INTERNATIONAL STANDARD

ISO/IEC 29168-1

Second edition
2023-03

Information technology — Open systems interconnection —

Part 1: Object identifier resolution system

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) —

Partie 1: Système de résolution d'identificateur d'objet

Reference number
ISO/IEC 29168-1:2023(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs)

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by ITU-T as ITU-T X.672 and drafted in accordance with its editorial rules, in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems.*

This second edition cancels and replaces the first edition (ISO/IEC 29168-1:2011), which has been technically revised.

A list of all parts in the ISO/IEC 29168 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

INTERNATIONAL STANDARD ISO/IEC 29168-1
RECOMMENDATION ITU-T X.672

Information technology – Open systems interconnection – Object identifier resolution system

Summary

Recommendation ITU-T X.672 | International Standard ISO/IEC 29168-1 specifies the object identifier (OID) resolution system (ORS). This enables (arbitrary) information to be associated with any ORS-supported OID node (of the international OID tree defined in Rec. 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 Abstract Syntax Notation One (ASN.1) OID-internationalized resource identifier value to identify the node.

Currently defined application information for a node includes the canonical form of an international OID, 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.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.672	2010-08-29	17	11.1002/1000/10831
2.0	ITU-T X.672	2022-06-06	17	11.1002/1000/14780

Keywords

Object identifier resolution system, object identifier, OID, ORS.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Introduction

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

It uses a mapping of the International OID tree naming scheme (using OID-internationalized resource identifier (OID-IRI) values) on to the domain name system (DNS) naming scheme (see 7.3).

This Recommendation | International Standard specifies requirements for the management of DNS zone files that are mapped from ORS-supported OID nodes to provide (standardized) information related to an international OID 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 canonical OID (COID) ORS service, supporting IRI comparison of names in the IETF "oid" IRI scheme (see Annex B);
- an application to determine child information (CINF) 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; RINF): the RINF service (see Annex D);
- an application to obtain a reference to the Abstract Syntax Notation One (ASN.1) module (if any) associated with a node: the module information (MINF) service (see Annex E);
- support for access to multimedia information (triggered by tag-based identification) using the ORS;
- support for access to information contained in an OID node that relates to cybersecurity features.

Three requirements emerged in 2019-2020:

- enhancement of the local performance of OID resolution to reduce the response time;
- high availability of the ORS;
- resolution of ORS-supported OID nodes for which not all superior OID nodes are ORS supported.

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 decided to map the OID tree into a part of the DNS tree (see IETF RFC 1035), with the root of the international OID tree mapped into .oid-res.org (see 7.3).

The mapping is from any OID-IRI value that identifies an international OID node into a DNS name (in the ORS 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 OID-IRI identifications for that international OID 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.

All DNS zone files for the ORS domain correspond to ORS-supported OID nodes, but not all DNS names algorithmically mapped from an OID-IRI are present in the DNS. All DNS zone files in the ORS domain are required to conform 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 naming authority pointer (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.

The procedures for the appointment of the ORS operational agency are contained in ISO/IEC 29168-2. These procedures involve only ISO/IEC for appointment and contractual purposes. They do not have any ITU-T involvement.

Clause 5 provides an overview of the ORS architecture and its interaction with the DNS.

Clause 6 specifies the requirements and restrictions on DNS zone files in the ORS 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 the use of delegation name (DNAME) DNS resource records and NAPTR resource records using a service field commencing "ORS+". Use of other DNS resource records lie outside the scope of this Recommendation | International Standard, and are neither forbidden (except when they would conflict with the 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 for 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 to 5.2.6, 6.4, 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 implementation guidance for a local cache and copies of ORS zones.

Annex I (informative) provides operational guidance for ORS operators.

Annex J (informative) explains the changes introduced in this edition of this Recommendation | International Standard.

Annex K (informative) provides a short history of the development of the international OID tree.

Annex L (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 object identifier (OID) resolution system (ORS), including the overall architecture and a resolution mechanism based on the domain name system (DNS).

This Recommendation | International Standard 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).

This Recommendation | International Standard does not restrict the number of applications it can support.

This Recommendation | International Standard 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 ORS has no role in the allocation or registration of OID nodes.

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 program interface is platform and software dependent, and lies outside the scope of this Recommendation | International Standard.

A special behaviour of an ORS client is specified to cache OID information in order to reduce the response time of OID resolution. This Recommendation | International Standard also specifies a mechanism to resolve an OID node when one of its superior OID nodes is not ORS supported.

This Recommendation | International Standard 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 in the ORS 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

– Recommendations ITU-T X.660 (2011) | ISO/IEC 9834-1:2012, *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree*.

– Recommendation ITU-T X.693 (2021) | ISO/IEC 8825-4:2021, *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)*.

2.2 Additional references

– Recommendation ITU-T X.675 (2015), *OID-based resolution framework for heterogeneous identifiers and locators*.

– 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 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 its entries listed in this clause.

- IETF RFC 7564 (2015), *PRECIS framework: Preparation, enforcement, and comparison of internationalized strings in application protocols*.
- Unicode Consortium (2021). *Unicode standard*, Version 14.0.0. Mountain View, CA: Unicode Consortium. Available [viewed 2022-07-27] at: https://www.unicode.org/versions/Unicode14.0.0/UnicodeStandard-14.0.pdf.

