INTERNATIONAL STANDARD

ISO/IEC 9834-8

First edition
2005-07-15

Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities: Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 Object Identifier components

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Procédures opérationnelles pour les organismes d'enregistrement de l'OSI: Génération et enregistrement des identificateurs uniques universels (UUID) et emploi de ces identificateurs comme composants d'identificateurs d'objet ASN.1

Reference number
ISO/IEC 9834-8:2005(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

CONTENTS

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 9834-8 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems* in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.667.

ISO/IEC 9834 consists of the following parts, under the general title *Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities*:

— *Part 1: General procedures and top arcs of the ASN.1 Object Identifier tree*

— *Part 2: Registration procedures for OSI document types*

— *Part 3: Registration of Object Identifier arcs beneath the top-level arc jointly administered by ISO and ITU-T*

— *Part 4: Register of VTE Profiles*

— *Part 5: Register of VT Control Object Definitions*

— *Part 6: Registration of application processes and application entities*

— *Part 7: Joint ISO and ITU-T Registration of International Organizations*

— *Part 8: Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 Object Identifier components*

Introduction

This Recommendation | International Standard standardizes the generation, and optional registration, of Universally Unique Identifiers (UUIDs).

UUIDs are an octet string of 16 octets (128 bits). The 16 octets can be interpreted as an unsigned integer encoding, and the resulting integer value can be used as an arc of the OID tree under the arc **{joint-iso-itu-t uuid(25)}**. This enables users to generate OIDs without any registration procedure.

UUIDs are also known as Globally Unique Identifiers (GUIDs), but this term is not used in this Recommendation | International Standard. UUIDs were originally used in the Network Computing System (NCS) [1] and later in the Open Software Foundation's Distributed Computing Environment (DCE) [2]. ISO/IEC 11578 [3] contains a short definition of some (but not all) of the UUID formats specified in this Recommendation | International Standard. The specification in this Recommendation | International Standard is consistent with all these earlier specifications.

UUIDs forming a component of an OID are represented in ASN.1 value notation as the decimal representation of their integer value, but for all other display purposes it is more usual to represent them with hexadecimal digits with a hyphen separating the different fields within the 16-octet UUID. This representation is defined in this Recommendation | International Standard.

If generated according to one of the mechanisms defined in this Recommendation | International Standard, a UUID is either guaranteed to be different from all other UUIDs generated before 3603 A.D., or is extremely likely to be different (depending on the mechanism chosen).

No centralized authority is required to administer UUIDs but central registration of self-generated UUIDs, and automatic generation (using the algorithm defined in this Recommendation | International Standard) and registration of UUIDs, is provided. Centrally generated UUIDs are guaranteed to be different from all other UUIDs centrally generated. Registered UUIDs are guaranteed to be different from all other registered UUIDs.

A UUID can be used for multiple purposes, from tagging objects with an extremely short lifetime, to reliably identifying very persistent objects across a network, particularly (but not necessarily) as part of an ASN.1 object identifier (OID) value, or in a Uniform Resource Name (URN).

The UUID generation algorithm specified in this Recommendation | International Standard supports very high allocation rates: 10 million per second per machine if necessary, so UUIDs can also be used as transaction IDs. An informative annex provides a program in the C language that will generate UUIDs in accordance with this Recommendation | International Standard.

Three algorithms are specified for the generation of unique UUIDs, using different mechanisms to ensure uniqueness. These produce different versions of a UUID.

The first (and most common) mechanism produces the so-called time-based version. These UUIDs can be generated at the rate of 10 million per second. For UUIDs generated within a single computer system, a 60-bit time-stamp (used as a Clock value) with a granularity of 100 nanoseconds, based on Coordinated Universal Time (UTC) is used to guarantee uniqueness over a period of approximately 1600 years. For UUIDs generated with the same time-stamp by different systems, uniqueness is obtained by use of 48-bit Media Access Control (MAC) addresses, specified in ISO/IEC 8802-3 (this is used as a Node value). (These addresses are usually already available on most networked systems, but are otherwise obtainable from the IEEE Registration Authority for MAC addresses – see [4].) Alternative ways of generating Clock and Node values are specified for the time-based version if UTC time is not available on a system, or if there is no MAC address available.

The second mechanism produces a single UUID that is a name-based version, where cryptographic hashing is used to produce the 128-bit UUID value from a globally unambiguous (text) name.

The third mechanism uses pseudo-random or truly random number generation to produce most of the bits in the 128-bit value.

Clause 5 specifies the notation used for octet-order and bit-order naming, and for specification of transmission order.

Clause 6 specifies the structure of a UUID and the representation of it in binary, hexadecimal, or as a single integer value.

Clauses 7 and 8 specify the use of a UUID in an OID or a URN respectively.

Clause 9 specifies rules for comparing UUIDs to test for equality or to provide an ordering relation between two UUIDs.

Clause 10 discusses the possibility of checking the validity of a UUID. In general, UUIDs have little redundancy, and there is little scope for checking their validity. However, if a UUID is accepted for registration, then it is guaranteed to be different from all other registered UUIDs.

