Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14242
Date:	2010-03-10
Replaces:	
Document Type:	Text for FCD ballot
Document Title:	Text for FCD ballot, ISO/IEC 29168, Information technology – Open Systems Interconnection – Object Identifier Resolution System (ORS)
Document Source:	Project Editor
Project Number:	
Document Status:	SC 6 NBs are requested to ballot on e-balloting system of SC 6 website (www.iso.org/jtc1/sc6) no later than 2010-07-10.
Action ID:	LB
Due Date:	2010-07-10
No. of Pages:	28

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

Title: **FCD ballot text for ISO/IEC 29168**
Date: **9 Mar 2010**
Source: **Project Editor (from the continuation Ballot Resolution meeting on CD 2)**

INTERNATIONAL STANDARD ISO/IEC 29168

ITU-T RECOMMENDATION X.oid-res

Information technology – Open Systems Interconnection – Object Identifier Resolution System (ORS)

Summary

This Recommendation | International Standard specifies the OID (Object Identifier) Resolution System (ORS). This enables (arbitrary) information to be associated with any ORS-supported OID node (of the International Object Identifier tree defined in ITU-T X.660 | ISO/IEC 9834-1). This associated information is identified by an application specification that may have a requirement for instances of that application (running on any computer system) to obtain the associated information by an ORS search, using an ASN.1 OID-IRI value to identify the node.

Currently defined application information for a node includes the canonical form of an International Object Identifier, child node information, registration information about the owner of the node, a reference to an ASN.1 module identified by the node, information supporting tag-based applications, and information supporting cybersecurity.

Keywords

Object Identifier Resolution System, Object Identifier, ORS, OID

CONTENTS

Introduction

This Recommendation | International Standard specifies the object identifier resolution system. This provides the return (using an ORS client) of information associated with an OID node.

It uses a mapping of the International Object Identifier tree naming scheme (using OID-IRI values) onto the DNS naming scheme (see 7.3).

This Recommendation | International Standard specifies requirements on the management of DNS zone files that are mapped from ORS-supported OID nodes to provide (standardised) information related to an International Object Identifier tree node for a variety of applications, and on the behaviour of an ORS client that interacts with the DNS system to obtain that information and provide it to an application.

Six requirements emerged in the mid/late-2000s:

- an application to be able to translate any OID-IRI value into a canonical OID-IRI (a unique string of numeric Unicode labels that would identify a node): the COID ORS service, supporting IRI comparison of names in the IETF "oid" IRI scheme (see Annex B);
- an application to determine child information from an OID node: the CINF service (see Annex C);
- an application to obtain registration information (such as contact information about the owner of the OID node, and how to request a child node, etc.): the RINF service (see Annex D);
- an application to obtain a reference to the ASN.1 module (if any) associated with a node: the MINF service (see Annex E);
- support of [b-ITU-T H.IRP] for access to multimedia information (triggered by tag-based identification) using the ORS;
- support of [b-ITU-T X.cybex-disc-oid] for access to information contained in an OID node that relates to cybersecurity features.

There are probably other applications that will require further information (specified by an application standard) contained in an ORS-supported OID node and accessible by the ORS.

To meet these needs, it was determined to map the OID tree into a part of the DNS tree (see IETF RFC 1035), with the root of the OID tree mapped into .oid-res.org (see 7.3).

The ORS operates by mapping the International OID tree into the DNS tree. The mapping is from any OID-IRI value that identifies an International OID node into a DNS name (in the .oid-res.org domain). The information about an ORS-supported OID node is inserted into DNS zone files and can then be retrieved by any ORS client (running on any computer system with DNS access), using any of the ASN.1 OID-IRI identifications for that International Object Identifier tree node.

The associated information is specified by those applications that choose to use the ORS. The requirements on such applications are included in this Recommendation | International Standard. Some application specifications are included as normative Annexes to this Recommendation | International Standard. Others are specified externally.

NOTE – The form and semantics of information obtained by use of the ORS service types COID, CINF and RINF (and their use) are fully specified in this Recommendation | International Standard. The form and semantics of information obtained by other ORS service types are specified in the standards referenced in Annex A.

All DNS zone files for the .oid-res.org domain correspond to ORS-supported OID nodes, but not all DNS names algorithmically mapped from an OID-IRI will be present in the DNS. All DNS zone files in the .oid-res.org domain are required to confirm to this Recommendation | International Standard.

Information for an International OID tree node (for each application) is specified by the owner of that node, and determines the appropriate configuration of DNS zone files, in accordance with the specification for each ORS service (see Annex A), and would be retrieved by an application using a local ORS client implementation interacting with a local DNS client (see clause 7). The information would be included in NAPTR resource records, qualified by the ORS service type.

An ORS client takes as input any OID-IRI value, together with an ORS service type. It will return node information for that OID-IRI value and ORS service type (based on the configuration of the DNS zone files, and

particularly of NAPTR resource records). Each resource record will consist of one or more pieces of information together with the requested ORS service type.

Clause 5 provides an overview of the OID resolution system architecture and its interaction with the DNS.

Clause 6 specifies the requirements and restrictions on DNS zone files in the .oid-res.org domain in order to support navigation to DNS names mapped from the International OID tree (including the use of long arcs) and the provision of information needed for the ORS resolution process using any specified ORS service type.

NOTE – This specification relates only to use of DNAME and CNAME DNS resource records, and NAPTR resource records using a service field commencing "ORS+". Use of other DNS resource records are not in the scope of this Recommendation | International Standard and are neither forbidden (except when they would conflict with use for the ORS) nor are they required.

Clause 7 specifies the operation of an ORS client, including the mapping of an OID-IRI value into a DNS name.

Clause 8 specifies the requirements on an ORS application specification, including specification of NAPTR information and recommendations on ORS application processing.

Security considerations are discussed and specified in 5.2.3 6.5, 7.5 and 8.2.2.

Annex A (normative) specifies the assigned ORS service types at the time of publication of this Recommendation | International Standard.

Annex B (normative) specifies the COID service.

Annex C (normative) specifies the requirements for the CINF service.

Annex D (normative) specifies the requirements for the RINF service.

Annex E (normative) specifies the requirements for the MINF service.

Annex F (informative) provides a description of the use cases for the ORS, referencing each application that has a specified ORS service type (see Annex A).

Annex G (informative) provides examples of possible DNS zone files to support the ORS and additional examples of NAPTR resource records.

Annex H (informative) provides a short history of the development of the International OID tree.