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 Rec. ITU-T X.660 | ISO/IEC 9834-1:

a) object identifier;
b) integer-valued Unicode label;
c) international object identifier tree;
d) long arc;
e) OID-internationalized resource identifier;
f) Registration Authority;
g) 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 AXFR: DNS zone transfer protocol.

NOTE – See IETF RFC 5936.

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

NOTE – An OID-IRI is an ASN.1 type defined in Rec. 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 Internet Assigned Numbers Authority (IANA) "oid:" internationalized resource identifier/uniform resource identifier (IRI/URI) scheme, with the omission of the initial "oid:".

3.2.4 delegation name (DNAME): A DNS resource record used to create an alias for a domain name and all of its subdomains.

3.2.5 DNS delegation: The process to create a separate zone in the DNS name space beneath the top name of a given domain.

NOTE 1 – See IETF RFC 7719.

NOTE 2 - Delegation happens when a name server RRset is added in the parent zone for the child origin, which is the domain name that appears at the top of the child zone.

3.2.6 DNS-mapped name: The result of transforming an OID-IRI value to an FQDN.

NOTE 1 – See 7.3.

NOTE 2 – The DNS-mapped name 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.

3.2.7 DNS name server (NS): A DNS resource record providing the authoritative name server for a domain.

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

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

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

3.2.10 fully qualified domain name: The name used in a DNS look-up operation.

NOTE – See IETF RFC 1594.

3.2.11 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.

3.2.12 local cache: A DNS cache server which synchronizes and hosts an ORS zone locally, based on a local configuration.

3.2.13 local resolution: ORS resolution using a local cache.

3.2.14 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.

3.2.15 OID resolution process: Process which provides information associated with an OID.

NOTE – This information can be application-specific (see Figure 1 and the annexes).

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

3.2.17 operational agency procedure: The specification of an action required by the .oid-res.org operational agency.

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

3.2.19 ORS domain: The .oid-res.org domain.

3.2.20 ORS root: OID resolution system hosted at the ORS domain.

3.2.21 ORS root operational agency: Organization that manages the DNS server for the ORS root and some subordinate nodes.

3.2.22 ORS service: A character string (used in NAPTR resource records) that identifies an ORS service.

NOTE – see Annex A.

3.2.23 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.

NOTE 1 – See Annex A.

NOTE 2 – The canonical OID service specified in Annex B requires the presence of a NAPTR record in the associated DNS zone file.

NOTE 3 – The ORS root operational agency is required by the operational 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 or one of its superior OID nodes, which is able to set up a delegation for that OID node.

3.2.24 ORS zone: Part of a DNS zone containing authoritative information about one or more OID nodes.

NOTE 1 – For DNS zone, see section 2.4 of IETF RFC 1034.

3.2.25 parent OID node: The OID node that is immediately above an OID node towards the root of the international object identifier tree.

3.2.26 resource record set (RRset): A set of resource records with the same label, class and type, but with different data.

NOTE 1 – See IETF RFC 7719.

3.2.27 secondary server (slave): An authoritative server which uses zone transfer to retrieve the zone.

NOTE – See section 2.1 of IETF RFC 1996.

3.2.28 superior OID node: Any OID node that is above an OID node (including its parent OID) towards the root of the international object identifier tree.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ASN.1	Abstract Syntax Notation One
ASCII	American Standard Code for Information Interchange
CD	Checking Disabled
CINF	Child Information
COID	Canonical OID
CYBEX	Cybersecurity Exchange information
DNAME	Delegation Name
DNS	Domain Name System
DNSSEC	Domain Name System Security
DO	DNS security OK
FQDN	Fully Qualified Domain Name
HTTPs	Hypertext Transfer Protocol secure
IRI	Internationalized Resource Identifier
ISP	Internet Service Provider
LINF	Locator Information
MINF	Module Information
NAPTR	Naming Authority Pointer
NFKC	Normalization Form KC
NS	Name Server
OID	Object Identifier
OID-IRI	OID-Internationalized Resource Identifier
ORS	OID Resolution System
RCODE	Return Code
RINF	Registration Information
RRset	Resource Record set
sFTP	secure File Transfer Protocol
SOA	Start Of Authority
TINF	Tag-based multimedia access Information
UINF	URI Information
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XML	Extensible Markup Language
XSD	XML Schema Definition

5 OID resolution system architecture

5.1 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 uniform resource locator (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, e.g., the canonical OID (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.

