Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14098
Date:	2009-10-13
Replaces:	
Document Type:	Text for CD ballot
Document Title:	Text for CD ballot, ISO/IEC 2nd CD 29168, Information technology – Open Systems Interconnection – Object Identifier Resolution System (ORS)
Document Source:	Project Editor
Project Number:	
Document Status:	As per the SC 6 Tokyo resolution 6.9.4, this document is authorized for 2nd CD ballot. SC 6 NBs are requested to ballot electronically on www.iso.org/jtc1/sc6 by 2010-01-13.
Action ID:	LB
Due Date:	2010-01-13
No. of Pages:	14

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

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

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

Title: **2nd CD text of ISO/IEC 29168**
Date: **12 October 2009**
Source: **Project Editor (Jun Seob LEE)**

This document contains 2nd CD text of ISO/IEC 29168.

INTERNATIONAL STANDARD ISO/IEC 29168

ITU-T RECOMMENDATION X.oid-res

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

Summary

This Recommendation | International Standard specifies the OID (Object Identifier) Resolution System which provides information associated with any object identified by an International Object Identifier. This associated information can be access information, child node information, canonical form of the International Object Identifier, or identifier structure information.

Keywords

OID, resolution, Object Identifier

CONTENTS

Information technology –
Open Systems Interconnection –
Object Identifier Resolution System

Introduction

This Recommendation | International Standard specifies an Object Identifier (OID) Resolution System which can provide information associated with any object identified by an International Object Identifier.

The OID Resolution System (ORS) is based on the hierarchical Domain Name System (DNS) and it maintains DNS zone files for OIDs.

This Recommendation | International Standard specifies the architecture of ORS, operation of this infrastructure and zone file configuration to providing information associated with OIDs.

The international OID tree introduced the concept of multiple “Unicode labels” (names of arcs in any language, using the Unicode character set) on each arc of the tree. It also introduced the concept of "long arcs", which are Unicode labels directly addressing a lower-level node from the OID root. These features are fully supported by the ORS.

The ORS is a part of the hierarchical DNS. Normally, all the nodes in the international OID tree will have Registration Authorities which will operate ORS server. But, some nodes which do not have Registration Authorities (high-level nodes of the OID tree) and associated information with OID for these nodes should be managed and supported by ORS root manager.

1 Scope

This Recommendation | International Standard specifies an ORS including the overall architecture and a DNS-based protocol. The ORS provides access to the information associated with a given OID using DNS servers.

The ORS consists of two processes: a general OID resolution process and an application-specific OID resolution process.

The general OID resolution process utilizes the DNS protocol (see RFC1035), and is fully specified in this Recommendation | International Standard.

The application-specific OID resolution process depends on the access information returned from the general OID resolution process, and is not standardized beyond the architectural discussions in clause 5.

This Recommendation | International Standard applies to the implementation, administration and maintenance of the ORS.

2 Normative references

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

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.660 (2008) series | ISO/IEC 9834:2008, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: General procedures.*
- ITU-T Recommendation X.680 (2008) series | ISO/IEC 8824:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

– ITU-T Recommendation X.690 (2008) series | ISO/IEC 8825:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Encoding Rules.*

2.2 Additional references

– IETF RFC 1035:1987, *Domain names – Implementation and specification*

– IETF RFC 2535:1999, *Domain Name System Security Extensions*

– IETF RFC 2915:2000, *The Naming Authority Pointer (NAPTR) DNS Resource Record*

– 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)*

– Unicode 5.2, *The Unicode Standard, Version 3.2.0:2002. The Unicode Consortium. (Reading, MA, Addison-Wesley)*

3 Definitions

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

3.1 Imported definitions

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

a) object identifier.

b) integer-valued Unicode label

c) international Object Identifier tree

d) OID international resource identifier

e) registration authority (RA)

f) Unicode label

3.2 Additional definitions

3.2.1 application-specific OID resolution process: Actions by an ORS client that retrieve application-specific information (in a non-standardized manner) from the information returned by the general OID resolution process (see clause 5)

3.2.2 general OID resolution process: The part of the ORS that returns information about any specified OID to an ORS client using the DNS protocol (see clause 5)

3.2.3 canonical form (of an OID international resource identifier): A form which uses only integer-valued Unicode labels