Annex I (informative) provides bibliographic references.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Open Systems Interconnection – Object Identifier Resolution System

1 Scope

This Recommendation | International Standard specifies the OID resolution system, including the overall architecture and a DNS-based resolution mechanism.

It specifies the means for inserting any application-defined information associated with an OID node into the DNS (see clause 6) and the means of retrieval of that information using the ORS (see clause 7).

It does not restrict the number of applications it can support.

It specifies the required operation of an ORS client (see clause 7), including the mapping of an OID-IRI value by the ORS client into a DNS name to produce a DNS query for the specified application information and the processing of any returned information.

The required behaviour of an ORS client is specified, but the interfaces to it are specified only in terms of the semantics of the interaction. A bit-level application programme interface is platform and software dependent, and is not in the scope of this Recommendation | International Standard.

It does not include a tutorial or complete specification on the management of DNS zone files (for that, see IETF RFC 1035 and IETF RFC 3403); it specifies (only) the DNS resource records (see 6.3) that need to be inserted in the zone files in order to support ORS access to the information associated with an OID node.

This Recommendation | International Standard specifies required DNS zone file resource records, and prohibits the use of other resource records of a similar form but with different semantics (in DNS zone files from in the .oid-res.org domain) – see 6.2. It does not otherwise restrict the general use of DNS zone files.

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 X.660 series | ISO/IEC 9834 multi-part standard, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities.*
- ITU-T X.680 (2008) series | ISO/IEC 8824:2008 multi-part standard, *Information technology – Abstract Syntax Notation One (ASN.1).*
- ITU-T X.693 (2008) | ISO/IEC 8825-4:2008, *Information technology – ASN.1 Encoding Rules: XML Encoding Rules (XER).*

2.2 Additional references

- IETF RFC 1034:1987, *Domain names – Concepts and facilities.*
- IETF RFC 1035:1987, *Domain names – Implementation and specification.*
- IETF RFC 3403:2002, *Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database.*

- IETF RFC 3454:2002, *Preparation of Internationalized Strings ("stringprep").*
- IETF RFC 3490:2003, *Internationalizing Domain Names in Applications (IDNA).*
- IETF RFC 3492:2003, *Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA).*
- IETF RFC 4033:2005, *DNS Security Introduction and Requirements.*
- IETF RFC 5155:2008, *DNS Security (DNSSEC) Hashed Authenticated Denial of Existence.*

  NOTE – It is recommended that the IETF RFC index be consulted for updates to the RFCs listed above.
- Unicode 5.2, *The Unicode Standard, Version 3.2.0:2002. The Unicode Consortium (Reading, MA, Addison-Wesley).*
- W3C HTML, *HTML Specification*, W3C Recommendation, Copyright © [2 May 2001] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/html401.

3 Definitions

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

3.1 Imported definitions

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

a) object identifier;

b) integer-valued Unicode label;

c) International Object Identifier tree;

d) OID internationalized resource identifier;

e) Registration Authority;

f) Unicode label.

3.2 Additional definitions

3.2.1 application-specific OID resolution process: Actions by an application to retrieve application-specific information from the information returned by the general OID resolution process.

3.2.2 canonical form (of an OID-IRI): A form which uses only integer-valued Unicode labels.

NOTE – OID-IRI is an ASN.1 type defined in ITU-T X.680 | ISO/IEC 8824-1. The term OID-IRI value refers to the ASN.1 value notation that is the same as the IANA "oid:" IRI/URI scheme, with the omission of the initial "oid:".

3.2.3 DNS-mapped name: The result of transforming an OID-IRI value to an FQDN (see 7.3).

NOTE – The DNS-mapped name may or may not exist in the DNS. If it does not, then an ORS query will result in an error message (see 7.4), and the node identified by the OID-IRI is not ORS-supported.

3.2.4 DNS resource record: A component of a DNS zone file.

3.2.5 DNS zone file: A text file that describes a portion of the DNS.

NOTE – The format of a DNS zone file is defined in IETF RFC 1035, section 5 and IETF RFC 1034, section 3.6.1.

3.2.6 fully qualified domain name: The name used in a DNS look-up operation (see [b-IETF RFC 1594]).

3.2.7 general OID resolution process: That part of the ORS where an ORS client obtains information from the DNS (recorded in a zone file) about any specified OID and returns it to an application.

3.2.8 maintenance agency procedures: The procedures specified in ITU-T X.oid-res – Supplement on procedures for the operation of the .oid-res.org maintenance agency.

3.2.9 NAPTR resource record: A DNS resource record used to store rules which can be retrieved by a DNS look-up for use by an application.

3.2.10 OID resolution process: Process supporting the OID resolution system which provides information associated with an OID using the general OID resolution process, followed if necessary by an application-specific OID resolution process (see Figure 1).

3.2.11 OID resolution system: Implementation of the OID resolution process in accordance with this Recommendation | International Standard.

3.2.12 .oid-res.org maintenance agency: Organization that manages the DNS server for .oid-res.org and some subordinate nodes specified in the maintenance agency procedures.

3.2.13 ORS client: Entity that interfaces between an application and a DNS client.

3.2.14 ORS service type: A character string (used in NAPTR resource records) that identifies an ORS service (see Annex A).

3.2.15 ORS-supported OID node: An OID node for which the DNS-mapped names for all of the OID-IRI values that identify the OID node exist in the DNS, and have all necessary DNS zone files configured as specified in this Recommendation | International Standard, including mandatory requirements for all ORS services (see Annex A).

NOTE 1 – The Canonical OID service specified in Annex B requires the presence of a NAPTR record in the associated DNS zone file.

NOTE 2 – The .oid-res.org maintenance agency is required by the maintenance procedures to provide ORS-support for all the OID nodes listed in those procedures. ORS support for nodes beneath these depends on agreements between that OID node and its parent.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CNAME	(DNS) Canonical Name
DNAME	(DNS) Delegation Name
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
NAPTR	(DNS) Naming Authority Pointer
NS	(DNS) Name Server
OID	Object Identifier
OID-IRI	OID Internationalized Resource Identifier (see the NOTE on 3.2.2)
ORS	OID Resolution System
RCODE	(DNS) Return Code

5 The OID resolution system architecture

5.1 The OID resolution process

5.1.1 The OID resolution process is illustrated in Figure 1. It consists of two processes: a general OID resolution process and an application-specific OID resolution process.