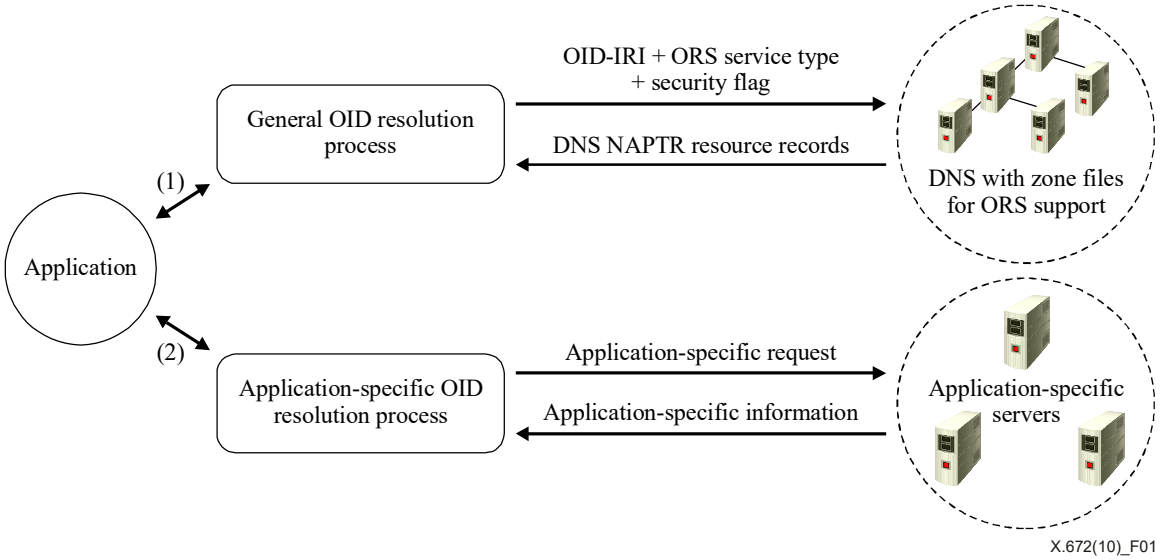

Figure 1 – OID resolution process

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 lies outside the scope of this Recommendation | International Standard. The realization of this architecture in hardware or software and its partitioning into separate modules is not constrained by this Recommendation | International Standard.

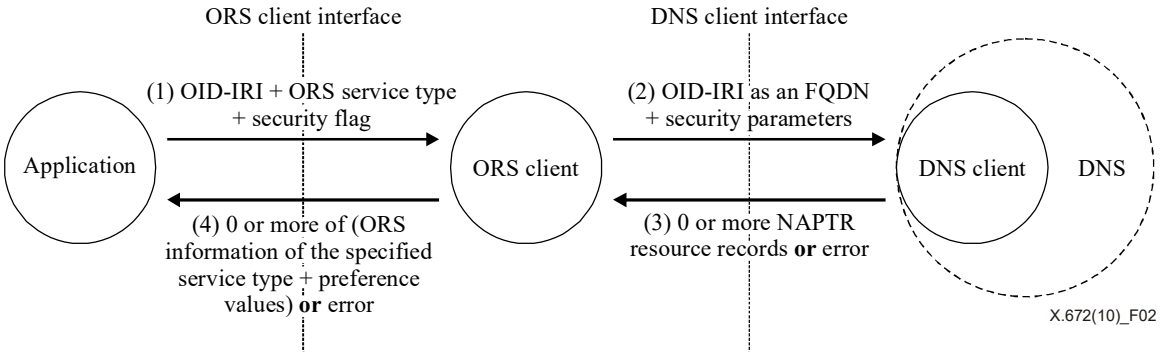

Figure 2 – Components of the general OID resolution system

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 a security flag, which determines whether a domain name system security (DNSSEC) extension – if available – is to be used (see 5.2.4).

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 operational agency procedures that the ORS root operational agency provide 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 for NAPTR resource records containing the requested ORS information type, as specified in 7.2. If the security flag is 1, then the DNS security OK (DO) parameter of the DNS query request shall be 1 and the checking disabled (CD) parameter shall be 0 (specified in IETF RFC 4033); otherwise, the DO and CD parameters are not passed.

5.2.5 (Step 3) The DNS client returns either zero or more NAPTR resource records, or an error (specified as a non-zero DNS return code (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 (the appropriate interpretation of the RCODE is given in Table 1). If the security flag was 1 (see 5.2.4), then only NAPTR resource records with an authenticated data flag (specified in IETF RFC 4033) set to 1 are returned; otherwise, all NAPTR resource records are returned.

Table 1 – Interpretation of DNS RCODE values

RCODE value	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

6 DNS zone files for the ORS domain

6.1 Overview

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

6.1.1 An OID node 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. The DNS-mapped names of an OID node can be either listed in the zone of its parent OID node or listed in its own zone if the owner of the OID node decides to administer the ORS-supported DNS zone itself (see clause 6.2.5 about the requirement for zone delegation in an ORS).

NOTE – The DNS is designed to allow divisions between the name hierarchy and the DNS authority structure to be created. The hierarchy DNS authority (zone) is not necessarily the same as the DNS name hierarchy. A more flattened structure of a DNS/ORS authority will make the OID resolution more efficient (an example is shown in Annex G).

6.1.3 If an OID node is not ORS supported, any ORS query using some of 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 not 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 resource records. Each of its child OID nodes may not be ORS supported.

6.1.5 The ORS root operational agency manages and maintains the DNS zone files corresponding to the OID nodes of the OID tree specified in the operational agency procedures in accordance with 6.2.

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

6.1.6 The ORS root operational agency is required (by operational 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 ORS root operational 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 DNAME resource records (as specified in 6.2) ensure that there is only a single 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.

6.1.9 Any OID node whose parent is not ORS supported can still implement the ORS with the help of one of its superior ORS-supported nodes. An example is given in Figure G.2. To avoid false information being published in the ORS, the inferior OID node should provide proof of ownership of the corresponding OID. The superior node is responsible for deciding what kind of proof is acceptable. The proof of ownership should include full path registration information (RINF) down to the inferior OID node.

