Network Working Group S. Josefsson

Internet-Draft October 26, 2003

Expires: April 25, 2004

Domain Name System Uniform Resource Identifiers

draft-josefsson-dns-url-09

Status of this Memo

This document is an Internet-Draft and is in full conformance with

all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering

Task Force (IETF), its areas, and its working groups. Note that other

groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months

and may be updated, replaced, or obsoleted by other documents at any

time. It is inappropriate to use Internet-Drafts as reference

material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://

www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at

http://www.ietf.org/shadow.html.

This Internet-Draft will expire on April 25, 2004.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

This document define Uniform Resource Identifiers for Domain Name

System resources.

Josefsson Expires April 25, 2004 [Page 1]

Internet-Draft DNS URI October 2003

Table of Contents

1. Introduction and Background . . . . . . . . . . . . . . . . . 3

2. DNS URI Registration . . . . . . . . . . . . . . . . . . . . . 4

3. Examples . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

4. Security Considerations . . . . . . . . . . . . . . . . . . . 8

5. IANA Considerations . . . . . . . . . . . . . . . . . . . . . 8

Normative References . . . . . . . . . . . . . . . . . . . . . 9

Informative References . . . . . . . . . . . . . . . . . . . . 9

Author's Address . . . . . . . . . . . . . . . . . . . . . . . 10

A. Revision Changes . . . . . . . . . . . . . . . . . . . . . . . 10

A.1 Changes since -06 . . . . . . . . . . . . . . . . . . . . . . 10

A.2 Changes since -07 . . . . . . . . . . . . . . . . . . . . . . 10

A.3 Changes since -08 . . . . . . . . . . . . . . . . . . . . . . 10

Intellectual Property and Copyright Statements . . . . . . . . 12

Josefsson Expires April 25, 2004 [Page 2]

Internet-Draft DNS URI October 2003

1. Introduction and Background

The Domain Name System (DNS) [1][2] is a widely deployed system used

to, among other things, translate host names into IP addresses.

Recent work has added support for storing certificates and

certificate revocation lists in the DNS [10].

The primary motivation behind defining a Uniform Resource Identifier

(URI) for DNS resources, instead of using another non-URI syntax that

embed the domain, type value and class value, is that applications

that stores or retrieve certificates today uses URIs for this

purpose. Thus, defining a URI scheme for DNS resources allows these

existing protocols to be used with certificates in the DNS without

having to add DNS specific modifications to said protocols. In order

to not introduce interoperability or security considerations,

protocols that uses these URIs naturally must have been written to

allow for future, as of writing yet undefined, URIs to be used.

A few examples of protocols that may utilize DNS URIs:

o The OpenPGP Message Format [8], where an end-user may indicate the

location of a copy of any updates to her key, using the "preferred

key server" field.

o The X.509 Online Certificate Status Protocol [11], where the OCSP

responder can indicate where a CRL is found, using the

id-pkix-ocsp-crl extension.

The DNS URI scheme defined here can, of course, be used to reference

any DNS data, and is not limited to only certificates. The purpose

of this specification is to define a generic DNS URI, not a specific

DNS solution for certificates stored in the DNS. Browsers may

implement support for DNS URIs by forming DNS queries and render DNS

responses using HTML [14], similar to what is done for the FTP [5].

The core part of this document is the URI Registration Template

according to [13].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",

"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this

document are to be interpreted as described in RFC 2119 [6].

Josefsson Expires April 25, 2004 [Page 3]

Internet-Draft DNS URI October 2003

2. DNS URI Registration

URL scheme name: "dns".

URL scheme syntax: A DNS URI designates a DNS resource record set

that can be referenced by domain name, type, class and optionally the

authority. The DNS URI follows the generic syntax from RFC 2396 [4],

and is described using ABNF [3]. Strings are not case sensitive and

free insertion of linear-white-space is not permitted.

dnsurl = "dns:" [ "//" dnsauthority "/" ] dnsname ["?" dnsquery]

dnsauthority = hostport

; See RFC 2396 for "hostport" definition.

dnsname = \*pchar

; See RFC 2396 for "pchar" definition.

; NB! Can be empty.

dnsquery = dnsqueryelement [";" dnsquery]

; First matching element MUST be used.

; E.g., dns:host.example.org?TYPE=A;TYPE=TXT

; means type A.

dnsqueryelement = ( "CLASS=" dnsclassval ) / ( "TYPE=" dnstypeval ) /

( 1\*alphanum "=" 1\*alphanum )

dnsclassval = 1\*digit / "IN" / "CH" / ...

; Any IANA registered DNS class expressed as

; mnemonic or as decimal integer.

dnstypeval = 1\*digit / "A" / "NS" / "MD" / ...

; Any IANA registered DNS type expressed as

; mnemonic or as decimal integer.

The digit representation of types and classes MAY be used when a

mnemonic for the corresponding value is not well known (e.g., for

newly introduced types or classes), but SHOULD NOT be used for the

types or classes defined in the DNS specification [2]. All

implementations MUST recognize the mnemonics defined in [2].

Unless specified in the URI, the authority ("dnsauthority") is

assumed to be locally known, "dnsclassval" to be the Internet class

("IN"), and "dnstypeval" to be the Address type ("A").

To resolve a DNS URI using the DNS protocol [2] a query is formed by

using the dnsname, dnsclassval and dnstypeval from the URI string (or

the previously mentioned default values if some value missing from

Josefsson Expires April 25, 2004 [Page 4]

Internet-Draft DNS URI October 2003

the string). If authority ("dnsauthority") is given in the URI

string, this indicate the server that should receive the DNS query,

otherwise the default DNS server should receive it. (Note that DNS

URIs could be resolved by other protocols than the DNS protocol. DNS

URIs does not require the use of the DNS protocol, although it is

expected to be the typical usage. This paragraph only illustrate how

DNS URIs are resolved using the DNS protocol.)

A client MAY want to check that it understands the dnsclassval and

dnstypeval before sending a query, so that it is able to correctly

parse the answer. A typical example of a client that would not need

to check dnsclassval and dnstypeval would be a proxy that just treat

the answer as opaque data.

Character encoding considerations: The characters are encoded as per

the "URI Generic Syntax" RFC [4]. The DNS protocol do not consider

character sets, it simply transports opaque data. In particular, the

"dnsname" field of the DNS URI is to be considered an

internationalized domain name (IDN) unaware domain name slot, in the

terminology of [16]. (The reason for this is that making these fields

be IDN aware by, e.g., specifying that they are UTF-8 [7] strings,

would require further encoding mechanisms to be able to express all

valid DNS domain names. This is because the DNS allows all octet

sequences to be used as domain labels, so UTF-8 strings do not cover

all possibilities. Instead of defining further encoding mechanisms,

we point applications with internationalization needs at the ASCII

encoding described in [16] which should be satisfactory.) The

considerations for "hostport" are discussed in [4]

To encode a "." that is part of a DNS label the "escaped" encoding

MUST be used, and a label delimiter MUST be encoded as ".". That is,

the only way to encode a label delimiter is ".", and the only way to

encode a "." as part of label is "%2e". This approach was chosen to

minimize the modifications users will have to do when manually

translating a domain name string into the URI form.

This URI specification allows all possible domain names to be encoded

(of course following the encoding rules of [4]), however certain

applications may restrict the set of valid characters and care should

be taken so that invalid characters in these contexts does not cause

harm. In particular, host names in the DNS have certain

restrictions. It is up to these application to limit this subset,

this URI scheme places no restrictions.

Intended usage: Whenever DNS resources are useful to reference by

protocol independent identifiers, often when the data is more

important than the access method. Since software in general has

coped without this so far, it is not anticipated to be implemented

Josefsson Expires April 25, 2004 [Page 5]

Internet-Draft DNS URI October 2003

widely, nor migrated to by existing systems, but specific solutions

(especially security related) may find this appropriate.

Applications and/or protocols which use this scheme: Security related

software. It may be of interest to auxilliary DNS related software

too.

Interoperability considerations: The data referenced by this URI

scheme might be transferred by protocols that are not URI aware (such

as the DNS protocol). This is not anticipated to have any serious

interoperability impact though.

Interoperability problems may occur if one entity understands a new

DNS type or class mnemonic but another entity do not understand it.

This is an interoperability problem for DNS software in general,

although it is not a major practical problem as the DNS types and

classes are fairly static. To guarantee interoperability

implementations could use integers for all mnemonics not defined in

[2].

Interaction with Binary Labels [12], or other extended label types,

has not been analyzed. However, they appear to be infrequently used

in practice.

Security considerations: See below.

Contact: simon@josefsson.org

Author/Change Controller: simon@josefsson.org

Josefsson Expires April 25, 2004 [Page 6]

Internet-Draft DNS URI October 2003

3. Examples

A DNS URI is of the following general form. This is intended to

illustrate, not define, the scheme.

dns:[//authority/]domain[?type=TYPE;class=CLASS]

The following illustrate a URI for a resource with the name

"www.example.org", the Internet (IN) class and the Address (A) type:

dns:www.example.org?class=IN;type=A

Since the default class is IN, and the default type is A, the same

resource can be identified by a shorter URI:

dns:www.example.org

The following illustrate a URI for a resource with the name

"simon.example.org", for the CERT type, in the Internet (IN) class:

dns:simon.example.org?type=CERT

The following illustrate a URI for a resource with the name

"ftp.example.org", in the Internet (IN) class and the address (A)

type, but from the DNS authority 192.168.1.1 instead of the default

authority (i.e., when DNS is used, the query is sent to that server):

dns://192.168.1.1/ftp.example.org?type=A

The following illustrate a strange, albeit valid, DNS resource. Note

the encoding of "." and 0x00, and the use of a named dnsauthority:

dns://internal-dns.example.org/\*.%3f%20%00%2e%25+?type=TXT

Josefsson Expires April 25, 2004 [Page 7]

Internet-Draft DNS URI October 2003

4. Security Considerations

If a DNS URI references domains in the Internet DNS environment, both

the URI itself and the information referenced by the URI is public

information. If a DNS URI is used within an "internal" DNS

environment, both the DNS URI and the data is referenced should be

handled using the same considerations that apply to DNS data in the

environment.

If information referenced by DNS URIs are used to make security

decisions (examples of such data include, but is not limited to,

certificates stored in the DNS), implementations may need to employ

security techniques such as Secure DNS [9], or even CMS [15] or

OpenPGP [8], to protect the data during transport. How to implement

this will depend on the usage scenario, and it is not up to this URI

scheme to define how the data referenced by DNS URIs should be

protected.

If applications accept unknown dnsqueryelement values (e.g., accepts

the URI "dns:www.example.org?secret=value" without knowing what the

"secret=value" dnsqueryelement means), a covert channel used to

"leak" information may be enabled. The implications of covert

channels should be understood by applications that accepts unknown

dnsqueryelement values.

This draft does not modify the security considerations related to the

DNS or URIs in general.

5. IANA Considerations

The IANA is asked to register the DNS URI scheme, using the template

in section 2, in accordance with RFC 2717 [13].

Josefsson Expires April 25, 2004 [Page 8]

Internet-Draft DNS URI October 2003

Acknowledgments

Thanks to Stuart Cheshire, Donald Eastlake, Pasi Eronen, Ted Hardie,

Peter Koch, Andrew Main, Larry Masinter, Michael Mealling, Steve

Mattson, and Paul Vixie for comments and suggestions. The author

acknowledges the RSA Laboratories for supporting the work that led to

this document.

Normative References

[1] Mockapetris, P., "Domain names - concepts and facilities", STD

13, RFC 1034, November 1987.

[2] Mockapetris, P., "Domain names - implementation and

specification", STD 13, RFC 1035, November 1987.

[3] Crocker, D. and P. Overell, "Augmented BNF for Syntax

Specifications: ABNF", RFC 2234, November 1997.

[4] Berners-Lee, T., Fielding, R. and L. Masinter, "Uniform Resource

Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

Informative References

[5] Postel, J. and J. Reynolds, "File Transfer Protocol", STD 9,

RFC 959, October 1985.

[6] Bradner, S., "Key words for use in RFCs to Indicate Requirement

Levels", BCP 14, RFC 2119, March 1997.

[7] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC

2279, January 1998.

[8] Callas, J., Donnerhacke, L., Finney, H. and R. Thayer, "OpenPGP

Message Format", RFC 2440, November 1998.

[9] Eastlake, D., "Domain Name System Security Extensions", RFC

2535, March 1999.

[10] Eastlake, D. and O. Gudmundsson, "Storing Certificates in the

Domain Name System (DNS)", RFC 2538, March 1999.

[11] Myers, M., Ankney, R., Malpani, A., Galperin, S. and C. Adams,

"X.509 Internet Public Key Infrastructure Online Certificate

Status Protocol - OCSP", RFC 2560, June 1999.

[12] Crawford, M., "Binary Labels in the Domain Name System", RFC

2673, August 1999.

Josefsson Expires April 25, 2004 [Page 9]

Internet-Draft DNS URI October 2003

[13] Petke, R. and I. King, "Registration Procedures for URL Scheme

Names", BCP 35, RFC 2717, November 1999.

[14] Connolly, D. and L. Masinter, "The 'text/html' Media Type", RFC

2854, June 2000.

[15] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3369,

August 2002.

[16] Faltstrom, P., Hoffman, P. and A. Costello, "Internationalizing

Domain Names in Applications (IDNA)", RFC 3490, March 2003.

Author's Address

Simon Josefsson

EMail: simon@josefsson.org

Appendix A. Revision Changes

Note to RFC editor: This appendix is to be removed on publication.

A.1 Changes since -06

The MIME registration templates for text/dns and application/dns was

removed, and will be defined in separate documents.

Improved discussion related to which mnemonics that must be

supported. The interoperability problem that provoked the

clarification is also mentioned.

Security consideration improvements.

A.2 Changes since -07

Author/Change Controller changed to author of this document, not

IESG. Terminology section collapsed into introduction. The second

paragraph of the introduction rewritten and gives explicit examples.

Intended usage and applications fields fixed. Moved this revision

tracking information to an appendix. Mention IDN in charset section.

All previous thanks to suggestions by Larry Masinter.

A.3 Changes since -08

Modifications derived from Last-Call comments: Made more clear that

DNS URIs does not imply use of the DNS protocol, but the issue is not

stressed because of the apparent inflamatory state of affairs. Added

Josefsson Expires April 25, 2004 [Page 10]

Internet-Draft DNS URI October 2003

informative references to HTML and FTP. Clarified that dnsname can

be empty. Clarified that first dnsqueryelement "win" in case of

ambiguity. Clarified security consideration with respect to unknown

dnsqueryelements. Use "authority" instead of "server". Say "IANA

registered" instead of "standard". Interoperability note about binary

DNS labels. Typos.

Josefsson Expires April 25, 2004 [Page 11]

Internet-Draft DNS URI October 2003

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any

intellectual property or other rights that might be claimed to

pertain to the implementation or use of the technology described in

this document or the extent to which any license under such rights

might or might not be available; neither does it represent that it

has made any effort to identify any such rights. Information on the

IETF's procedures with respect to rights in standards-track and

standards-related documentation can be found in BCP-11. Copies of

claims of rights made available for publication and any assurances of

licenses to be made available, or the result of an attempt made to

obtain a general license or permission for the use of such

proprietary rights by implementors or users of this specification can

be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any

copyrights, patents or patent applications, or other proprietary

rights which may cover technology that may be required to practice

this standard. Please address the information to the IETF Executive

Director.

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to

others, and derivative works that comment on or otherwise explain it

or assist in its implementation may be prepared, copied, published

and distributed, in whole or in part, without restriction of any

kind, provided that the above copyright notice and this paragraph are

included on all such copies and derivative works. However, this

document itself may not be modified in any way, such as by removing

the copyright notice or references to the Internet Society or other

Internet organizations, except as needed for the purpose of

developing Internet standards in which case the procedures for

copyrights defined in the Internet Standards process must be

followed, or as required to translate it into languages other than

English.

The limited permissions granted above are perpetual and will not be

revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an

"AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING

TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING

BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION

Josefsson Expires April 25, 2004 [Page 12]

Internet-Draft DNS URI October 2003

HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF

MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgment

Funding for the RFC Editor function is currently provided by the

Internet Society.

Josefsson Expires April 25, 2004 [Page 13]