5.1.2 The general OID resolution process uses the DNS (see IETF RFC 1035) and DNS resource records (see IETF RFC 3403). It involves an interaction between the application and an ORS client to retrieve information (specified by that application) from the DNS system. The general OID resolution process normally returns a URL for a document, a canonical OID-IRI or a DNS name, but there is no restriction on what could be returned. This is usually followed by an application-specific OID resolution process, where the application uses the information obtained from the general resolution process to obtain the final information required by the application.

NOTE – For some services, for example the COID service (see Annex B), the information returned from the ORS client will be sufficient, and there will be no application-specific OID resolution process.

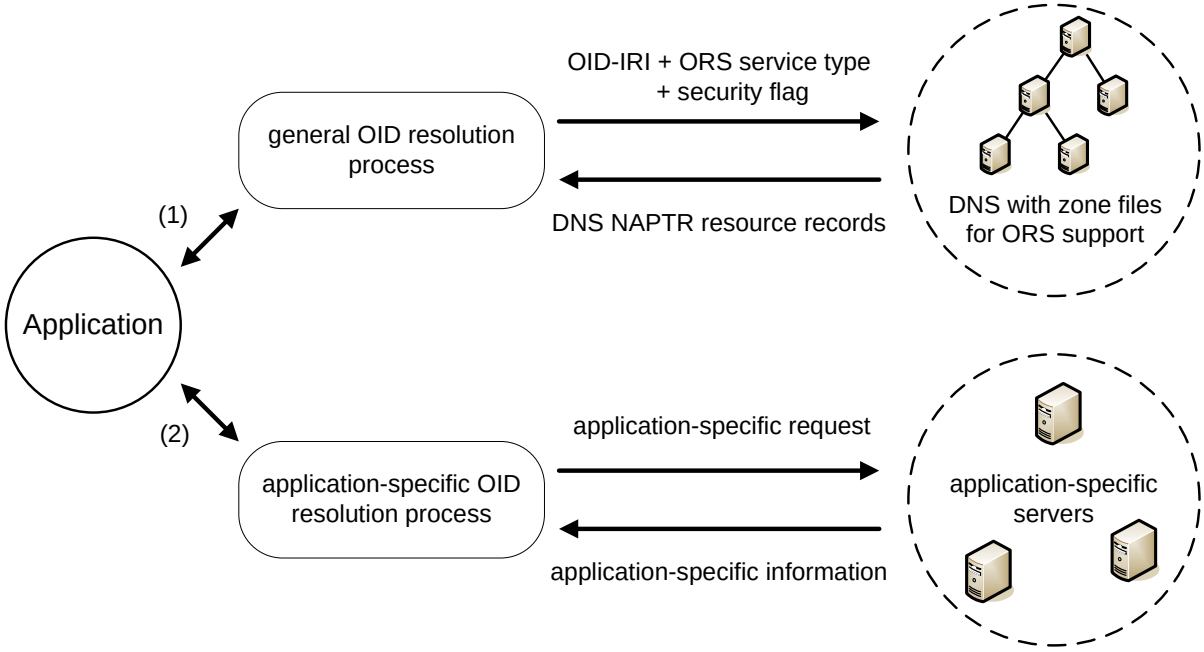

Figure 1 – The OID resolution process

5.2 Interactions between components in the general OID resolution process

5.2.1 Figure 2 shows the functional interfaces between the components of the general OID resolution process, and the semantics of the interactions. Bit-level encoding of these interfaces and interactions is platform and software dependent, and is not in the scope of this Recommendation | International Standard. The realisation of this architecture in hardware or software and its partitioning into separate modules is not constrained by this Recommendation | International Standard.

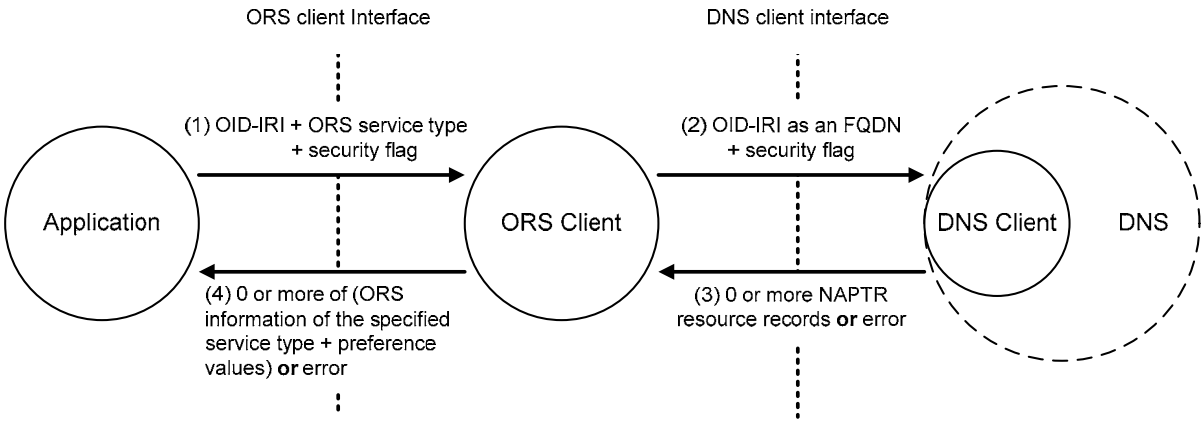

Figure 2 – Components of the general OID resolution system

5.2.2 There are three main actors: the application, an ORS client, and the DNS system.

5.2.3 (Step 1) The application makes a request to the ORS client for information about an OID, giving one of the OID-IRI values that identifies that OID node and the ORS service type that it is interested in (see Annex A). It also sets the "security flag". If this flag is set, it is passed to the DNS client, and no information

from NAPTR resource records will be returned to the ORS client (and hence to the application) unless they have been signed (and verified by the DNS) in accordance with IETF RFC 4033 (DNSSEC).

NOTE 1 – The application has to trust the ORS client and the DNS client to pass on the security flag setting, and for the DNS servers to correctly implement IETF RFC 4033 and IETF RFC 5155 (NSEC3). If the application does not trust the ORS client or the DNS client that it is using, it should not set the security flag, as it will not provide any security benefit.

NOTE 2 – It is a requirement of the maintenance agency procedures that the .oid-res.org maintenance agency provides full support for security as required by IETF RFC 4033 and IETF RFC 5155.

5.2.4 (Step 2) The ORS client transforms the OID-IRI value into an FQDN as specified in 7.3 and sends a query request to a DNS client (copying the security flag) for NAPTR resource records containing the requested ORS information type, as specified in 7.2.