Clause 11 describes the historical use of some bits in the UUID to define different variants of the UUID format, and specifies the value of these bits for UUIDs defined in accordance with this Recommendation | International Standard.

Clause 12 specifies the use of the fields of a UUID in the different versions that are defined (time-based, name-based, and random-number based versions). It also defines the transmission byte order.

Clause 13 specifies the setting of the fields of a time-based UUID.

Clause 14 specifies the setting of the fields of a name-based UUID.

Clause 15 specifies the setting of the fields of a random-number-based UUID.

Clause 16 is concerned with the operation of a Registration Authority for UUIDs, enabling their central registration and providing uniqueness guarantees.

All annexes are informative.

Annex A describes various algorithms for the efficient generation of time-based UUIDs.

Annex B discusses the properties that a name-based UUID should have, affecting the selection of name spaces for use in generating such UUIDs.

Annex C provides guidance on mechanisms that can be used to generate random numbers in a computer system.

Annex D contains a complete program in the C programming language that can be used to generate UUIDs.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 object identifier components

1 Scope

This Recommendation | International Standard specifies the format and generation rules that enable users to produce 128-bit identifiers that are either guaranteed to be globally unique, or are globally unique with a high probability.

The UUIDs generated in conformance with this Recommendation | International Standard are suitable either for transient use, with generation of a new UUID every 100 nanoseconds, or as persistent identifiers.

This Recommendation | International Standard is derived from earlier non-standard specifications of UUIDs and their generation, and is technically identical to those earlier specifications.

This Recommendation | International Standard specifies the procedures for the operation of a Web-based Registration Authority for UUIDs.

This Recommendation | International Standard also specifies and allows the use of UUIDs (registered or not registered) as OID components under the arc `{joint-iso-itu-t uuid(25)}`. This enables users to generate OIDs without any registration procedures.

This Recommendation | International Standard also specifies and allows the use of UUIDs (registered or not registered) to form a URN.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.660 (2004) | ISO/IEC 9834-1:2005, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the ASN.1 Object Identifier tree*.
- ITU-T Recommendation X.680 (2002) | ISO/IEC 8824-1:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

2.2 Other normative references

- ISO/IEC 8802-3:2000, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*.
- ISO/IEC 10118-3:2004, *Information technology – Security techniques – Hash functions – Part 3: Dedicated hash-functions*.
- ISO/IEC 10646:2003, *Information technology – Universal Multiple-Octet Coded Character Set (UCS)*.

- FIPS PUB 180-2:2002, *Federal Information Processing Standards Publication, Secure Hash Standard (SHS)*.
- IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm*.
- IETF RFC 2141 (1997), *URN Syntax.*

3 Terms and definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

3.1 ASN.1 notation

This Recommendation | International Standard uses the following terms defined in ITU-T Rec. X.680 | ISO/IEC 8824-1:

a) Coordinated Universal Time (UTC);

b) (ASN.1) object identifier.

3.2 Registration authorities

This Recommendation | International Standard uses the following terms defined in ITU-T Rec. X.660 | ISO/IEC 9834-1:

a) object identifier tree (or OID tree);

b) registration;

c) registration authority;

d) registration procedures.

3.3 Network terms

This Recommendation | International Standard uses the following term defined in ISO/IEC 8802-3:

- MAC address.

3.4 Additional definitions

3.4.1 cryptographic-quality random-number: A random number or pseudo-random number generated by a mechanism, which ensures sufficient spread of repeatedly-generated values to be acceptable for use in cryptographic work (and is used in such work).

3.4.2 name-based version: A UUID that is generated using cryptographic hashing of a name space name and a name in that name space.

3.4.3 name space: A system for generating names of objects that ensures unambiguous identification within that name space.

NOTE – Examples of name spaces are the network domain name system, URNs, OIDs, Directory distinguished names (see [5]), and reserved words in a programming language.

3.4.4 random-number-based version: A UUID that is generated using a random or pseudo-random number.

3.4.5 standard UUID variant: The variant of the possible UUID formats that is specified by this Recommendation | International Standard.

NOTE – Historically, there have been other specifications of UUID formats that differ from the variant specified in this Recommendation | International Standard. UUIDs generated according to all these variant formats are all distinct.

3.4.6 time-based version: A UUID in which uniqueness is obtained by the use of a MAC address to identify a system, and a Clock value based on the current UTC time.

3.4.7 Universally Unique Identifier (UUID): A 128-bit value generated in accordance with this Recommendation | International Standard, or in accordance with some historical specifications, and providing unique values between systems and over time (see also 3.4.5).

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

ASN.1	Abstract Syntax Notation One
GUID	Globally Unique Identifier
IEEE	Institute of Electrical and Electronics Engineers, Inc.
MAC	Media Access Control
MD5	Message Digest algorithm 5
OID	ASN.1 Object Identifier
RA	Registration Authority
SHA-1	Secure Hash Algorithm 1
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTC	Coordinated Universal Time
UUID	Universally Unique Identifier

5 Notation

5.1 This Recommendation | International Standard specifies a sequence of octets for a UUID using the terms first and last. The first octet is also called "octet 15" and the last octet "octet 0".