3.2.4 high-level nodes of the OID tree: Nodes of the OID tree that are specified in the Rec. ITU-T X.660 series | ISO/IEC 9824 series – see also 7.3

3.2.5 identifier structure information: Identifier processing rule. This rule is substitution syntax of identifier into certain form for identifier resolution process

3.2.6 OID resolution process: Process which translates an OID into information associated with that OID

3.2.7 OID Resolution System: System which provides OID resolution functions for any OID

3.2.8 ORS client: Client-side of the ORS which is responsible for initiating the OID resolution process

3.2.9 ORS root manager: Organization that manages DNS server for oid.foo. and maintains the zone files for the high-level nodes of the OID tree

NOTE – The location of ORS root server in DNS hierarchy is not decided yet. In this 2nd CD text "oid.foo." is used for domain name of ORS root server. This will be changed when the actual domain name is determined.

3.2.10 ORS server: Server-side of the ORS which supports the maintenance of a distributed database of information associated with OIDs, using the DNS servers

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DNS	Domain Name System
FQDN	Fully Qualified Domain Name
NAPTR	Naming Authority Pointer (see RFC 2915)
OID	Object Identifier
OID-IRI	OID international resource identifier
ORS	OID Resolution System

5 OID Resolution System Architecture

5.1 Overview

The overall architecture and operation of the ORS is illustrated in Figure 1. The ORS consists of two processes: a general OID resolution process and an application-specific OID resolution process. The general OID resolution process uses the DNS protocol between an ORS client and an ORS server. The ORS client submits an OID for resolution and this OID is resolved via a series of linked ORS servers. An ORS server sends information related to an object identified by the OID back to the ORS client.

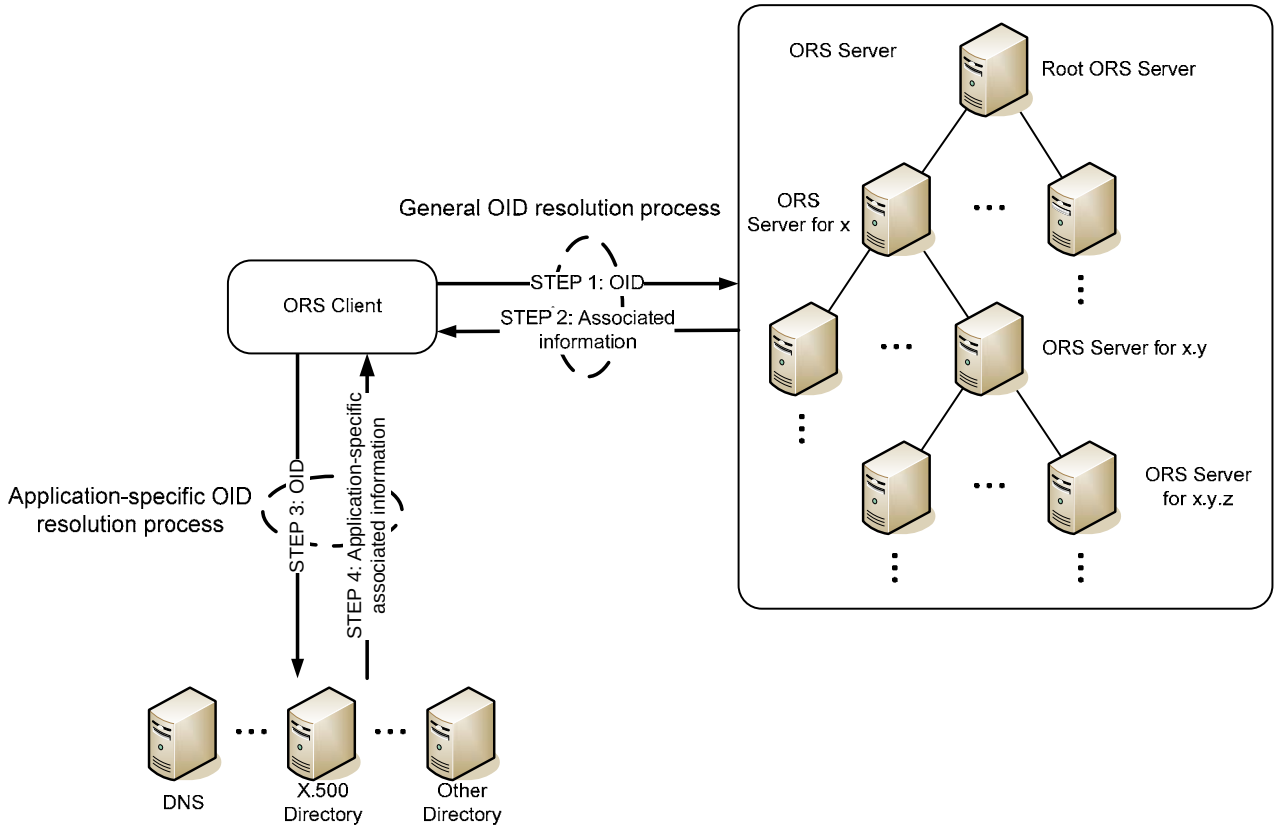

Figure 1. Architecture of the OID Resolution System

The associated information related to an object identified by the OID in STEP 2 in Figure 1 could be access information (see 6.3.2), child nodes information (see 6.3.3), the canonical form of the OID-IRI (see 6.3.4) or identifier structure information (see 6.3.5).

If the result of the general OID resolution process is child node information or the canonical form of the OID-IRI, then the OID resolution process is finished. If the result of the general OID resolution process is access information then the application-specific OID resolution process is initiated.

5.2 General OID resolution process

The general OID resolution process utilizes the DNS protocol. An ORS client always initiates this general OID resolution process. The result of the general OID resolution process could be access information, child nodes information, the canonical form of the OID-IRI or identifier structure information.

5.3 Application-specific OID resolution process

The application specific OID resolution process is only initiated when the result of the general OID resolution process is access information. In this process any kind of protocol can be used (depending on the returned URLs). The access information from the ORS server should include access methods and locations for obtaining additional information.

6 The DNS protocol for the general OID resolution process

6.1 General

The general OID resolution process uses the DNS protocol (see RFC 1035) and NAPTR Resource Record (see RFC 2915).

6.2 The form of a query to an ORS server

An input to an ORS server is a canonical form of an OID-IRI (for example, /2/27/99) or a non-canonical OID-IRI (for example, /joint-iso-itu-t/tag-based/examplecode). The ORS resolution client converts these object identifiers into an FQDN form (see RFC 1594 [2]) for use in a DNS query message (see 4.1 of RFC 1035) (for example, 99.27.2.oid.foo and examplecode.tag-based.joint-iso-itu-t.oid.foo). Figure 2 illustrates the DNS message format for a query.

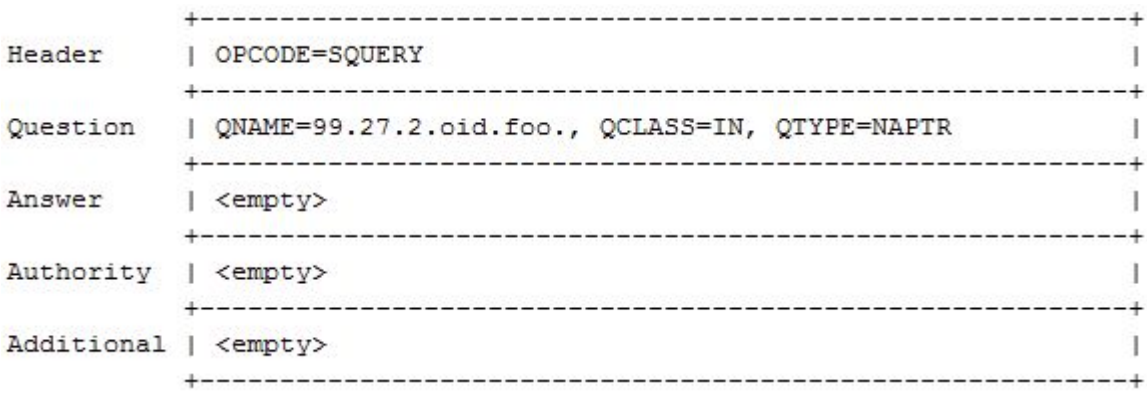

Figure 2. DNS message format for query

6.2.1 Converting the canonical form of an OID into FQDN form

The canonical form of an OID can be converted into FQDN form using the following procedure:

a) The canonical form of the OID is written in its full form. For example, /2/27/99

b) Remove the first "/", producing for example, 2/27/99

c) Put dots (".") instead of "/", producing for example, 2.27.99

d) Reverse the order, producing for example, 99.27.2

e) Append the string ".oid.foo.", producing for example, 99.27.2.oid.foo.

6.2.2 Converting a general OID-IRI into an FQDN form

A general OID-IRI can be converted into FQDN form using following procedure:

a) The OID-IRI is written in its full form. For example, /joint-iso-itu-t/tag-based/examplecode

b) Remove the first "/", producing for example, joint-iso-itu-t/tag-based/examplecode

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

d) Reverse the order, producing for example, examplecode.tag-based.joint-iso-itu-t

e) Append the string ".oid.foo.", producing for example, examplecode.tag-based.joint-iso-itu-t.oid.foo.

6.2.3 Encoding of Unicode labels

Each Unicode label shall be transformed as specified in IETF RFC 3490, clause 4 which references IETF RFC 3454 (case folding) and IETF RFC 3492 (punycode encoding). It also uses the Compatibility Decomposition, followed by Canonical Composition (KFCD) specified by Unicode 5.2.

6.3 Response from the ORS server

6.3.1 General

The result of a query to the ORS server can be access information, child node information the canonical form of the OID-IRI (which has the same information content as the value of an OID) or Identifier structure information. The result from the ORS server is delivered to the ORS client using a NAPTR Resource Record in DNS message format for a response. Figure 3 illustrates DNS response message format (see RFC 1035).

Header	OPCODE=SQUERY, RESPONSE, AA
Question	QNAME=99.27.2.oid.foo., QCLASS=IN, QTYPE=NAPTR
Answer	99.27.2.oid.foo. IN NAPTR 100 100 "flag" "service" "regexp" "replacement"
Authority	<empty>
Additional	<empty>

Figure 3. DNS message format for response

This Recommendation | International Standard specifies Service Parameters for the general OID resolution process. Service Parameters take the following form and are found in the service field of the NAPTR Resource Record.

Service-field = "O2I" servicespec

servicespec = "+" orpservice

orpservice = "AI" | "COI" | "CINFO" | "FFT" | "VFT"

A Unicode label that is to be entered into a DNS zone file shall be transformed as specified in 6.2.3.

6.3.2 Access information

The access information contains access protocol and access location for the application-specific OID resolution process. An access protocol is specified in the service field of a NAPTR Resource Record. An access location and method is specified as a URL in the RegExp field of NAPTR Resource Record.

An example of NAPTR Resource Record for access information is:

99.27.2.oid.foo. IN NAPTR 0 100 "u" "O2I+AI" "!^.*$!http://examplecode.kr!" .

This describes that the access information for OID {joint-iso-itu-t(2) tag-based(27) examplecode(99)}. In the application-specific OID resolution process, the client can access information associated with the OID using the HTTP protocol at "examplecode.kr".

6.3.3 Child node information

The child node information contains the number of child nodes and the primary integer value and all Unicode Labels of the child nodes in an XML file. The location of this XML file is specified as a URL in the RegExp field of the NAPTR Resource Record.

An example of a NAPTR Resource Record for access information is:

99.27.2.oid.foo. IN NAPTR 0 100 “u” “O2I+CINFO” “!^.*$!http://oid.kr/example.xml!” .

6.3.4 Canonical form of an OID-IRI

The canonical form of an OID-IRI is specified in the service field of a NAPTR Resource Record.

An example of a NAPTR Resource Record for the canonical form of an OID is:

examplecode.tag-based.joint-iso-itu-t.oid.foo. IN NAPTR 0 100 “u” “O2I+COI” “!^.*$!/2/27/99!” .

The Service Parameter “O2I+COI” indicates that this NAPTR Resource Record includes a canonical form of OID-IRI.

6.3.5 Identifier structure information

The identifier structure information is specified in the service field of a NAPTR Resource Record. It contains identifier processing rule. This rule is substitution syntax of identifier into certain form for identifier resolution process. For this purpose following Service Parameters are defined.

FFT: Fixed Form Type ID scheme. It indicates that RegExp field contains rule for converting ID into certain form for ID resolution process and it needs no more query to ORS

VFT: Variable Form Type ID scheme. It indicates that RegExp field contains rule for extracting some fields from an ID and it needs more query to ORS

An example of a NAPTR Resource Record for the identifier structure information is:

99.27.2.oid.foo. IN NAPTR 0 100 “u” “O2I+FFT’ “!^(.{3})(.{5}).{3}$!\\2.\\1.example.com!”.

Applying above RegExp to ID, it returns text string in form of “nnnnn.nnn.example.com” where n is a binary digit.

Another example of a NAPTR Resource Record for the identifier structure information is:

99.27.2.oid.foo. IN NAPTR 0 100 “u” “O2I+VFT” “!^(.{2}).{11}$!\\1!”.

Applying above RegExp to ID, it returns first 2 bits of ID which is totally 13 bits.

The ORS client converts OID into FQDN form as defined in clause 6.2 and sends it to the ORS server. When ORS client gets a NAPTR resource record with Service field value “FFT”, it applies the rule in RegExp field on ID and used that result for ID resolution process. When ORS client gets a NAPTR resource record with Service field value “VFT”, it applies the rule in RegExp field on ID and adding the result in front of OID in FQDN form. For example, if OID in FQDN form is “99.27.2.oid.foo” and result of query is “5” then virtual OID “5.9927.2.oid.foo” will be generated.

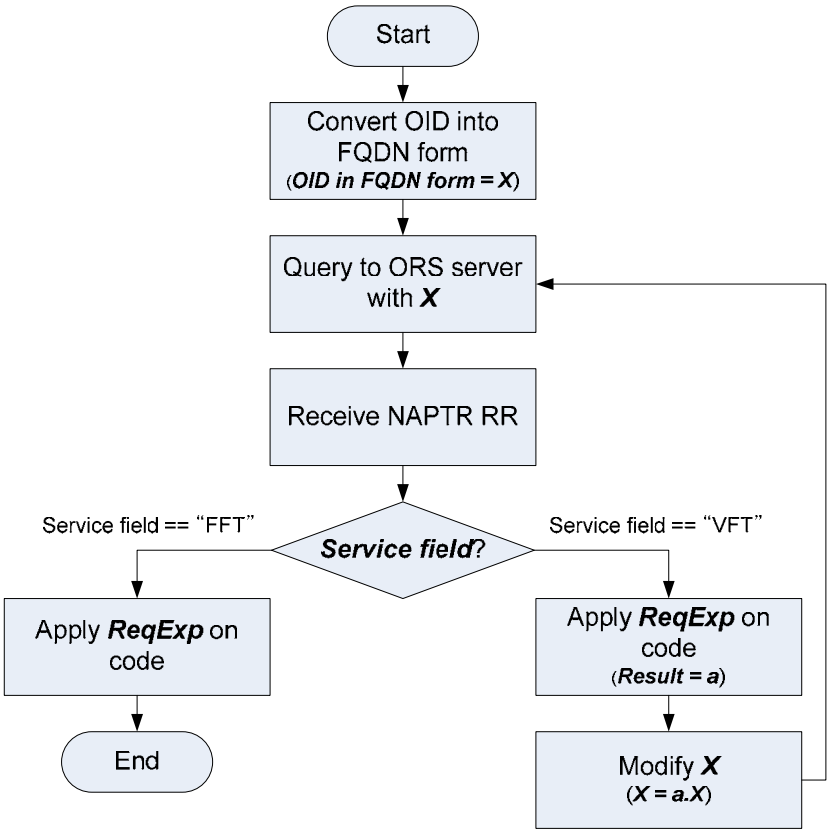

Figure 4. ORS client operation for identifier structure information

7 Configuration and operation of the OID Resolution System

7.1 Configuration of ORS

Figure 5 illustrates the hierarchical structure and the delegation structure of ORS servers.

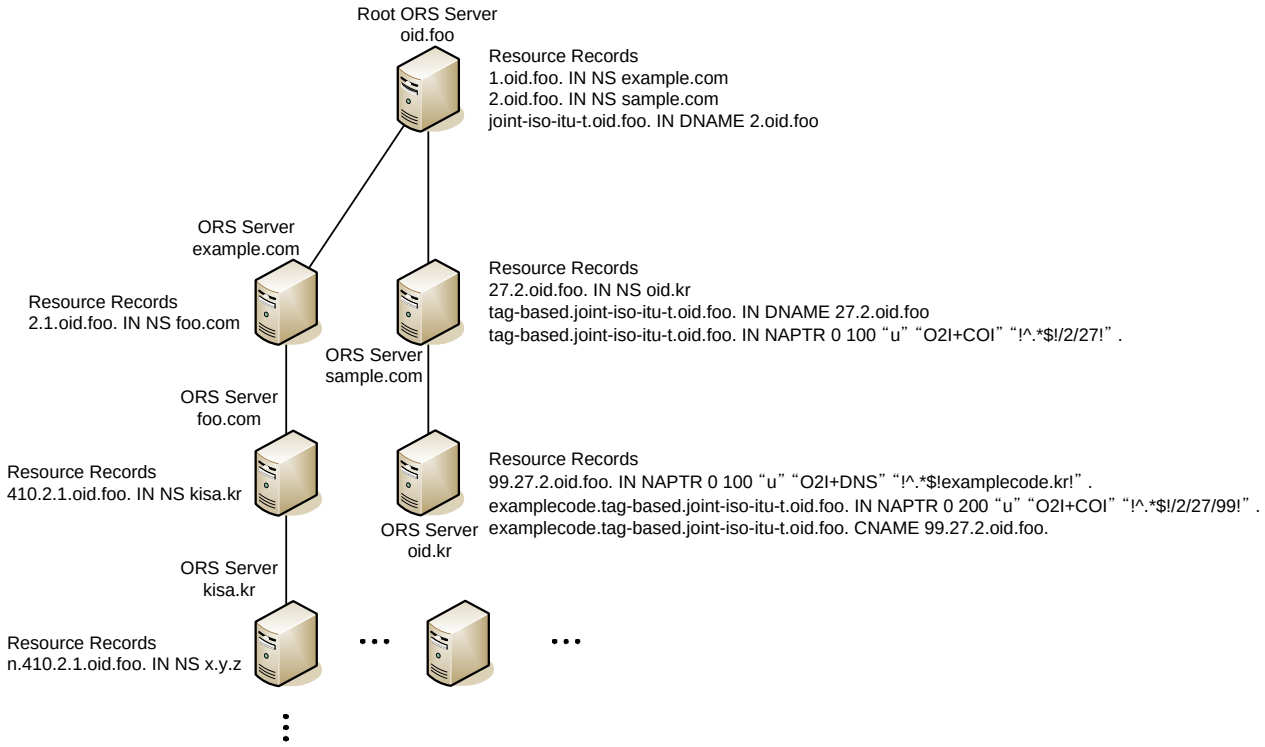

Figure 5. An example of the structure of ORS servers

The DNAME and CNAME Resource Records should be used to avoid exponential explosions of Resource Records in zone files to use Unicode labels and to allow later addition of new Unicode labels without changing Resource Records in a lower level zone files. The DNAME Resource Record should be used for non-leaf node and the CNAME Resource Record should be used for leaf node.

7.2 OID tree and DNS

The OID tree exists independently of the ORS support, and the allocation of OIDs and their optional inclusion in the OID Repository [1] are in no way affected by the ORS.

The OID tree has a canonical numeric form for identifying a node from the root of the OID tree by the integer-valued Unicode labels. It also has multiple Unicode labels for each arc of the tree.

It also has the concept of "long-arcs" from the root to a lower-level node, identified only by a Unicode label.

Some nodes of the OID tree will be mapped into DNS nodes. The root of the OID tree is mapped into the DNS node .oid.foo.

It will always be possible to obtain the canonical form of the OID-IRI with input of any sequence of Unicode labels leading to that node, including long arcs.

Associated information with the high-level nodes of the OID tree should be managed by ORS root manager.

The zone files for the high-level nodes of OID tree can be supported by a single server or multiple servers in accordance with normal practice for DNS implementation.

7.3 Zone file configuration for the high-level nodes of OID tree

ORS root manager should manage and maintain all the information for the high-level nodes of OID tree and all the long arcs form the root.

7.4 Operation of ORS

Figure 6 shows the operation example of general OID resolution process with the configuration as Figure 5.

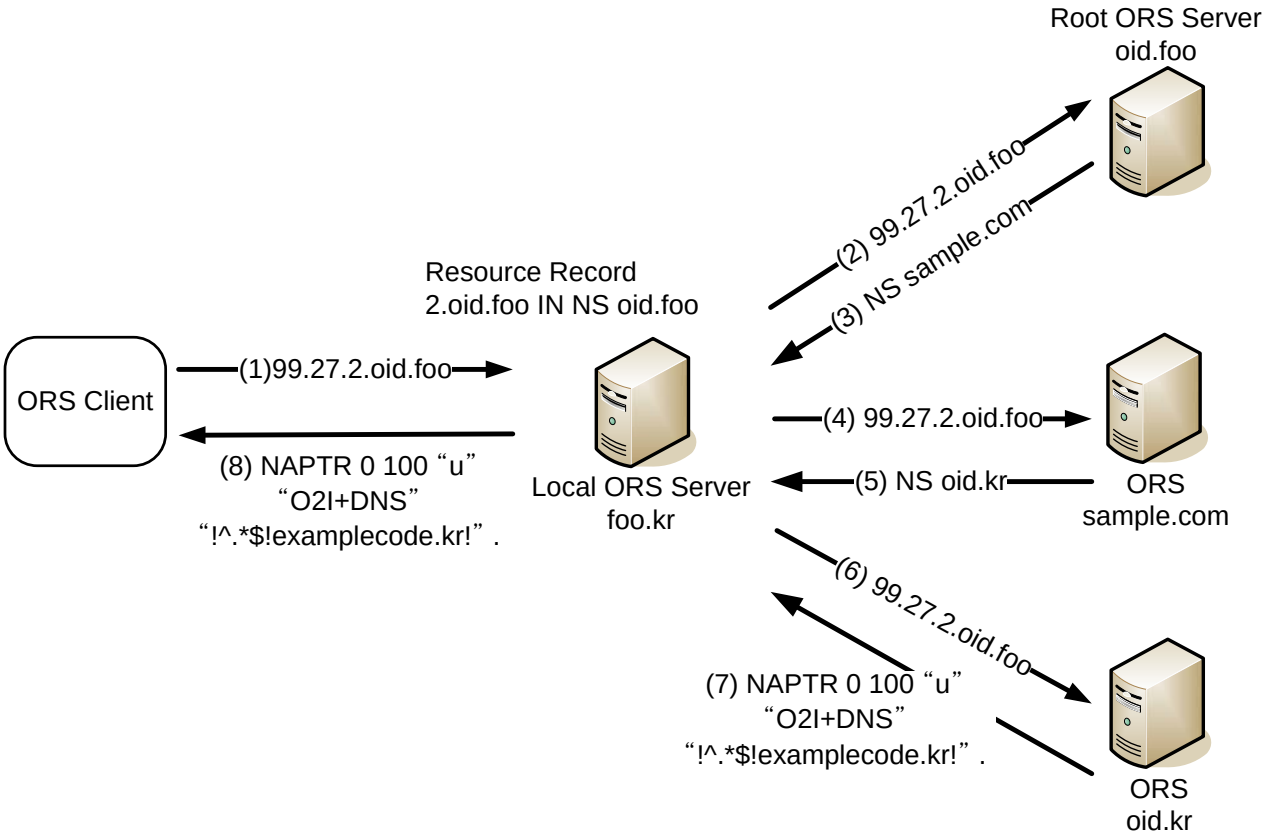

Figure 6. Example operation of general OID resolution process

8 Security issues

As the general OID resolution process in the ORS uses the DNS protocol, there is no mechanism for ensuring that the data one gets back is authentic. DNSSEC (RFC 2535) can be used in the general OID resolution process for information requiring a high degree of trust.

There are no other phishing issues introduced by X.oid-res other than those covered by ITU-T X.660 | ISO/IEC 9834-1.

Bibliography

[1] URL www.oid-info.com, *The OID Repository*