INTERNATIONAL STANDARD

ISO/IEC 29168-1

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 29168-1:2011(E)

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

Published in Switzerland

CONTENTS

Foreword

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

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

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

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

ISO/IEC 29168-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems* in collaboration with ITU-T. The identical text is published as Rec. ITU-T X.672 (08/2010).

ISO/IEC 29168 consists of the following parts, under the general title *Information technology — Open systems interconnection*:

— *Part 1: Object identifier resolution system*

— *Part 2: Procedures for the object identifier resolution system operational agency*

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 (standardized) 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 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.

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 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 .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 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.

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.

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 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 the use of DNAME 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 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 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 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 a short history of the development of the International OID tree.

Annex I (informative) provides bibliographic references.

INTERNATIONAL STANDARD
RECOMMENDATION ITU-T

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 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 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 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

- Recommendation ITU-T X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- Recommendations ITU-T X.660 series | ISO/IEC 9834 multi-part standard, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities*.
- Recommendations ITU-T X.680 (2008) series | ISO/IEC 8824:2008 multi-part standard, *Information technology – Abstract Syntax Notation One (ASN.1)*.
- Recommendation 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 (2002), *The Unicode Standard, Version 3.2.0,* The Unicode Consortium (Reading, MA, Addison-Wesley).
- W3C, *HTML 4.01 Specification*, W3C Recommendation 24 December 1999, http://www.w3.org/TR/1999/REC-html401-19991224.

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 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 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 IANA "oid:" IRI/URI scheme, with the omission of the initial "oid:".

3.2.3 DNS delegation name (DNAME): A DNS resource record used to create an alias for a domain name and all of its sub-domains.

3.2.4 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.

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

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

3.2.7 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.

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

3.2.9 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.

3.2.10 operational agency procedures: The specification of the actions required by the .oid-res.org operational agency.

3.2.11 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.

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

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

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

3.2.14 .oid-res.org operational agency: Organization that manages the DNS server for .oid-res.org and some subordinate nodes.

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

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

3.2.17 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 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.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AD	Authenticated Data
CD	Checking Disabled
CINF	Child Information
COID	Canonical OID
CYBEX	Cybersecurity Exchange Information
DNAME	(DNS) Delegation Name
DNS	Domain Name System
DO	DNS Security OK
FQDN	Fully Qualified Domain Name
MINF	Module Information
NAPTR	(DNS) Naming Authority Pointer
NS	(DNS) Name Server
OID	Object Identifier
OID-IRI	OID Internationalized Resource Identifier (see Note in 3.2.2)
ORS	OID Resolution System
RCODE	(DNS) Return Code
RINF	Registration Information
TINF	Tag-based multimedia access Information
URL	Uniform Resource Locator

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 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.

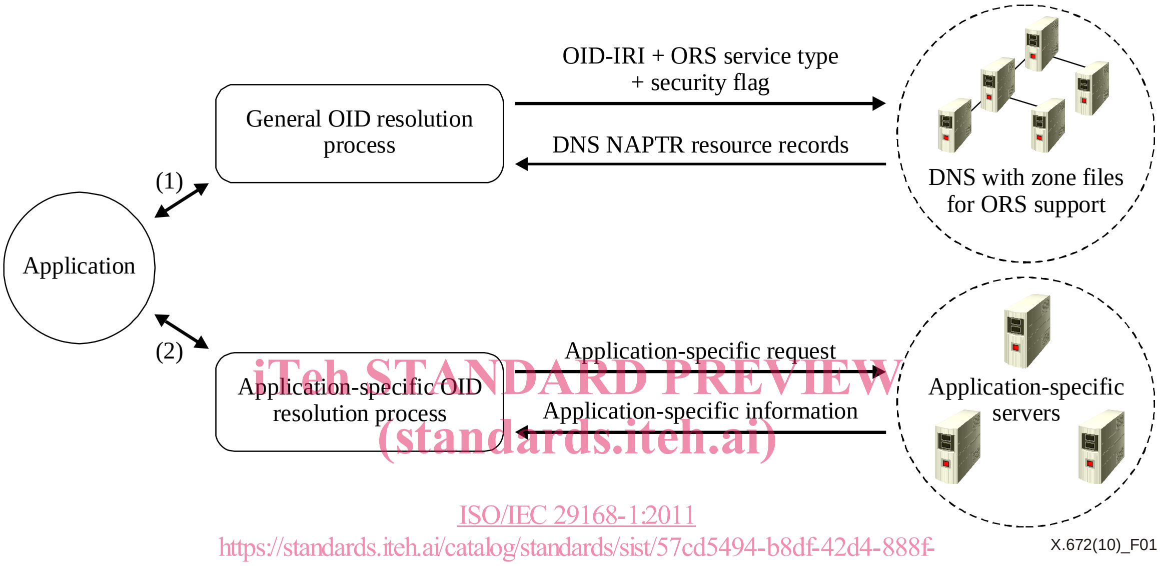
OID-IRI + ORS service type
+ security flag
General OID resolution process
DNS NAPTR resource records
DNS with zone files for ORS support
(1)
Application
(2)
Application-specific request
Application-specific OID resolution process
Application-specific information
Application-specific servers
X.672(10)_F01

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 is not in 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.

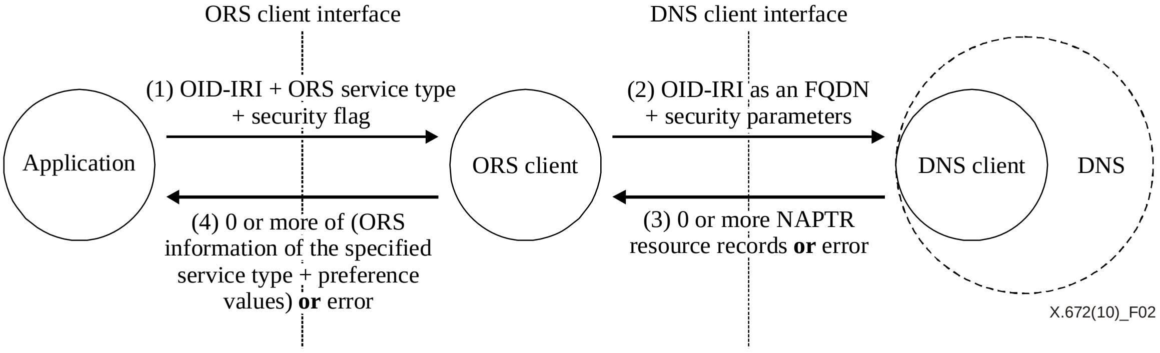
ORS client interface
DNS client interface
(1) OID-IRI + ORS service type
+ security flag
Application
ORS client
(2) OID-IRI as an FQDN
+ security parameters
DNS client
DNS
(4) 0 or more of (ORS information of the specified service type + preference values) or error
(3) 0 or more NAPTR resource records or error
X.672(10)_F02

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". This determines whether DNSSEC – 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 .oid-res.org operational 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 for NAPTR resource records containing the requested ORS information type, as specified in 7.2. If the security flag is 1, then the DO parameter of the DNS query request shall be 1 and the 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 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 AD 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 .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 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 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 resource records. 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 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 .oid-res.org operational agency is required (by the 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.