NOTE – There should be an agreement between the node whose parent is not ORS supported and its superior ORS-supported nodes. The nature of the agreement lies outside the scope of this Recommendation | International Standard.

6.1.10 In order to enhance the high availability of the ORS root, the ORS root operational agency can implement secondary servers.

6.2 Requirements and restrictions on DNS zone files in the ORS domain

6.2.1 These requirements are placed on the ORS root operational agency (and recursively on all DNS zone files in the ORS domain).

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

6.2.3 All DNS zone files in the ORS domain shall (with appropriate use of DNAME resource 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 ORS domain shall not contain NAPTR resource records with a service field that 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.

6.2.5 For the delegation requirement, if the owner of the OID node decides to administer the ORS-supported DNS zone itself, a DNS delegation will be required and shall be set up by adding NS resource records in its parent zone for that OID node. If the parent of that OID node does not administer its DNS mapped name, a DNS delegation will be made in the zone of the superior node which is able to set up a delegation for that OID node.

NOTE – There should be an agreement between the two parties before the OID node is ORS supported. The nature of the agreement lies outside the scope of this Recommendation | International Standard.

6.3 Use of DNS resource records for ORS services

6.3.1 Use of DNAME resource records

6.3.1.1 If an OID node is ORS supported, then the zone file supporting the parent of that child OID node shall, for every non-integer-valued Unicode label identifying that child OID node, provide a DNAME resource record as specified in 6.3.1.3 and 6.3.1.4. For the purposes of this clause, the nodes that are linked by a long arc form a parent-child pair.

6.3.1.2 In addition, the zone file for any ORS-supported node shall contain a NAPTR record (see 6.3.2) for each supported ORS service type.

6.3.1.3 The DNAME resource record shall be preceded by:

a) the Unicode label on the arc to that child transformed as specified in section 4.1 of IETF RFC 3490, including case folding (see IETF RFC 7564) and punycode encoding (see IETF RFC 3492) using compatibility decomposition followed by canonical composition (normalization form KC (NFKC)) specified in Annex 15 of Unicode 5.2; then

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

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

EXAMPLE – See Figure G.1 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 the use of the DNS-mapped name from the canonical OID-IRI for the OID node that it is supporting, preceded by the FQDN form (of the canonical form) preceded by "**ors-dummy.**" (see the examples in G.1). It can also be accessed by other names derived from Unicode labels leading to that node, subject to the correct use of the DNAME resource record.

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!"	.

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

6.4 Security considerations

6.4.1 A DNS zone file manager is strongly recommended to sign NAPTR resource records, but is not required to do so. The ORS root operational agency is required to provide support for security as specified by IETF RFC 4033 and IETF RFC 5155.

6.4.2 In the case of queries with the security flag set to 1 by the application (see 5.2), then if any NAPTR resource record is not signed (or the certificate chain is not accepted), the DNS client will return an error code (and 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 in 7.3.

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 "**/**" (e.g., **/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) add "**ors-dummy.**" in front (producing, for example, **ors-dummy.27.2**);

f) append the string "**.oid-res.org.**" for the ORS domain (producing, for example, **ors-dummy.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) add "**ors-dummy.**" in front (producing for example, **ors-dummy.tag-based.joint-iso-itu-t**);

f) append the string "**.oid-res.org.**" for the ORS domain (producing, for example, **ors-dummy.tag-based.joint-iso-itu-t.oid-res.org.**);

g) transform the FQDN as specified in section 4.1 of IETF RFC 3490.

NOTE – This includes case folding and Unicode NFKC normalization (see IETF RFC 7564), followed by punycode encoding (see IETF RFC 3492).

7.4 Processing DNS results

7.4.1 If a DNS RCODE that is non-zero is returned, then an error return is passed to the application with the RCODE value.

NOTE – Guidance on the application to handle this is provided in Table 1.

7.4.2 If an RCODE of zero is returned, then the following steps shall be taken.

7.4.3 (Step 1) Select only those NAPTR resource records that have a flag field value "**u**".

7.4.4 (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 that was requested by the application.

7.4.5 (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.

7.4.6 (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.

7.6 Local performance considerations

7.6.1 An ORS client may experience high response time due to the lack of adjacent ORS servers and an inefficient local cache.

7.6.2 In order to enhance the ORS performance in terms of response time, the ORS client could serve ORS information locally and provide private copies of ORS zones frequently used when resolving OIDs.

NOTE – In such cases, it is the responsibility of the ORS client to keep private copies of ORS zones up-to-date and maintain the latest accurate information.

7.6.3 Optional local caching of ORS-related NAPTR records is done by normal queries periodically sent by an ORS client without coordination from the server side.

7.6.4 A DNS operator can keep a local copy of specific ORS zones using the normal DNS capabilities.

NOTE 1 – It is not mandatary for an ORS to implement local cache and ORS zone copies. More cases and advice are provided in Annex H.

NOTE 2– Zone transfer or online zone file service are optional for an ORS zone operator.

8 Requirements for 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 (e.g., 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 A.1.