5.2 The bits within a UUID are also numbered as "bit 127" to "bit 0", with bit 127 as the most significant bit of octet 15 and bit 0 as the least significant bit of octet 0.

5.3 When figures and tables are used in this Recommendation | International Standard, the most significant octet (and the most significant bit) are displayed on the left of the page. This corresponds with a transmission order of octets in which the left-most octets are transmitted first.

5.4 A number of values used in this Specification are expressed as the value of an unsigned integer of a given bit-length (N say). The bits of the N-bit unsigned integer value are numbered "bit N-1" to "bit 0", with bit N-1 as the most significant bit and bit 0 as the least significant bit.

5.5 These notations are used solely for the purposes of this Specification. Representations in computer memory are not standardized, and depend on the system architecture.

6 UUID structure and representation

6.1 UUID field structure

6.1.1 A UUID is specified as an ordered sequence of six fields. A UUID is specified in terms of the concatenation of these UUID fields. The UUID fields are named:

a) the "TimeLow" field;

b) the "TimeMid" field;

c) the "VersionAndTimeHigh" field;

d) the "VariantAndClockSeqHigh" field;

e) the "ClockSeqLow" field;

f) the "Node" field.

6.1.2 The UUID fields are defined to have a significance in the order listed above, with "TimeLow" as the most significant field (bit 31 of "TimeLow" is bit 127 of the UUID), and "Node" as the least significant field (bit 0 of "Node" is bit 0 of the UUID).

6.1.3 The contents of these UUID fields are specified in terms of a Version, Variant, Time, Clock Sequence, and Node unsigned integer value (each with a fixed bit-size). The setting of these values is specified in clause 12 and their mapping to the above UUID fields is specified in 12.1.

NOTE – As part of the names of some of the UUID fields (for example, TimeLow, TimeMid, and TimeHigh) imply, the sequential order of the bits in a UUID (bit 127 to bit 0) that derive from a particular unsigned integer value (for example, from bits 59 to 0 of the Time value) is not the same as the sequential order of the bits in that unsigned integer value. This is for historical reasons.

6.2 Binary representation

6.2.1 A UUID shall be represented in binary as 16 octets formed by the concatenation of the unsigned integer fixed-length encoding of each of its fields into one or more octets. The number of octets to be used for each field shall be:

a) the "TimeLow" field: four octets;

b) the "TimeMid" field: two octets;

c) the "VersionAndTimeHigh" field: two octets;

d) the "VariantAndClockSeqHigh" field: one octet;

e) the "ClockSeqLow" field: one octet;

f) the "Node" field: six octets.

NOTE – This order of UUID fields is the usual representation within a computer system, and in the hexadecimal text representation (see 6.4).

6.2.2 The most significant bit of the unsigned integer encoding of each UUID field shall be the most significant bit of its first octet (octet N, the most significant octet), and the least significant bit of the unsigned integer encoding shall be the least significant bit of its last octet (octet 0, the least significant bit).

6.2.3 The UUID fields shall be concatenated in the order of their significance (see 6.1.2) with the most significant field first and the least significant field last.

6.3 Representation as a single integer value

A UUID can be represented as a single integer value. To obtain the single integer value of the UUID, the 16 octets of the binary representation shall be treated as an unsigned integer encoding with the most significant bit of the integer encoding as the most significant bit (bit 7) of the first of the sixteen octets (octet 15) and the least significant bit as the least significant bit (bit 0) of the last of the sixteen octets (octet 0).

NOTE – The single integer value is used when the UUID forms part of an OID as specified in clause 7.

6.4 Hexadecimal representation

For the hexadecimal format, the octets of the binary format shall be represented by a string of hexadecimal digits, using two hexadecimal digits for each octet of the binary format, the first being the value of the four high-order bits of octet 15, the second being the value of the four low-order bits of octet 15, and so on, with the last being the value of the low-order bits of octet 0 (see 6.5). A HYPHEN-MINUS (45) character (see ISO/IEC 10646) shall be inserted between the hexadecimal representations of each pair of adjacent fields, except between the "VariantAndClockSeqHigh" field and the "ClockSeqLow" field (see the example in clause 8).

6.5 Formal syntax of the hexadecimal representation

6.5.1 The formal definition of the UUID hexadecimal representation syntax is specified using the extended BNF notation defined in ITU-T Rec. X.680 | ISO/IEC 8824-1, clause 5, except that there shall be no white-space between the lexical items.

6.5.2 The "hexdigit" lexical item is used in the BNF specification and is defined as follows:

Name of lexical item – hexdigit

A "hexdigit" shall consist of exactly one of the characters:

```
A B C D E F a b c d e f 0 1 2 3 4 5 6 7 8 9
```

6.5.3 The hexadecimal representation of a UUID shall be the production "UUID":

UUID ::=
TimeLow
"-" TimeMid
"-" VersionAndTimeHigh
"-" VariantAndClockSeqHigh ClockSeqLow
"-" Node