5.2.5 (Step 3) The DNS client returns either zero or more NAPTR resource records, or an error (specified as a non-zero RCODE – see IETF RFC 1035).

5.2.6 (Step 4) The ORS client processes the NAPTR resource records as specified in 7.4 and returns to the application zero or more information fields with preference values, and the DNS RCODE (to be interpreted by the application with the guidance suggested in Table 1).

RCODE value	**Suggested interpretation by the application**
0	OK
1	ORS system failure
2	DNS system failure
3	No such domain name
4	Retrieval of NAPTR resource records not supported for this domain name (the DNS is not correctly configured for ORS-support of this OID-IRI value)
5	Security policy restriction
6 upwards	No interpretation available

Table 1 – Suggested interpretation of DNS RCODE values

6 DNS zone files for the .oid-res.org domain

6.1 Overview

NOTE – This Recommendation | International Standard does not provide a tutorial or complete specification on the use of DNS zone files. This is not in its scope. It is assumed that zone file managers supporting the ORS will understand such issues.

6.1.1 An OID node may or may not be ORS-supported.

6.1.2 For an OID node to be ORS-supported, all its DNS-mapped names have to be available for retrieval of information from DNS zone files.

6.1.3 If an OID node is not ORS-supported, any ORS query using some the OID-IRI values that identify that OID node should return a DNS RCODE value of 3 (no such domain name), and information associated with that OID node cannot be obtained by an ORS query to an ORS client. Its parent OID node may or may not be ORS-supported. Its child OID nodes can never be ORS-supported.

6.1.4 If the OID node is ORS-supported, any of its DNS-mapped names can be used to obtain NAPTR information. Its parent OID node is required to be ORS-supported. Each of its child OID nodes may or may not be ORS-supported.

6.1.5 The .oid-res.org maintenance agency manages and maintains the DNS zone files corresponding to the OID nodes of the OID tree specified in the management agency procedures in accordance with 6.2.

NOTE – This means that all those OID nodes are ORS-supported.

6.1.6 The .oid-res.org maintenance agency is required (by the maintenance agency procedures) to add an NS resource record for any child OID node (of any OID node that it supports) if that child OID node wishes to become ORS-supported. Any child OID node that wishes to become ORS-supported shall arrange for the management of the corresponding DNS zone files in accordance with 6.2.

6.1.7 Any OID node that is not one of those supported by the .oid-res.org management agency, but which is itself ORS-supported, shall determine by mutual agreement between that OID node and each of its child OID nodes whether the child becomes ORS-supported. The requirements of 6.2 shall then be recursively applied.

6.1.8 The requirements to use CNAME and DNAME resource records (as specified in 6.2) ensure that there is only a single final DNS zone file accessed for the return of NAPTR resource records for all the ORS queries that use any of the OID-IRI values that identify an ORS-supported OID node.

6.2 Requirements and restrictions on DNS zone files in the .oid-res.org domain

6.2.1 These requirements are placed on the .oid-res.org maintenance agency (and recursively on all DNS zone files in the **`.oid-res.org`** domain.

6.2.2 Names in the .oid-res.org domain shall not be allocated unless they are DNS-mapped names.

6.2.3 All DNS zone files in the .oid-res.org domain shall (with appropriate use of DNAME and CNAME records as specified in 6.3) support DNS queries using any of the Unicode labels on the arcs leading to an ORS-supported OID node.

6.2.4 A DNS zone file in the .oid-res.org domain shall not contain NAPTR resource records with a service field which starts with "ORS+" except as specified in this Recommendation | International Standard, and with the semantics specified here.

NOTE – This Recommendation | International Standard does not restrict the use of NAPTR resource records with other service field values.

6.3 Use of DNS resource records for ORS services

6.3.1 Use of DNAME and CNAME resource records

6.3.1.1 If an OID node is ORS-supported, then the zone file supporting the parent of that OID node shall, for every Unicode label identifying that child OID node that is not an integer-valued Unicode label, provide a DNAME or CNAME resource record (see the examples in).

6.3.1.2 If an ORS-supported OID node has no ORS-supported child OID nodes, then a CNAME resource record shall be used in the zone file, otherwise a DNAME resource record shall be used. If an ORS-supported child is subsequently added to the node, then the CNAME in its zone files shall be changed to DNAME.

NOTE – This requirement is imposed to avoid an exponential explosion of DNS resource records in zone files supporting lower level ORS-supported nodes, and to allow a higher level OID-arc to have additional Unicode labels added later without requiring change to DNS zone files supporting lower-level OID nodes.

6.3.1.3 The zone files for each ORS-supported OID node that has an ORS-supported child shall contain a DNAME or CNAME resource record for each non-integer Unicode label on the arc to that child (as specified in 6.3.1.2). For the purposes of this clause, any node that can be reached by a long arc is also a child node.

6.3.1.4 The DNAME or CNAME resource record shall be preceded by:

a) the Unicode label on the arc to that child transformed as specified in IETF RFC 3490, section 4.2, including case folding (see IETF RFC 3454) and punycode encoding (see IETF RFC 3492) using the Compatibility Decomposition followed by Canonical Composition (NFKC) specified by Unicode 5.2, Annex 15; then

b) the FQDN for the parent, derived from the canonical form of the OID-IRI for the parent.

6.3.1.5 The DNAME or CNAME resource record shall contain the FQDN for the child mapped from the canonical OID-IRI for that child.

EXAMPLE – See Figure 3 for several examples.

6.3.2 Use of NAPTR resource records

6.3.2.1 Each NAPTR resource record supporting the ORS shall be placed in the DNS zone file accessed by use of the DNS-mapped name from the canonical OID-IRI for the OID node that it is supporting, preceded by that DNS-mapped name. It can also be accessed by other names derived from Unicode labels leading to that node, subject to correct use of DNAME and CNAME.

6.3.2.2 The contents of a NAPTR resource record shall be as follows:

a) the order field shall be zero;

b) the preference field shall be a non-negative integer;

c) the flags field shall be set to **"u"**;

d) the service field shall be set to **"ORS+*xxxx*"**, where ***xxxx*** is an ORS service type specified in Annex A;

e) the regular expression field shall be the string **"!^.*$!*information*!"**, where ***information*** is specified in the reference given in Annex A for the corresponding ORS service type.

EXAMPLE – The following is an example of a NAPTR resource record supporting return of the canonical form of an OID-IRI.