Table A.1 – Assigned ORS service types

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	Tag-based multimedia access information (TINF)	Reserved for use in the OID resolution protocol specified by ITU-T and ISO/IEC JTC 1/SC 31.
Cybersecurity information	Cybersecurity exchange information (CYBEX)	Reserved for use in discovery mechanisms in the exchange of cybersecurity information specified by ITU-T.
URI	URI information (UINF)	ORS service with a regular expression containing a URI which indicates a service point for various service actions.
ID registry	Locator information (LINF)	ORS service with a regular expression containing a locator which indicates the IP address of an ID registry as specified in ITU-T X.675.

A.2 Proposals for support of new ORS services shall be submitted to the Rapporteur of the ITU-T Question and 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 and ISO/IEC JTC 1 Sub-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 website.

Annex B

Specification of the canonical OID (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 that is not zero, it should attempt to report that failure of the ORS system, but the means of doing this are 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 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 CINF file (with a ".xml" extension) that provides CINF 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 are 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 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 extensible markup language (XML) file at the location returned by the general ORS resolution process in order to obtain CINF 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 are not standardized.

C.2 CINF XML file

C.2.1 The CINF XML file shall conform to the EXTENDED-XER encoding (specified in Rec. ITU-T X.693 | ISO/IEC 8825-4) 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) XML schema definition (XSD) specification (XSD structures, XSD datatypes) for an identical XML encoding is available from ITU-T (2022), 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 CINF XML file. A parent node may always choose to use **`<ChildInformation><noDisclosure/></ChildInformation>`**, revealing no CINF. The parent may also list the number of undisclosed children (at its discretion) if it has agreement to disclose CINF 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(0) version1(1)}
             "/ORS/Modules/CINF/Version1"
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
ChildInformation ::= CHOICE {
             noDisclosure     NULL /* No information is provided */,
             disclosure       Information }
Information ::= SEQUENCE {
             disclosedChildren      SEQUENCE 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 */,
             unicodeLabels          UnicodeLabels }
UnicodeLabels ::= SEQUENCE {
             numericLabel     INTEGER,
             non-numeric      SEQUENCE OF
                              labels Non-numericUnicodeLabel }
Non-numericUnicodeLabel ::= UTF8String
```

```
            /* Restricted according to clause 7.2.5 of Rec. ITU-T X.660 | ISO/IEC 9834-
            1*/
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 RINF file (with a ".xml" extension) that provides RINF 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 are 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 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 RINF 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 are not standardized.

D.2 RINF XML file

D.2.1 The RINF XML file shall conform to the EXTENDED-XER encoding (specified in Rec. ITU-T X.693 | ISO/IEC 8825-4) 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 (XSD structures, XSD datatypes) for an identical XML encoding is available from ITU-T (2022), 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 RINF XML file. An OID node may always choose to use **`<RegistrationInformation><noDisclosure/></RegistrationInformation>`**, revealing no RINF.

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 **`<RegistrantContactDetails>`** (if present) shall be enciphered in accordance with the security policy determined by the OID node. The means of distributing encipherment parameters are not standardized in this Recommendation | International Standard.

D.2.5 The ASN.1 module (aligned with the requirements of Rec. ITU-T X.660 | ISO/IEC 9834-1), with added semantics of the fields as ASN.1 comments where necessary, is:

```
RINF-module
             {joint-iso-itu-t ors(50) modules(0) rinf(1) version1(1)}
             "/ORS/Modules/RINF/Version1"
        DEFINITIONS AUTOMATIC TAGS ::=
        BEGIN
        IMPORTS ALGORITHM, AlgorithmIdentifier{}, SupportedAlgorithms
        FROM AuthenticationFramework {joint-iso-itu-t ds(5) module(1)
        authenticationFramework(7) 6};
        /* This is an importation of security types from Rec. ITU-T X.509 | ISO/IEC 9594-8
        to provide the semantics and types used for encipherment */
RegistrationInformation ::= CHOICE {
             noDisclosure     NULL /* No information is provided */,
             disclosure       Information }
Information ::= SEQUENCE {
             description            HTMLString,
             additionalInformation  HTMLString OPTIONAL,
             firstRegistration      RegistrationDetails OPTIONAL,
             currentRegistration    RegistrationDetails OPTIONAL
```

```
                /* It is recommended that this information be provided if available. */}
RegistrationDetails ::= SEQUENCE {
            registrationDate            TIME(SETTINGS "Basic=Date
                                        Date=YMD") ,
            registrant            CHOICE {
                 non-enciphered              RegistrantContactDetails,
                 enciphered-registrant       SEQUENCE {
                      algorithmIdentifier    AlgorithmIdentifier{{SupportedAlgorithms}},
                      enciphered             OCTET STRING (CONSTRAINED BY {
                      /* Shall contain the result of applying the encipherment procedure
                         to the EXTENDED-XER encoding */ RegistrantContactDetails})}
            /* See clause 6.1 of Rec. ITU-T X.509 | ISO/IEC 9594-8  for how to encipher
            data. To obtain encryption keys, consult the parent node. */}}
RegistrantContactDetails ::= SEQUENCE {
            familyNameOrOrganization          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 Recommendation (2018), HTML 4.01
specification) using only the markups
        <p>, <b>, </b>, <i>, </i>, <br/>, <a href> and </a> */})
ENCODING-CONTROL XER
            GLOBAL-DEFAULTS MODIFIED-ENCODINGS
            BASE64 RegistrationDetails.registrant.enciphered-registrant.enciphered
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 are 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 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 are not standardized.

Annex F

Description of use cases

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

F.1 Canonical OID (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 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 CINF 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 CINF to information that has the approval of child OID nodes, and the parent node can always choose non-disclosure.

F.3 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 RINF 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 RINF, 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 Module information (MINF) ORS service

F.4.1 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.4.2 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.4.3 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 Figure 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 purposes and any URL can be used.

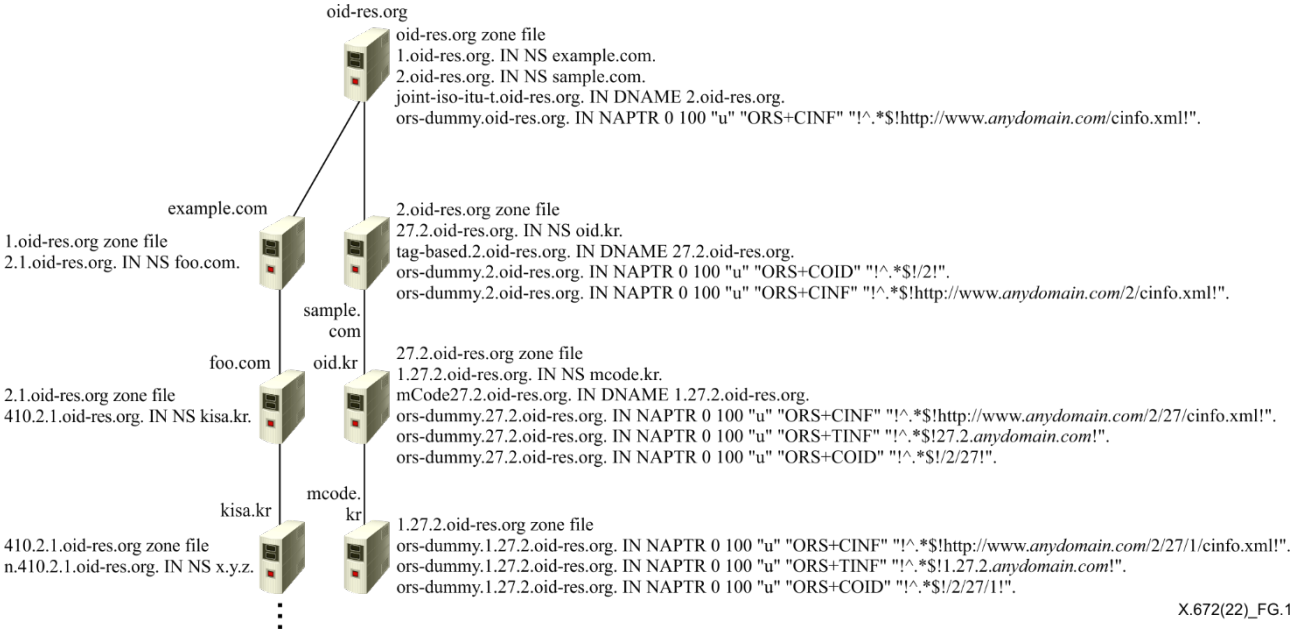

Figure G.1 – An example of zone file configuration

G.1.2 Figure G.2 shows an example of zone file configuration to support the addition of a node whose parent is not ORS supported

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

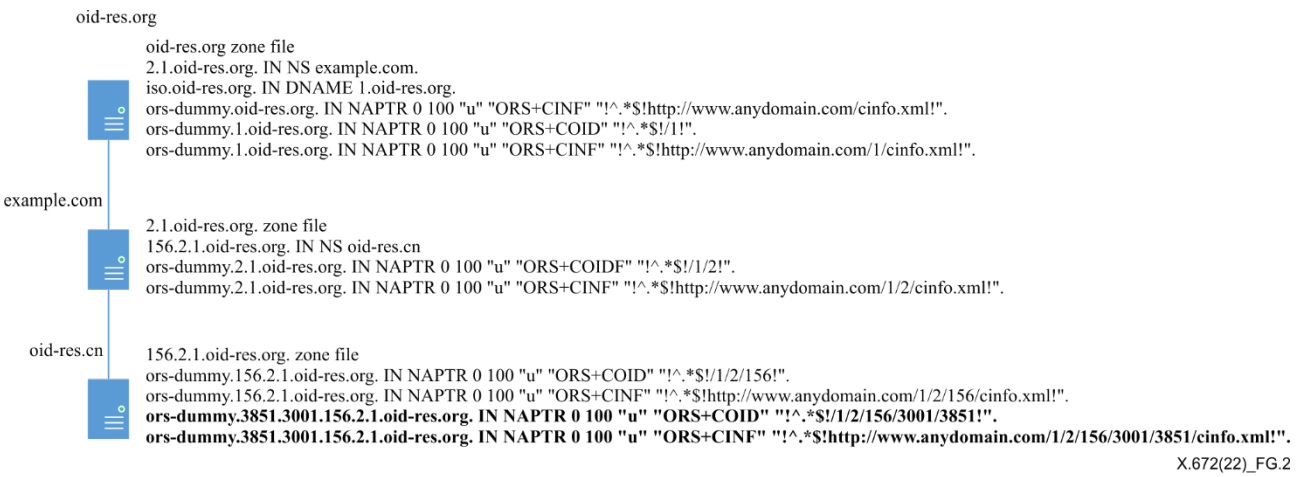

Figure G.2 – An example of zone file configuration to support the addition of a node whose parent is not ORS supported

G.2 Examples of NAPTR resource records

G.2.1 An example of a NAPTR resource record for OID canonicalization (see Annex B):

```
ors-dummy.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 CINF (see Annex C):

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

G.2.3 An example of a NAPTR resource record for RINF (see Annex D):

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

G.2.4 An example of a NAPTR resource record for module information (see Annex E):

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

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

```
ors-dummy.1.27.2.oid-res.org. IN NAPTR 0 100 "u" "ORS+TINF"
"!^.*$!1.27.2.anydomain.com!" .
```

Annex H

Implementation guidance for a local cache and copies of ORS zones

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

H.1 Local cache for OID resolution

In addition to NS operation, the cache managed by the DNS resolver is another effective means to reduce the response time. However, in the case of the ORS, the DNS resolver may be out of control of ORS client users (e.g., when the DNS resolver is provided by a local Internet service provider (ISP)). It is very hard to adopt a cache strategy in a local ISP resolver.

An ORS client is able to maintain a cache of popular OIDs that is pre-configured or learned from the recent OID resolution process. The cache can be kept warm by periodically fetching the popular OIDs considering their time to live.

A typical use case is in IoT grouped services introduced in Rec. ITU-T X.676. When an emergency (i.e., accident) occurs and people call an emergency service based on an OID resolution, the ORS client can respond promptly from the cache. In addition, it also increases the resilience of OID resolution against network failure.

H.2 Local copies of ORS zones

Another approach to serving ORS information locally is to provide private copies of ORS zones frequently used when resolving OIDs. An example use case is in a vertical industry (e.g., medical devices) where a single DNS zone might contain many names of interest to a specific application using OIDs.

An application doing OID resolution is required to take two steps. First, upon acceptance of a query for information from the ORS, the application constructs a DNS query for the FQDN. Second, this FQDN is submitted to the ORS server in the usual way. In addition, the ORS client also uses DNS caching for the root zone of the related OID. The system relies entirely on existing DNS technology but requires the ORS client to issue both standard queries and use DNS caching for zones related to commonly used arcs.

The advantage of this solution is that it solves the problem of local caching of the ORS-related NAPTR records by having the DNS client maintain a local DNS cache of the important zones.

H.3 Local copies of ORS zones independent of the local DNS

In clause H.2, the local copies of ORS zones are an internal component of the ORS client. Alternatively, the function can also act as an independent actor outside of the ORS client (called local root) as shown in Figure H.1. It is composed of a DNS authoritative server and a DNS resolver (local root client) running on the same host. The local root can cache and slave the important zone locally as specified in IETF RFC 7706.

NOTE 1 – IETF RFC 7706 was first developed to slave the root zone locally to reduce the response latency and provide more reliable answers for queries to the root. Although the primary goal of the design is to serve the root zone, the method can be used for any zone.

Assuming that an important zone, `example.oid-res.org`, is going to be slaved locally, the operation of `example.oid-res.org` on the local root client is described as follows:

1) retrieve a copy of the zone of `example.oid-res.org` from its NS;

   NOTE 2 – If the OID root zone is going to be hosted locally, the zone of `oid-res.org` should be retrieved.

2) start the authoritative service for `example.oid-res.org`.

The contents of the `example.oid-res.org` zone shall be refreshed using the timers from the start of authority (SOA) record in the zone file. In a resolver that is using an internal service for the `example.oid-res.org` zone, if the contents of the zone cannot be refreshed before the expiration time in the SOA record, the resolver shall immediately switch to forward the query to the standard DNS resolver.

In this design, the local resolution should switch to forward the query to the normal DNS client if the local authoritative server specified in IETF RFC 7706 failed.

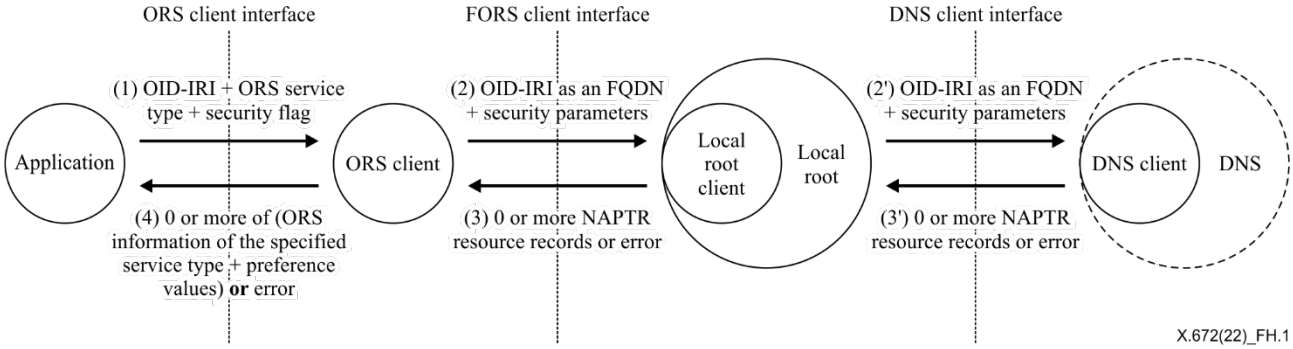

Figure H.1 – General OID resolution process including a local root component

Annex I

Operational guidance for ORS operators

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

Guidance on implementation, administration and operation of the ORS is given.

- ORS operators should check and follow best practice of DNS for the operation of the ORS. It is suggested that ORS operators cooperate with DNS operators to provide a service level agreement for the ORS service.
- To reduce the ORS response time and enhance its performance, it is strongly suggested that ORS operators deploy more secondary servers in different geographic location ORS root zone and other important ORS servers.
- ORS-supported zones that are willing to be "subscribed" by the local resolution of an ORS client can make the update-to-date zone publicly accessible. For example, the `example.oid-res.org` NS should open the access of its ORS zone file via DNS zone transfer, a web service, or a peer-to-peer file-sharing network. The local resolution can retrieve available ORS-supported zones via DNS AXFR, hypertext transfer protocol secure (HTTPs) or secure file transfer protocol (sFTP).
- A monitoring system should be designed and set up to periodically evaluate the availability and performance of an ORS implementation.

Annex J

Changes and compatibility of this edition of this Recommendation | International Standard

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

In this edition of this Recommendation | International Standard, a mechanism is specified to resolve an OID node when one of its superior nodes is not ORS supported. To achieve this, the ORS-supported superior node is able to administer the ORS-supported DNS zone for that OID node or to make a DNS delegation for that OID node. This is described in clauses 6.1.2, 6.1.9 and 6.2.5.

In clause 6.1.10, a behaviour of an ORS client is also recommended for caching OID information in order to reduce the response time for OID resolution.

In clause 6.1.10, it is suggested that the ORS root operational agency implement secondary servers in order to enhance the high availability and operational diversity of the ORS root.

Note that this edition of this Recommendation | International Standard does not change the OID resolution architecture established in clause 5, which specifies the OID resolution process and the OID resolution components. It does not change the way the ORS uses the DNS for general OID resolution process specified in clauses 5 and 7.

Annex K

History of object identifiers

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

In 1986, ITU-T and ISO/IEC recognized the need for unambiguous naming of objects on a worldwide basis, and jointly established an OID tree (now in the Rec. ITU-T X.660 series | ISO/IEC 9834 (all parts)). The OID tree is a hierarchical allocation with a few top-level nodes standardized, 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 organization to obtain a node in the OID tree and to make sub-allocations.

NOTE – Information about many allocated OIDs can be obtained from the OID Repository (Internet).

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 (long arcs – from the root to a node two or more levels down – were introduced later).

From the beginning, arcs were identified by unambiguous integer values (called "integer-valued Unicode labels" in the international OID tree), but identifiers (not necessarily unambiguous or unique, and with a very restricted American standard code for information interchange (ASCII) character set) could also be associated with each arc.

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

In 2002, the concept of "Unicode labels" (names using any Unicode characters, see Rec. 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. While unambiguous (the same Unicode label cannot be used on two separate arcs from the same parent), 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 OID-IRI notation, to distinguish them from the old OID notations (which are still available) and consist of a series of Unicode labels (possibly numeric) separated by the "/" character. This identification scheme for a node is also registered with IANA (Internet) as the "oid:" IRI scheme.

Bibliography

– Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

– Recommendations ITU-T X.66x series | ISO/IEC 9834-x (all parts), *Information technology –Procedures for the operation of object identifier registration authorities.*

– Recommendation ITU-T X.676 (2018), *Object identifier-based resolution framework for IoT grouped services.*

– Recommendations ITU-T X.680 (2021) | ISO/IEC 8824-1:2021, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

– ITU-T (2022). *Search for ITU-T Recommendations formal descriptions.* Geneva: International Telecommunication Union. Available [viewed 2022-07-31] at: https://www.itu.int/ITU-T/recommendations/fl.aspx?lang=4

– ISO/IEC 29168-2:2011, *Information technology – Open systems interconnection – Part 2: Procedures for the object identifier resolution system operational agency*.

– IANA (Internet). *Uniform resource identifier (URI) schemes*. Marina del Rey, CA: Internet Assigned Numbers Authority. Available [viewed 2022-07-31] at: https://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml

– IETF RFC 1594 (1994), *FYI on questions and answers – Answers to commonly asked "new Internet user" questions*.

– IETF RFC 1996 (1996), *A mechanism for prompt notification of zone changes (DNS NOTIFY).*

– IETF RFC 5936 (2010), *DNS zone transfer protocol (AXFR)*.

– IETF RFC 7706 (2015), *Decreasing access time to root servers by running one on loopback*.

– IETF RFC 7719 (2015), *DNS terminology*.

– OID Repository (Internet). *Object identifier (OID) repository*, Paris: Orange. Available [viewed 2022-07-31] at: http://www.oid-info.com.

– W3C Recommendation (2018-03-27), *HTML 4.01 specification.* Available [viewed 2022-07-27] at: https://www.w3.org/TR/html401/ .

ICS 35.100.01

Price based on 26 pages