的不同变体，以及规定了按照本部分定义的 UUID 的这些比特的值。

第 12 章规定了在不同版本中使用的 UUID 的字段，而这些不同版本是定义的（基于时间的、基于名称的和基于随机数的版本）。它还定义了传输字节次序。

第 13 章规定了设置基于时间的 UUID 的字段。

第 14 章规定了设置基于名称的 UUID 的字段。

第 15 章规定了设置基于随机数的 UUID 的字段。

第 16 章涉及到 UUID 的登记机构的操作，以使它们能集中登记和提供唯一性保证。

所有附录都是资料性附录。

附录 A 描述了有效生成基于时间的 UUID 用的各种算法。

附录 B 讨论了基于名称的 UUID 宜具有的特性，这些特性对选择供生成这样的 UUID 时用的名称空间有影响。

附录 C 提供了关于在计算机系统中能用来生成随机数的机制的指南。

附录 D 包含了以 C 程序设计语言表示的完整程序，它能用来生成 UUID。

信息技术　开放系统互连 OSI登记机构操作规程 第8部分:通用唯一标识符(UUID)的生成和登记及其用作ASN.1客体标识符部件

1　范围

GB/T 17969的本部分规定了使用户能产生128比特标识符的格式和生成规则,而这些128比特标识符或被保证是全球唯一的或被保证是高概率的、全球唯一的。

遵守本部分以每100 ns生成一个新的UUID的速率来生成的UUID既适用于暂时使用,也可作为永久标识符。

本部分是起源于UUID及其生成的早期非标准规范,并且在技术上等同于这些早期规范。

本部分规定了用于UUID的基于Web的登记机构操作规程。

本部分还规定和允许使用UUID(登记的或不登记的)作为在弧{joint-iso-itu-t uuid(25)}之下的OID部件。这使用户能生成OID,而无需任何登记规程。

本部分还规定和允许使用UUID(登记的或不登记的)来形成URN。

2　规范性引用文件

下列文件中的条款通过GB/T 17969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 17969.1　信息技术　开放系统互连　OSI登记机构的操作规程　第1部分:一般规程(GB/T 17969.1—2000,eqv ISO/IEC 9834-1:1993)

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 15629.3　信息技术系统　局域网　第3部分:带碰撞检测的载波侦听多址访问(CSMA/CD)的访问方法和物理层规范(GB/T 15629.3—1995,idt ISO/IEC 8802-3:1990)

GB/T 13000—2010　信息技术　通用多八位编码字符集(UCS)(ISO/IEC 10646:2003,IDT)

GB/T 18238.3　信息技术　安全技术　散列函数　第3部分:专用散列函数(GB/T 18238.3—2002,idt ISO/IEC 10118-3:1998)

FIPS PUB 180-2:2002　联邦信息处理标准,安全散列标准(SHS)

IETF RFC 1321(1992)　MD5消息摘要算法

IETF RFC 2141(1997)　URN语法

3　术语和定义

下列术语和定义适用于本部分。

3.1　ASN.1记法

本部分使用了在GB/T 16262.1—2006中定义的下列术语: