Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14071
Date:	2009-09-14
Replaces:	
Document Type:	Other Document (Defined)
Document Title:	UK's Proposed revision of CD1 ballot text, ISO/IEC CD 29168 Information technology - Open Systems Interconnection - Object Identifier Resolution System
Document Source:	National Body of UK
Project Number:	
Document Status:	For your information.
Action ID:	FYI
Due Date:	
No. of Pages:	17

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

INTERNATIONAL STANDARD ISO/IEC 29166

ITU-T RECOMMENDATION X.oid-res

삭제됨: XXXX

삭제됨: XXX

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, or the canonical form of the International Object Identifier.

삭제됨: OID

삭제됨: Resource Identifier (OID-IRI)

Keywords

OID, resolution, Object Identifier

Contact: Jun Seob LEE
ETRI
Republic of Korea

Tel: +82 42 860 3859
Fax: + 82 42 861 5404
Email: juns@etri.re.kr

CONTENTS

Information technology –
Open Systems Interconnection –
Object Identifier Resolution System

Introduction

(See GB 7)

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, provide the OID parent of that object makes its information (and that of children – with their agreement – publicly available).

삭제됨: s

The OID resolution system maps OID nodes into nodes of the hierarchical Domain Name System, and retrieves information from the zone files of the DNS nodes.

This Recommendation | International Standard specifies the operation of this infrastructure, and the means by which the owner of an OID can make use of it to make accessible on-line information related to the OID node.

The international OID tree introduced the concept of multiple "Unicode labels" (perhaps in different languages) on each arc of the tree, but with a canonical representation of a path using only the traditional integer-valued labels. It also introduced the concept of "long arcs", which are Unicode labels directly addressing (from the OID root) a lower-level node.

These features are fully supported by the ORS, which allows any identification of a node (using any Unicode label on the path two it, and including "long arcs", to return the canonical OID for that node.

An important concept is that of the partial DNS-OID-mirror. Not all OID nodes will need or will have DNS (and hence ORS) support. This is an optional feature. All the high-level nodes of the OID tree were initially provide with DNS support by the DNS OID RA as part of its initial actions. They form a fundamental part of the DNS-OID-mirror infrastructure. Other lower-level OID nodes are added on demand.

Adding a lower-level (child) OID node to the DNS-OID-mirror requires two things:

a) that the child desires it and that its parent agrees;

b that arrangements are established between the child and its parent for the hosting of the necessary DNS zone files on some server, and for any payments that may be exchanged between them.

The ORS also enables minimal information about its children to be associated with any OID node that is in the DNS-OID-mirror, and for that information to be returned by a DNS query on that OID (whether the child node is in the DNS-OID-mirror or not.

Finally, it is important to recognise that the ORS provides fully secure operation, using a DNS facility called DNSSEC (RFC 2535). This enables any information returned by the ORS to be digitally signed with an X.509 [1] certificate chain starting with a public key called a "trust anchor". The means of obtaining the trust anchor for ORS queries is specified in this Recommendation | International Standard (make sure it is – see discussions on IAB, ICANN or OID Repository).

It is also possible for application-specific information delivered by the ORS application-specific resolution process to be encrypted. There is no support in this version of the ORS for encryption key management, and the URLs returned by the ORS general resolution process (while authenticated) are not encrypted.

삭제됨:

1 Scope

This Recommendation | International Standard specifies an OID Resolution System including the overall architecture and a DNS-based protocol. The OID Resolution System provides access to authenticated information associated with a given OID using DNS servers. (See GB5 Q1).

삭제됨: the

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

삭제됨: .

The general OID resolution process utilizes the DNS (Domain Name System) 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 OID Resolution System.

2 Normative references (See GB 8)

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*

삭제됨: .

– IETF RFC 2181:1997, *Clarifications to the DNS Specification*

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

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

– IETF RFC 3403:2002, *Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database*

삭제됨: .

– IETF RFC 4033:2005, *DNS Security Introduction and Requirements*

삭제됨: .

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:

삭제됨: a) object identifier.

a) integer-valued Unicode label

b) international Object Identifier tree

c) OID international resource identifier

d) registration authority (RA)

f) relevant ITU-T Study Group

g) relevant ISO/IEC JTC 1 Sub-Committee

h) Unicode label

3.2 Additional definitions (see GB 9)

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

3.2.1new DNS protocol: the protocol specified in RFC1035 used for the general OID resolution process

3.2.1new general OID resolution process: that part of the OID resolution system that returns to an OID resolution client (using the DNS protocol) information about any specified OID (see clause 5)

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

3.2.1bis 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 and are supported in the initial deployment of the partial DNS-OID-mirror through the high-level OID DNS administrative Registration Authority (OID DNS RA) – see also 10.1

3.2.1ter high-level OID DNS administrative Registration Authority: that administrative Registration Authority appointed jointly by the relevant ITU-T Study Group and the relevant ISO/IEC JTC 1 Sub-Committee (see clause 10)

3.2.1quatobject identifier: the identification of an object by providing the sequence of Unicode labels on the arcs from the root of the international object identifier tree to the node representing that object.

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

3.2.3 OID Resolution System: system which provides OID resolution functions for any OID present in the DNS-OID-mirror

3.2.4 OID resolution client: client-side of the OID Resolution System which is responsible for initiating the OID resolution process

3.2.5 OID resolution server: part of the server-side of the OID Resolution System which supports the maintenance of a distributed database of information associated with OIDs, using the DNS servers

3.2.5bis partial DNS-OID-mirror: the set of nodes of the OID tree that have corresponding DNS zone files

NOTE – A node in the OID tree can only become part of the partial DNS-OID-mirror if its parent node is already part of the DNS-OID-mirror (see 10.3)

3.2.5ter trust anchor: the public key that provides a chain of authenticated public keys that enable an entry in the DNS-OID-mirror to be authenticated (see clause 6bis)

삭제됨: ized
삭제됨:
삭제됨: a
삭제됨: associated
삭제됨: e
삭제됨: a
삭제됨: the
삭제됨: the
삭제됨: ain
삭제됨: s
삭제됨: associated

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DNS	Domain Name System
FQDN	Fully Qualified Domain Name (see RFC 1594 [2])
NAPTR	Naming Authority Pointer (see RFC 2915)
OID	Object Identifier
OID-IRI	OID international resource identifier
ORS	See GB 6

삭제됨: ized

4bis Relation of DNS nodes and zone files to OID tree nodes (See GB 11)

4bis.1 The OID tree exists independently of the ORS DNS support, and the allocation of OIDs and their optional inclusion in the OID Repository [3] are in no way affected by the ORS.

4bis.2 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 from the root to a node. It also has (potentially, and particularly at the higher levels) multiple Unicode labels (catering for different languages) for each arc of the tree, thus providing multiple identification of lower-level nodes.

4bis.3 It also has the concept of "long-arcs" from the root to a lower-level node, identified only by a Unicode label.

4bis.4 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.xxx.yyy (eventually this will be determined). Any other node of the OID tree can potentially be mapped into a DNS node provided its parent node has been mapped to a DNS node, and the parent and child agree to its inclusion in the DNS-OID-mirror (see clause 10). The set of nodes of the OID tree mapped (at any point in time) to a DNS node is called the DNS-OID-mirror.

4bis.5 For OID nodes in the DNS-OID-mirror, there can (but need not) be application-specific references recorded in the zone files for the corresponding DNS node. For OID nodes in the DNS-OID-mirror, it will always be possible to obtain the canonical form of the OID reference using DNS look-up with input of any sequence of Unicode labels leading to that node, including long arcs.

4bis.6 In the initial deployment of the DNS-OID-mirror by the DNS OID RA, only high-level nodes of the OID tree were part of the DNS-OID-mirror (see clause 10), and there was no application-specific information associated with any of these nodes. Thus the sole functionality of the initial deployment of the DNS-OID-mirror was to provide a mapping to DNS and sufficient DNS zone files to:

a) map any OID represented in the DNS-OID-mirror into its canonical form;

b) return a statement that there is no associated information for a DNS-OID-mirror node, and that there are no OID children of the leaf nodes of that initial partial DNS-OID-mirror

4bis.7 Clause 10 specifies the procedures for "growing" the DNS-OID-mirror downwards, initially by interaction with the DNS OID RA, and for adding application-specific information to a DNS node in the DNS-OID-mirror.

4bis.8 For DNS nodes that mirror OID nodes, there will be a set of zone files for that node. Some of these may be supported by a single server for multiple zone files, and some may be mirrored to other DNS servers, in accordance with normal practice for DNS implementation. This is not generally of interest to the users of the ORS, but is described more fully in clause 10.

5 OID Resolution System Architecture

5.1 Overview

5.1.1 The overall architecture and operation of the OID Resolution System is illustrated in Figure 1. The OID Resolution System 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 OID resolution client and an OID resolution server. The OID resolution client submits an OID for resolution and this OID is resolved via a series of linked OID resolution servers. An OID resolution server sends information related to an object identified by the OID back to the OID resolution client.

삭제됨: the

삭제됨: the

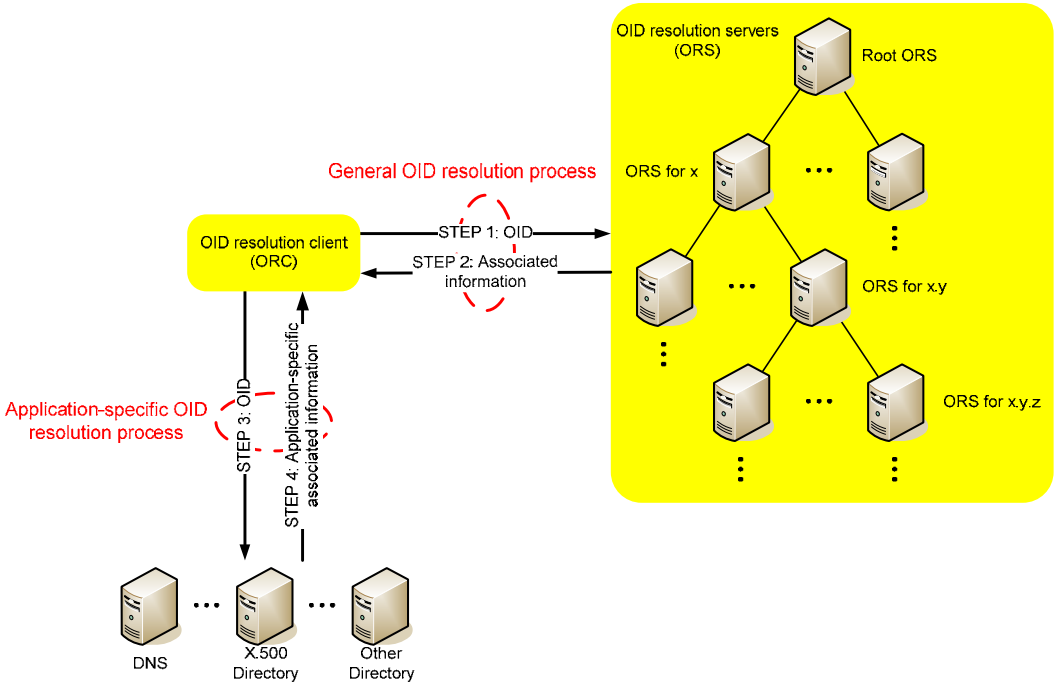

Figure 1. Architecture of the OID Resolution System

5.1.2 The associated information related to an object identified by the OID in STEP 2 in Figure 1 could be access information (see 6.6.2), child nodes information or the canonical form of the OID-IRI.

5.1.3 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.

Already covered in the amended Scope, which is the right place for it.

삭제됨: 6.62.21

삭제됨: 6.2.1

삭제됨: NOTE – This Recommendation | International Standard specifies only the overall architecture of the OID Resolution System and general OID resolution process. The application-specific OID resolution process is out of scope of this Recommendation | International Standard.

삭제됨: and

5.2 General OID resolution process

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

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 OID resolution server should include access methods and locations for obtaining additional information. See GB 12.

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 Handling of case sensitivity and of non-ASCII characters See GB 14

Text needs to be added here based on Geneva 2009 discussions. The UK recommends use of punycode, but a proper reference will need to be added in clause 2, and the circumstances in which it is to be used need to be specified.

Text for case sensitivity also needs to be produced out of Geneva discussions related to case sensitivity of Unicode labels and a reference to a case-folding RFCis likely to be needed.

6.3 The form of a query to an OID resolution server See GB 15

An input to an OID resolution 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.

Header	OPCODE=SQUERY
Question	QNAME=99.27.2.oid.foo., QCLASS=IN, QTYPE=NAPTR
Answer	<empty>
Authority	<empty>
Additional	<empty>

Figure 2. DNS message format for query

6.4 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. .foo, here and elsewhere, need to be replaced, but all occurrences should be yellowed for now. JL

6.5 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.

6.6 Response from the OID resolution server See GB 16

6.6.1 General

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

삭제됨:
삭제됨: 1
삭제됨: Q
삭제됨: In the DNS query message,
삭제됨: should be converted
삭제됨: 1.1
삭제됨: A
삭제됨: 1
삭제됨: See that t
삭제됨: 2
삭제됨: .
삭제됨: F
삭제됨: 3
삭제됨: .
삭제됨: F
삭제됨: 4
삭제됨: .
삭제됨: F
삭제됨: 5
삭제됨: F
삭제됨: 1.2
삭제됨: n
삭제됨: 1
삭제됨: See that t
삭제됨: 2
삭제됨: . F
삭제됨: 3
삭제됨: . F
삭제됨: 4
삭제됨: . F
삭제됨: 5
삭제됨: F
삭제됨: 2

Header	OPCODE=SQUERY, RESPONSE, AA
Question	QNAME=99.27.2.oid.foo., QCLASS=IN, QTYPE=NAPTR
Answer	1.27.2.oid. IN NAPTR 100 100 "flag" "service" "regexp" "replacement"
Authority	<empty>
Additional	<empty>

Figure 3. DNS message format for response

6.6.1.2 This Recommendation | International Standard specifies new 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 See GB 17

orpservice = “DNS” | “X.500” | “LDAP” | “HTTP” | “HTTPS” | “COI” | “CINFO” See GB 18

6.6.2 Access information

6.6.2.1 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. This Recommendation | International Standard specifies 5 access methods: DNS, X.500, LDAP, HTTP and HTTPS. An access location is specified as a URI in the RegExp field of NAPTR Resource Record.

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

99.27.2.oid.foo. IN NAPTR 0 100 “u” “O2I+DNS” “!^.*$!examplecode.kr!” .

6.6.2.3 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 DNS protocol at “examplecode.kr”.

6.6.3 Child node information

6.6.3.1 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. See GB 19 The location of this XML file is specified as a URI in the RegExp field of the NAPTR Resource Record.

6.6.3.2 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!” .

6.6.4 Canonical form of an OID-IRI

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

6.6.4.2 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!” .

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

6bis DNS zone file implementation See GB 20

TBD Use of DNAME, CNAME or whatever, in zone files. Specify the requirements to avoid exponential explosions, and to allow later addition of new Unicode labels without changing lower-level zone files. Text is needed. This should detail what is in the high-level zone files maintained by the DNS OID RA, and give a recommendation on the handling of zone files at lower nodes.

삭제됨: 2
삭제됨: 1
삭제됨: e
삭제됨: associate
삭제됨: 2
삭제됨: 2
삭제됨: 2
삭제됨: 3
삭제됨: A

6ter Security issues See GB 21

Outline text should be developed in Geneva for this section as outlined in GB21, and addressed by a Geneva agenda item

7 Operation of the OID Resolution System

7.1 Figure 4 illustrates the hierarchical structure and the delegation structure of OID resolution servers.

삭제됨: describes

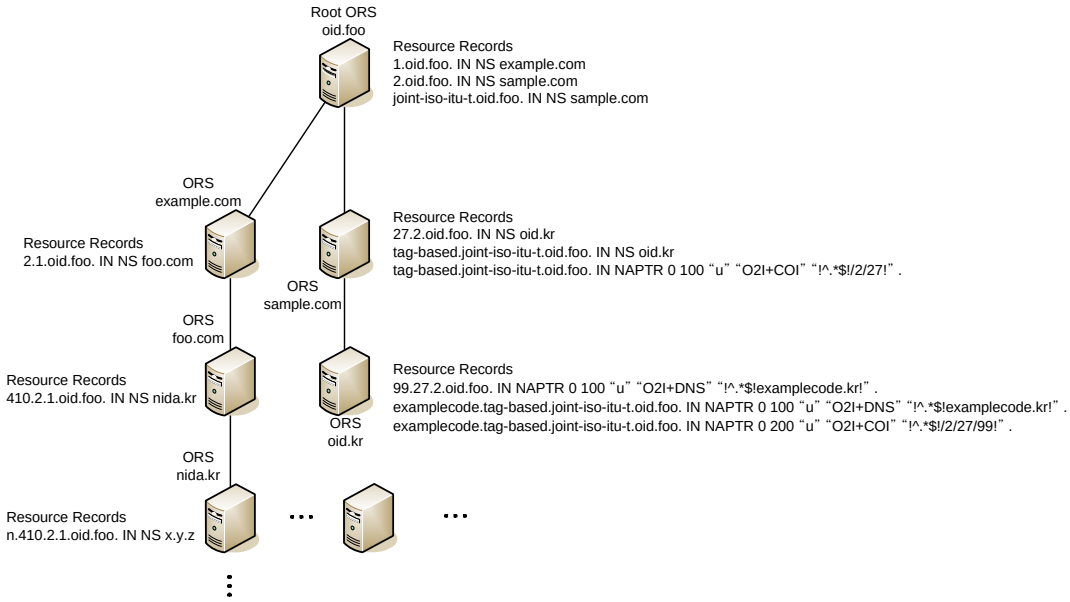

Figure 4. An example of the structure of OID resolution servers

7.2 Figure 5 shows the operation example of general OID resolution process with the configuration as Figure 4.

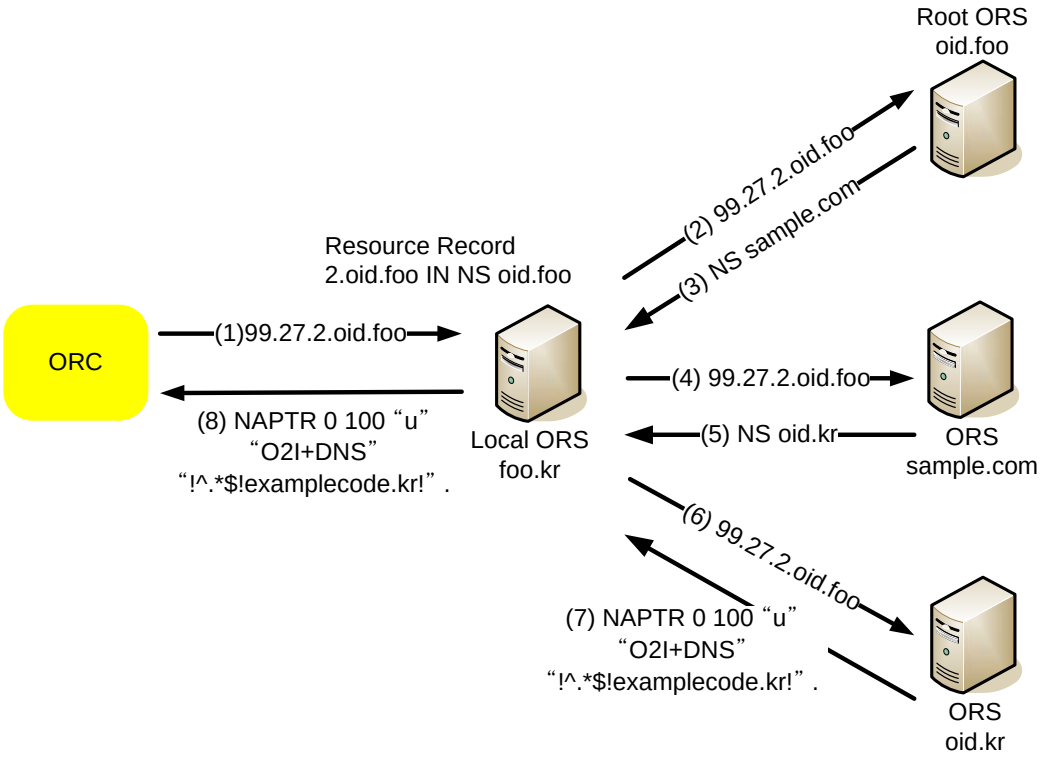

Figure 5. Example operation of general OID resolution process

8 Implementation architecture

8.1 For performance reasons, all zone files for the high-level arcs of the OID tree should ideally be located in a single root server for the OID Resolution System.

8.2 It is expected that the DNS OID RA will normally ensure this.

8.3 Zone files for lower level nodes can also be located on this server, subject to contractual agreements. See GB 24. (See clause 10)

9 Security and Trust Aspects of the OID Resolution System (see GB 25, which proposes moving this into the new 6bis

As the general OID resolution process in the OID Resolution System 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.

10 Operational matters (see GB 26)

10.1 The high level nodes supported by the DNS OID RA

10.1.1 The DNS zone files for the OID root node are supported by the DNS OID RA.

10.1.2 Table x lists, in column 1, all other high-level nodes (in pre-order traversal sequence). In many cases, additional information is available from the OID Repository .

삭제됨: Default setting of zone file for OID Resolution System

삭제됨: the

삭제됨: issues

삭제됨: top

삭제됨: sec

NOTE – Nodes not listed in the table have not been assigned at the time of publication of this Recommendation | International Standard.

10.1.3 Column 2 contains either:

a) "√" (fully supported); or

b) "CS" (conditionally supported) – see 10.1.8; or

c) "NS" (not supported, and not intended to be supported);

Nodes in the "NS" category are largely obsolete, and cannot become part of the DNS-OID-mirror (and hence their children cannot.

10.1.4 In some cases a set of nodes are identified in column 1 as, for example, "1 to 26" for the series of a Recommendation, or "All numbers" for the set of Recommendations in a given series or for International Standards, or "All countries" for the set of possible country codes. In all these cases, the entry is flagged as "CS" (see 10.1.8).

10.1.5 In some cases, there are known children operating RAs in the "All countries" category. These are listed in column 1, and column 4 (see 10.1.7) gives the dates that a letter from the country was first notified to the relevant Study Group or the relevant Sub-Committee, where available.

10.1.6 Column 3 gives in each row the OID-IRIs (starting with the canonical OID-ORI) that are available for each node listed in column 1, including use of long arcs. Column 3 also gives in ASN.1 Object Identifier value names that are deprecated for that node,

NOTE TO THE RAPPORTEUR – Long arcs and Unicode labels have not yet been assigned for some of these table entries. This should be handled by a Resolution in Geneva 2009, and the table updated.

10.1.7 Column 4 of table x gives, for each column 2 entry, either a reference to the X.660 series | ISO/9834 series specifying that OID-ORI, or to the date(s) of the Resolutions by the relevant Study Group and the relevant Sub-Committee that established that OID-IRI. For brevity, a reference to X.66x | 9834-y is shown simply as x | y.

NOTE – In some cases, the date cannot easily be determined, and is indicated as "NK" (not-known). Note from the UK to the Rapporteur: It is hoped that homework in Geneva can reduce the list of NKs to a minimum.

10.1.8 In some cases, a node is not supported by the DNS OID RA unless there is a child node beneath that node which requires DNS support, and has applied to, and been accepted by the DNS OID RA (see 10.2.2) for a reference to zone files for the child node (which may be maintained by the DNS OID RA or by the child, depending on commercial arrangements). Such nodes are listed as "CS" (conditionally supported) in column 2, but no further information is given in the table.

삭제됨:

Table x – High-level nodes of the OID tree, recording support from the DNS OID RA

This table needs more work, but time did not permit its completion. Some of the entries, such as /ITU-T and itu-t are subject to discussion on case-folding and case sensitivity

It is hoped that this can be completed and agreed in Geneva Sep 2009

Canonical form of the OID-IRI	Support	OID-IRI paths to the node	Reference to allocations
/0	√	/0	0 | 1 (A.2.2)
		/ITU-T	0 | 1 (A.2.2)
		/itu-t	0 | 1 (A.2.2)
		/ITU-R	0 | 1 (A.3.8 NOTE)
		/itu-r	0 | 1 (A.3.8 NOTE)
		/ccitt will not be included	
/0/0	√	<all /0>/0	0 | 1 (A.3.2)
		<all /0>/Recommendation	0 | 1 (A.3.2)
		<all /0>/recommendation	0 | 1 (A.3.2)

Canonical form of the OID-IRI	Support	OID-IRI paths to the node	Reference to allocations
/0/0/<1 to 26>	CS	<all /0/0>/<1 to 26>	0 | 1 (A.3.3.1)
/0/0/<1 to 26>/<number>	CS	<all /0/0/<1 to 26>/<number>	0 | 1 (A.3.3.2)
/0/1	NS		
/0/2	√	<all /0>/2 <all /0>/Administration <all /0>/administration	0 | 1 (A.3.2) 0 | 1 (A.3.2) 0 | 1 (A.3.2)
/0/2/<all X.121 numerical country codes>	CS	<all /0/2>/<all X.121 numerical country codes> <all /0/2>/<all X.121 alpha-2 codes>	0 | 1 (A.3.5) 0 | 1 (A.3.5)
/0/3	√	<all /0>/3	0 | 1 (A.3.2)
/0/3/<all X.121 DNICS	CS	<all /0/3>/<all X.121 DNICS>	0 | 1 (A.3.6)
/0/4	√	<all /0>/4 Sub-arcs are TBD	9 | -
/0/5	√	<all /0>/4 Sub-arcs are TBD	TBD
/1 TBD	√	TBD Sub-arcs are TBD	TBD
/2 TBD	√	TBD Sub-arcs are TBD	TBD

10.2 Expanding the DNS-OID-mirror

10.2.1 Restrictions and requirements

10.2.1.1 An OID child cannot become part of the DNS-OID-mirror unless its parent is already part of the DNS-OID-mirror.

10.2.1.2 An OID parent that is part of the DNS-OID-mirror shall not provide a pointer to zone files for a child (implying inclusion of that child node in the DNS-OID-mirror) unless that child explicitly gives permission for the parent to do so.

NOTE – Whether the child's zone files are on a server maintained by the parent, or are on a server maintained by the child are for agreement between the parent and the child, and may be subject to charging arrangements that are not constrained by this Recommendation | International Standard, except for interactions with the DNS OID RA (see 10.2.2).

10.2.1.3 A DNS parent is required by this Recommendation | International Standard to provide DNS look-up information as a simple Boolean value – see x.y) saying that it has (unspecified) OID children that are not part of the DNS-OID-mirror.

10.2.1.4 An OID parent with a DNS mirror shall not add a child to its zone files (even if it supports the child zone files in its own server) without the explicit permission of the OID child.

10.2.1.5 **The detailed arrangements (including charging and giving permission for inclusion in the DNS-OID-mirror) between an OID parent and an OID child for the inclusion of that child in the DNS-OID-mirror (where permitted by 10.2.1.1 and 10.2.1.2) are not standardised.**

10.2.2 Application for inclusion of an OID child node in the DNS-OID-mirror

삭제됨:

10.2.2.1 Any entity with an OID allocation under a parent node which is already part of the DNS-OID-mirror, but is not supported by the DNS OID RA (see table x in 10.1) is entitled to request its parent to include it in the DNS-OID-

mirror. The parent is not required to accept the request, and the mechanisms and charging for doing this are not standardised.

10.2.2.2 Any entity with an OID allocation under a parent node which is part of the DNS-OID-mirror supported or conditionally supported by the DNS OID RA (see table x in 10.1) shall apply to the DNS OID RA for inclusion in the DNS-OID-mirror.

10.2.2.3 The contact point for the DNS OID RA is listed in the OID Repository. The commercial arrangements for adding a child node into the DNS-OID-mirror will in this case depend on the extent of support required from the DNS OID RA, are subject to change, and are published from time to time on the DNS OID RA web-site. They may involve any or all of an initial charge, a charge for changes, and an annual charge for retention of the child. (See also 10.2.3).

10.2.3 Charging issues

10.2.3.1 A parent which is part of the DNS-OID-mirror may choose to include a child in the DNS-OID-mirror.

10.2.3.2 This will always be done by a link from the parent node zone files to the child's zone file.

10.2.3.3 The child's zone files may be on a server provided by the child, or may be on a server administered by the parent.

10.2.3.4 The charges for the link to the child's zone files will depend on the options above, and may be an initial charge, an annual charge for retention, and/or a charge for changes. This is not constrained by this Recommendation | International Standard.

10.2.3.5 Where the inclusion of a child involves the DNS OID RA, the charges and options are published on the DNS OID RA web-site.

NOTE – It is expected that inclusion of a permanent link to a server for zone files of a child supported or conditionally supported by the DNS OID RA will be zero or cost-recovery. Charges for enhanced service involving the maintenance and changing of child zone files on the parents server are expected to be subject to be cost-plus-profit charging.

10.3 Secondaries of the primary DNS zone files managed by the DNS OID RA

TBD Note that the terms primary and secondary DNS zone files may need defining (or referencing from an RFC)

Duties, synchronization and timing and contractual/charging issues with the DNS OID RA need addressing, but may be adequately covered by normal DNS implementation specifications and practice (see also 10.5)

10.4 Appointment of the DNS OID RA and of DNS secondary servers

10.4.1 The DNS OID RA shall be appointed by a plenary decision of the relevant Study Group with a Resolution by the relevant Sub-Committee, followed by an ISO contract. If possible, before publication, add a footnote saying who is appointed, and give contact details (in the OID Repository?).

10.4.2 Appointment of DNS secondary servers shall be subject to the agreement of the DNS OID RA, and a simple plenary decision by the relevant Study Group and a Resolution by the relevant Sub-Committee. Commercial arrangements will be determined between the DNS OID RA and applicants for provision of secondary servers. If possible, before publication, add a footnote on where the secondary servers are.

10.5 Synchronisation of the DNS-OID-mirror with the OID Repository

This will hopefully be done by reference to an RFC, and may not need a separate clause

Bibliography

[1] Rec. ITU-T X.509 | ISO/IEC 9594-8, *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*

[2] RFC 1594, *Answers to Commonly asked "New Internet User" Questions*

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

_____