Order	Preference	Flags	Service	Regular expression	Replacement
0	**100**	**"u"**	**"ORS+COID"**	**"!^.*$!/2/27!"**	**.**

6.3.2.3 Other examples of the use of NAPTR resource records are given in G.1.

6.5 Security considerations

6.5.1 A DNS zone file manager will choose whether to sign NAPTR information or not. There is no requirement to do so in general, but the .oid-res.org management agency is required to provide support for security as specified by IETF RFC 4033 and IETF RFC 5155

6.5.2 If any NAPTR resource record is not signed (or the certificate chain is not accepted), then the DNS client will return an error code, no NAPTR resource records will be returned to the ORS client, and no information will be returned to the application.

7 Operation of an ORS client

7.1 Functional interfaces

An ORS client shall support functional interfaces to an application and to a DNS client as specified in steps 1 to 4 of 5.2

7.2 Processing a query

7.2.1 The ORS client shall convert the OID-IRI value into an FQDN as specified in 7.3, for use in the query as specified below.

7.2.2 The ORS client shall then send a query to the DNS client containing the FQDN, requesting the return of NAPTR resource records for that FQDN.

7.3 Converting an OID-IRI value to an FQDN

7.3.1 The canonical form of an OID-IRI shall be converted to an FQDN using the following procedure:

a) write the canonical form of the OID-IRI as a sequence of numbers, each preceded by a "**/**" (for example, **/2/27**);

b) remove the first "**/**" (producing for example, **2/27**);

c) put dots ("**.**") instead of "**/**" (producing for example, **2.27**);

d) reverse the order (producing for example, **27.2**);

e) append the string "**.oid-res.org.**" (producing for example, **27.2.oid-res.org.**).

7.3.2 A general OID-IRI shall be converted to an FQDN using the following procedure:

a) write the OID-IRI as a sequence of Unicode labels, each preceded by a "**/**" (for example, **/joint-iso-itu-t/tag-based**);

b) remove the first "**/**" (producing for example, **joint-iso-itu-t/tag-based**);

c) put dots ("**.**") instead of "**/**" (producing for example, **joint-iso-itu-t.tag-based**);

d) reverse the order (producing for example, **tag-based.joint-iso-itu-t**);

e) append the string **".oid-res.org.**" (producing for example, **tag-based.joint-iso-itu-t.oid-res.org.**).

f) transform the FQDN as specified in IETF RFC 3490, section 4.2, including case folding (see IETF RFC 3454) and punycode encoding (see IETF RFC 3492). It shall use the Compatibility Decomposition, followed by Canonical Composition (NFKC) specified by Unicode 5.2, Annex 15.

7.4 Processing DNS results

7.4.1 This clause specifies the processing of DNS results.

7.4.2 If a DNS RCODE which is non-zero is returned, then an error return will be passed to the application with the RCODE value.

NOTE – Guidance to the application on handling this is provided in 5.2.6.

7.4.3 If an RCODE of zero is returned, then the following steps shall be performed.

7.4.4 (Step 1) Select only those NAPTR resource records which have flag field value **"u"**.

7.4.5 (Step 2) If there are any results from step 1, select only NAPTR resource records with service field value "**ORS+*xxxx***" where ***xxxx*** is the ORS service type which was requested by the application.

7.4.6 (Step 3) If there are any results from step 2, for all NAPTR resource records, extract the substring between the "**!^.*$!**" and the "**!**" in the regular expression (the information part of the NAPTR resource record), and the preference field value.

7.4.7 (Step 4) Return all results (if any) from step 3 to the application with the RCODE value of zero.

7.5 Security considerations

The ORS client has no security responsibilities, other than to copy the security flag from an ORS query to a DNS query.

8 Requirements on ORS service specifications

8.1 Specification of NAPTR information

8.1.1 An ORS service shall specify the values to be provided in the regular expression field of NAPTR resource records for this application.

NOTE – Examples are available in the Annexes to this Recommendation | International Standard.

8.1.2 The ORS service shall specify the application-specific resolution (if any) that is to occur when the result of a DNS query is returned to an application implementing that ORS service, or to the use the application will make of the results of the DNS query.

8.2 Recommendations for ORS application processing

8.2.1 General

It is recommended that an application processes the returned information for an RCODE of zero (if any) by attempting application-specific processing of the information with the highest preference value, and (if that fails) to use the information (if any) with the next highest preference value.

8.2.2 Processing security data

The application is not provided with any security data (for example, a signature and a certificate chain). It can only set the security flag on a query and then trust the ORS client and the DNS to have returned only valid data.

Annex A

Assigned ORS service types

(This annex forms an integral part of this Recommendation | International Standard)

A.1 ORS service types are assigned in Table 2.

Name of ORS service	Service type value	Specification of the service
OID canonicalization	COID	Annex B
Child information	CINF	Annex C
Registration information	RINF	Annex D
Module information	MINF	Annex E
Tag-based multimedia access	TINF	[b-ITU-T H.IRP]
Cybersecurity information	CYBEX	[b-ITU-T X.cybex-disc-oid]

Table 2 – Assigned ORS service types

A.2 Proposals for support of new ORS services shall be submitted to the Rapporteur of the ITU-T Question | the Convenor of the ISO/IEC Working Group responsible for this Recommendation | International Standard. They shall include a proposed name for the ORS service, a proposed service type value, and a description of the use case. The request is accepted (or perhaps modified or rejected) by joint approval of the relevant ITU-T Study Group | ISO/IEC Committee. An accepted proposal for a new ORS service, its service type value, and the description of its use-case will be published on the relevant ITU-T Study Group web site.

Annex B

Specification of the OID canonicalization (COID) ORS service

(This annex forms an integral part of this Recommendation | International Standard)

B.1 All DNS zone files for an ORS-supported OID node shall contain a NAPTR resource record (see 6.3.2) with ORS service type **`COID`** and with the regular expression **`information`** containing the DNS-mapped name (see 7.3) of the canonical form of the OID-IRI for that node.

B.2 If an application supporting this ORS service receives (from a query to an ORS client) an RCODE value which is not zero, it should attempt to report that failure of the ORS system, but the means of doing this is not standardized.

NOTE – Failure can result from incorrect configuration of DNS zone files, temporary or permanent failure of the DNS system, incorrect ORS client implementation, incorrect mapping of an OID-IRI by the application or for other reasons (see also 5.2.6)

B.3 There is no application-specific ORS resolution process needed or specified for this ORS service, as the canonical form of the OID-IRI is returned from the general ORS resolution process.

B.4 Examples of NAPTR resource records containing the canonical form of an OID-IRI are given in G.2.

Annex C

Specification of the child information (CINF) ORS service

(This annex forms an integral part of this Recommendation | International Standard)

C.1 General

C.1.1 All DNS zone files for an ORS-supported OID node shall contain a NAPTR resource record (see 6.3.2) with ORS service type **`CINF`** and with the regular expression **`information`** containing a URL for a child information file (with a ".xml" extension) that provides child information for the OID node in accordance with C.2.

C.1.2 If an application supporting this ORS service receives a non-zero RCODE value from a query to an ORS client (using an OID node that it believes to be ORS-supported), it should attempt to report that failure, but the means of doing this is not standardized.

NOTE – Failure will always result (RCODE value 3) if that OID node is not ORS-supported. It can also result from incorrect configuration of DNS zone files, temporary or permanent failure of the DNS system, incorrect ORS client implementation, incorrect mapping of an OID-IRI by the application or for other reasons (see also 5.2.6).

C.1.3 If the RCODE returned is zero, the application-specific ORS resolution process shall access the XML file at the location returned by the general ORS resolution process in order to obtain child information for the node identified by the OID-IRI submitted to the ORS client.

NOTE – If the file at that location is not an XML file conforming to C.2 then the application should attempt to report that failure, but the means of doing this is not standardized.

C.2 The CINF XML file

C.2.1 The CINF XML file shall conform to the EXTENDED-XER encoding (specified in [ITU-T X.693]) of the ASN.1 module specified in C.2.3. The semantics of the fields are included in this module specification as comment, and are normative.

NOTE – In order to enable both ASN.1 and XML tools to be used in ORS applications, an (informative) XSD specification [b-XSD Structures, b-XSD Datatypes] for an identical XML encoding is available at http://www.itu.int/ITU-T/recommendations/fl.aspx?lang=4 (followed by a search for the Recommendation). If discrepancies are detected between the two specifications of allowed XML, there should be a Defect Report on this Recommendation | International Standard.

C.2.2 A parent OID node shall not provide a **`<ChildDetails>`** element for a child OID node without the agreement of that child.

NOTE – There are several privacy options available in the specification of the child information XML file. A parent node may always choose to use **`<ChildInformation><noDisclosure/></ChildInformation>`**, revealing no child information. The parent may also list the number of undisclosed children (at its discretion) if it has agreement to disclose child information for at least one child (or may choose not to disclose the number of undisclosed children).

C.2.3 The ASN.1 module (with semantics of the fields as ASN.1 comments is):

```
CINF-module
{joint-iso-itu-t ors(50) modules(0) cinf(1) version1(1)}
"/ORS/modules/cinf/version1"
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

ChildInformation ::= CHOICE {
      noDisclosure     NULL /* No information is provided */ ,
      disclosure       Information }

Information ::= SEQUENCE {
      disclosedChildren      SEQUENCE SIZE (0..MAX) OF
```

```
                              disclosedChild  ChildDetails ,
      otherChildren           INTEGER (-1..MAX)
      /* The number of additional non-disclosed children (-1 indicates that
      the node is not prepared to disclose the number of other children) */ }

ChildDetails ::= SEQUENCE {
      orsSupported      BOOLEAN
                  /* Set to TRUE if the child OID node is ORS-supported */ ,
      arcDetails        UnicodeLabels }

Unicode Labels ::= SEQUENCE {
      numericLabel            INTEGER,
      non-numeric       SEQUENCE SIZE (0..MAX)OF
                        labels Non-numericUnicodeLabel }

Non-numericUnicodeLabel ::= UTF8String
      /* Restricted according to [ITU-T X.660], 7.2.5 */

ENCODING-CONTROL XER
GLOBAL-DEFAULTS MODIFIED-ENCODINGS

END
```

Annex D

Specification of the registration information (RINF) ORS service

(This annex forms an integral part of this Recommendation | International Standard)

D.1 General

D.1.1 All DNS zone files for an ORS-supported OID node shall contain a NAPTR resource record (see 6.3.2) with ORS service type **`RINF`** and with the regular expression **`information`** containing a URL for a registration information file (with a ".xml" extension) that provides registration information in accordance with D.2.

D.1.2 If an application supporting this ORS service receives a non-zero RCODE value from a query to an ORS client (using an OID node that it believes to be ORS-supported), it should attempt to report that failure, but the means of doing this is not standardized.

NOTE – Failure will always result (RCODE value 3) if that OID node is not ORS-supported. It can also result from incorrect configuration of DNS zone files, temporary or permanent failure of the DNS system, incorrect ORS client implementation, incorrect mapping of an OID-IRI by the application or for other reasons (see also 5.2.6).

D.1.3 If the RCODE returned is zero, the application-specific ORS resolution process shall access the XML file at the location returned by the general ORS resolution process in order to obtain registration information for the node identified by the OID-IRI submitted to the ORS client.

NOTE – If the file at that location is not an XML file conforming to D.2 then the application should attempt to report that failure, but the means of doing this is not standardized.

D.2 The RINF XML file

D.2.1 The RINF XML file shall conform to the EXTENDED-EXER encoding (specified in [ITU-T X.693]) of the ASN.1 module specified in D.2.5 . The semantics of the fields are included in this module specification as comment or by use of appropriate ASN.1 names, and are normative.

NOTE – In order to enable both ASN.1 and XML tools to be used in ORS applications, an (informative) XSD specification [b-XSD Structures, b-XSD Datatypes] for an identical XML encoding is available at http://www.itu.int/ITU-T/recommendations/fl.aspx?lang=4 (followed by a search for the Recommendation). If discrepancies are detected between the two specifications of allowed XML, there should be a Defect Report on this Recommendation | International Standard.

D.2.2 There are several privacy options available in the specification of the registration information XML file. An OID node may always choose to use **`<RegistrationInformation><noDisclosure/></RegistrationInformation>`**, revealing no registration information.

D.2.3 It shall not provide any of the optional fields of the first registrant or the current registrant without the permission of the current registrant.

NOTE – Contact information can be particularly sensitive.

D.2.4 The **`<RegistrantContactInformation>`** (if present) shall be enciphered in accordance with the security policy determined by the OID node. The means of distributing encipherment parameters is not standardized in this ITU-T Recommendation | International Standard.

D.2.5 The ASN.1 module (with semantics of the fields as ASN.1 comments is):

```
RINF-module
{joint-iso-itu-t ors(50) modules(1) rinf(1) version1(1)}
"/ORS/modules/rinf/version1"
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

RegistrationInformation ::= CHOICE {
      noDisclosure      NULL /* No information is provided */ ,
      disclosure        Information }
```

```
Information ::= SEQUENCE {
      firstRegistration      RegistrationDetails ,
      currentRegistration    RegistrationDetails }

RegistrationDetails ::= SEQUENCE {
      registrationDate             TIME(SETTINGS "Basic=Date
                                   Date=YMD") ,
      registeringOrganization      UTF8String ,
      registrant                   Encyphered {RegistrantContactDetails}
                                    OPTIONAL,
      descriptionOfUseCases        HTMLString ,
      additionalInformation        HTMLString }

Encyphered {ToBeEncrypted} ::= BIT STRING (CONSTRAINED BY {
      /* Shall be the result of applying encryption to the EXTENDED-XER
      encoding of */ ToBeEncrypted})

RegistrantContactDetails ::= SEQUENCE {
      familyName       UTF8String  OPTIONAL,
      givenName        UTF8String  OPTIONAL,
      e-mailAddress    UTF8String  OPTIONAL,
      phone            IA5String   OPTIONAL -- Starting with "+" -- ,
      fax              IA5String   OPTIONAL -- Starting with "+" -- ,
      postalAddress    SEQUENCE OF UTF8String OPTIONAL}

HTMLString ::= UTF8String(CONSTRAINED BY {
     /* Shall be a valid HTML document (see [W3C HTML])using only the markups
        <p>, <b>, </b>, <i>, </i>, <br/>, <a href> and </a> */})

END
```

Annex E

Specification of the module information (MINF) ORS service

(This annex forms an integral part of this Recommendation | International Standard)

E.1 Some (but not all) ORS-supported OID nodes identify an ASN.1 or XSD module. Where they do not, there are no NAPTR records for this ORS service, and a query to an ORS client will normally return an RCODE of zero with no information.

E.2 All DNS zone files for an ORS-supported OID node that identifies an ASN.1 or XSD module shall contain a NAPTR resource record (see 6.3.2) with ORS service type **`MINF`** and with the regular expression **`information`** which is a URL for a text file (with an **`asn`** or **`xsd`** extension) that contains the module specification.

E.3 If an application supporting this ORS service receives a non-zero RCODE value (or a zero value with no information) from a query to an ORS client (using an OID node that it believes to be ORS-supported and to identify an ASN.1 or XSD module), it should attempt to report that failure, but the means of doing this is not standardized.

NOTE – Failure will always result (RCODE value 3) if that OID node is not ORS-supported. If the OID node does not have an associated ASN.1 or XSD module, an RCODE of zero and no information will result. It can also result from incorrect configuration of DNS zone files, temporary or permanent failure of the DNS system, incorrect ORS client implementation, incorrect mapping of an OID-IRI by the application or for other reasons (see also 5.2.6).

E.4 If the RCODE returned is zero, but there is no returned information, then the OID-IRI does not identify an ASN.1 or an XSD specification (unless the DNS system has been wrongly configured). Otherwise, the application-specific ORS resolution process shall access the file at the location returned by the general ORS resolution process in order to obtain the (ASN.1 or XSD) module specification identified in the OID-IRI submitted to the ORS client.

NOTE – If the file at that location is not a syntactically correct ASN.1 or XSD file then the application should attempt to report that failure, but the means of doing this is not standardized.

Annex F

Description of use cases

(This annex does not form an integral part of this Recommendation | International Standard)

F.1 The OID canonicalization (COID) ORS service

F.1.1 The purpose of this service is to enable an application to determine whether two OID-IRI values refer to the same OID node.

F.1.2 This is achieved by the requirement (see Annex B) that all ORS-supported OID nodes contain the canonical form of the OID for that node. This canonical form can then be obtained from the ORS using any of the OID-IRI values that reference that OID node.

F.2 The child information (CINF) ORS service

F.2.1 The purpose of this service is to enable an application (such as a robot) to recursively discover the structure of ORS-supported OID nodes.

F.2.2 This is achieved by the inclusion of a NAPTR record containing a URL (which can be obtained by an ORS request) for an XML file that gives child information for the OID node. The XML file can then be retrieved by the application-specific resolution process (see Annex C)

F.2.3 There are a number of privacy provisions in Annex C that are available to restrict the return of child information to information that has the approval of child OID nodes, and the parent node can always choose non-disclosure.

F.3 The registration information (RINF) ORS service

F.3.1 The purpose of this service is to enable a description of the purpose and use cases of the OID allocation to be recorded, together with further information and the name of the registering organization.

F.3.2 This is achieved by the inclusion of a NAPTR record containing a URL (which can be obtained by an ORS request) for an XML file that gives registration information for the OID node. The XML file can then be retrieved by the application-specific resolution process (see Annex D).

F.3.3 This service provides for the non-disclosure of registration information, and for encryption of any contact details that are supplied within the XML file, in accordance with the security policy of the OID node.

F.4 The module information (MINF) ORS service

F.3.1 The purpose of this service is to enable the retrieval of an ASN.1 or XSD module associated with the OID node (if any).

F.3.2 This is achieved by the inclusion of a NAPTR record containing a URL (which can be obtained by an ORS request) for a text file with an **`.asn`** or **`.xsd`** XML file that contains the module (see Annex E).

F.3.3 There are no privacy or security implications of this service, but if DNSSEC(NSEC3) is available for the associated zone files, the application can set the security flag and ensure that a correct module has been returned.

Annex G

Examples of ORS operation

(This annex does not form an integral part of this Recommendation | International Standard)

G.1 Example of DNS zone files for the ORS

G.1.1 G.1 shows an example of zone file configuration to support the ORS.

NOTE – In the diagram, *www.anydomain.com* is used for the URL. This is purely for illustrative purpose and any URL can be used.

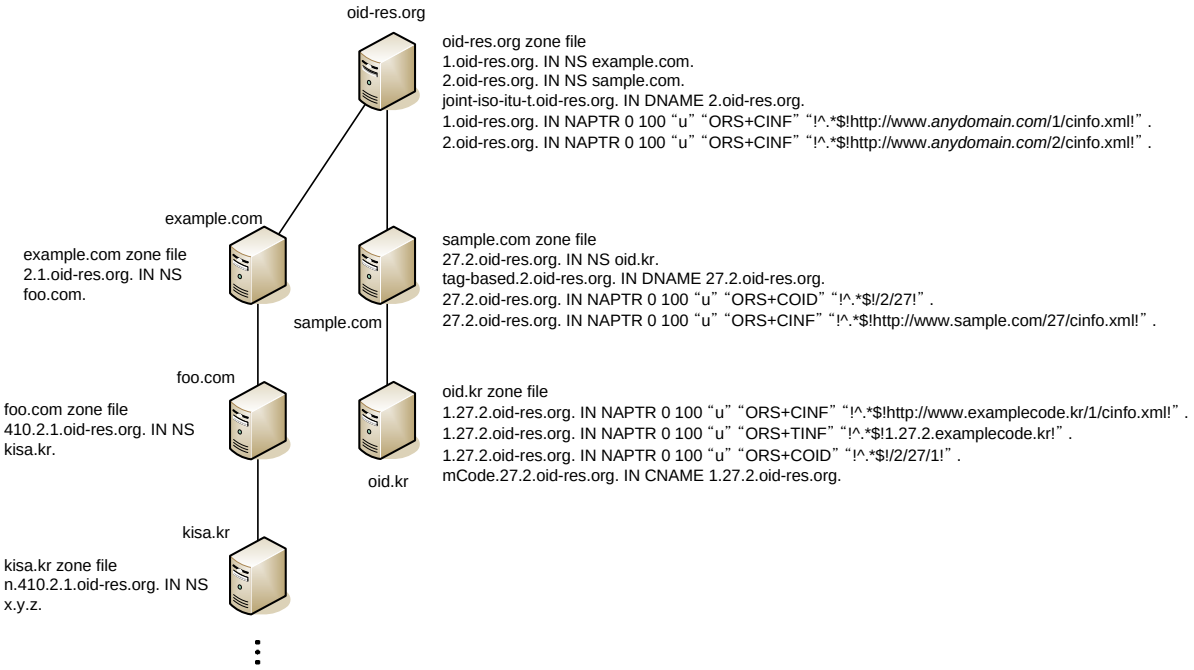

Figure 3 – An example of zone file configuration

G.2 Examples of NAPTR resource records

G.2.1 An example of a NAPTR resource record for OID canonicalization:

```
1.27.2.oid-res.org. IN NAPTR 0 100 "u" "ORS+COID" "!^.*$!/2/27/1!" .
```

G.2.2 An example of a NAPTR resource record for child information:

```
 2.oid-res.org. IN NAPTR 0 100 "u" "ORS+CINF"
"!^.*$!http://www.sample.com/2/cinfo.xml!" .
```

G.2.3 An example of a NAPTR resource record for registration information:

```
 2.oid-res.org. IN NAPTR 0 100 "u" "ORS+RINF"
"!^.*$!http://www.sample.com/27/rinfo.xml!" .
```

G.2.4 An example of a NAPTR resource record for module information:

```
 2.oid-res.org. IN NAPTR 0 100 "u" "ORS+MINF"
"!^.*$!http://www.sample.com/2/minfo.xsd!" .
```

G.2.5 An example of a NAPTR resource record for tag-based multimedia information:

```
1.27.2.oid-res.org. IN NAPTR 0 100 "u" "ORS+TINF"
"!^.*$!1.27.2.examplecode.kr!" .
```

Annex H

History

(This annex does not form an integral part of this Recommendation | International Standard)

In 1986, ITU-T and ISO/IEC recognised the need for unambiguous naming of objects on a world-wide basis, and jointly established an Object Identifier tree (now in the ITU-T X.660 series | ISO/IEC 9834 multi-part standard). The OID tree is a hierarchical allocation with a few top-level nodes standardised, and responsibilities for further child nodes left to the relevant parents, with minimal requirements from the Recommendations | International Standards.

From the very beginning, the OID tree was designed to allow any public or private organisation, etc to obtain a node in the OID tree, and to make sub-allocations.

NOTE – Information about many allocated OIDs can be obtained from the [b-OID Repository].

Initially, the OID tree nodes were in a strict set of levels, with each node at any level having a set of arcs from that node to nodes at the next level.

From the beginning, arcs were identified by unambiguous integer values (called "integer-valued Unicode labels" in the International Object Identifier Tree), but identifiers (not necessarily unambiguous or unique, and with a very restricted ASCII alphabet) could also be associated with each arc.

These identifiers are extensively used in human-readable ASN.1 OID notation (see ITU-T X.680 | ISO/IEC 8824-1), but are not relevant for this Recommendation | International Standard, should be ignored, and are not normally used in the ORS.

In 2002, the concept of "Unicode labels" (names using any Unicode characters, see ITU-T X.660 | ISO/IEC 9834-1) was introduced as an alternative form of unambiguous naming of an OID arc, and the OID tree was renamed as the International OID tree. Whilst unambiguous (the same Unicode label cannot be used on two separate arcs from the same parent), the Unicode labels are not unique: any arc (including long arcs) can have multiple Unicode labels, but all arcs that are not long arcs are required to have a single unambiguous integer-valued Unicode label.

Thus identifying a node now requires the use of a series of (unambiguous) Unicode labels from the root of the International OID tree to the node being identified (possibly using only integer-valued Unicode labels). These identifications are called an OID-IRI notation, to distinguish it from the old OID notations (which are still available) and consists of a series of Unicode labels (possibly numeric) separated by the "/" character. This identification scheme for a node is also registered with IANA[1] as the "oid:" IRI scheme.

[1] Currently provisionally assigned (see http://www.iana.org/assignments/uri-schemes.html).

Annex I

Bibliography

(This annex does not form an integral part of this Recommendation | International Standard)

[b-IETF RFC 1594] IETF RFC 1594:1994, *Answers to Commonly asked "New Internet User" Questions*.

[b-ITU-T H.IRP] Draft Recommendation ITU-T H.IRP, *ID resolution protocols for multimedia information access triggered by tag-based identification.*

[b-ITU-T X.cybex-disc-oid] Draft Recommendation ITU-T X.cybex-disc-oid, *OID-based discovery mechanisms in the exchange of cybersecurity information.*

[b-OID Repository] *The OID Repository*, http://www.oid-info.com.

[b-XSD Structures] *XML Schema Part 1: Structures*, W3C Recommendation, Copyright © [2 May 2001] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2001/REC-xmlschema-1-20010502.

[b-XSD Datatypes] *XML Schema Part 2: Datatypes*, W3C Recommendation, Copyright © [2 May 2001] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2001/REC-xmlschema-2-20010502.