Network Working Group
Request for Comments: 4002
Category: Standards Track

R. Brandner
Siemens AG
L. Conroy
Siemens Roke Manor Research
R. Stastny
Oefeg

February 2005

IANA Registration for Enumservice 'web' and 'ft'

Status of This Memo

Copyright Notice

Abstract

This document registers the Enumservices 'web' and 'ft' by using the URI schemes 'http:', 'https:' and 'ftp:' as per the IANA registration process defined in the ENUM specification (RFC 3761).

Table of Contents

1. Introduction

ENUM (E.164 Number Mapping, RFC 3761 [2]) is a system that transforms E.164 numbers [3] into domain names and that then uses DNS (Domain Name Service, RFC 1034 [4]) services such as delegation through NS records and NAPTR records to look up what services are available for a specific domain name.

This document registers 'Enumservices' according to the guidelines given in RFC 3761 [2] to be used for provisioning in the services field of an NAPTR [7] resource record to indicate what class of functionality a given end point offers. The registration is defined within the DDDS (Dynamic Delegation Discovery System [5][6][7][8][9]) hierarchy, for use with the "E2U" DDDS Application, defined in RFC 3761 [2].

The following 'Enumservices' are registered with this document: 'web' and 'ft'. These share a common feature in that they each indicate that the functionality of the given end points and the associated resources are primarily sources of information.

According to RFC 3761 [2], the 'Enumservice' registered must be able to function as a selection mechanism when one chooses between one NAPTR resource record and another. This means that the registration MUST specify what is expected when that NAPTR record is used, and the URI scheme that is the outcome of use.

Therefore an 'Enumservice' acts as a hint, indicating the kind of service with which the URI constructed by using the regexp field is associated. More than one 'Enumservice' can be included within a single NAPTR; this indicates that there is more than one service that can be achieved by using the associated URI scheme.

The common thread with this set of definitions is that they reflect the kind of service that the end user will hope to achieve with the communication by using the associated URI.

The services specified here are NOT intended to specify the protocol or even the method of connection that MUST be used to achieve each service. Instead, we define the kind of interactive behavior that an end user will expect, leaving the end system to decide (based on policies outside the scope of this specification) how to execute the service.

As the same URI scheme may be used for different services (e.g., 'tel:') and the same kind of service may use different URI schemes (e.g., for VoIP, 'sip:', 'h323:', and 'tel:' may be used), it is necessary in some cases to specify the service and the URI scheme used.

The service parameters defined in RFC 3761 [2] therefore allow a 'type' and a 'subtype' to be specified. Within this set of specifications, it is assumed that the 'type' (being the more generic term) defines the service and the 'subtype' defines the URI scheme.

2. Terminology

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 BCP 14, RFC 2119 [1].

3. Web Service

3.1. Introduction

The Enumservices registered in this section indicate that the resource identified by the associated URI is capable of being a source of information.

3.2. Web Service Registration with 'http:'

Enumservice Name: "web"

Enumservice Type: "web"

Enumservice Subtype: "http"

URI Scheme: 'http:'

Functional Specification:

This Enumservice indicates that the resource identified by the associated URI scheme is capable of being a source of information.

Note that the kind of information retrieved can be manifold. Usually, contacting a resource by an 'http:' [11] URI provides a document. This document can contain references that will trigger the download of many different kinds of information, such as audio, video, or executable code. Thus, one cannot be more specific about the kind of information expected when contacting the resource.

Security Considerations:

There are no specific security issues with this 'Enumservice'. However, the general considerations of Section 5 apply.

Intended Usage: COMMON

Authors:

Rudolf Brandner, Lawrence Conroy, Richard Stastny (for author contact detail, see the Authors' Addresses section)

Any other information the author deems interesting:

None

3.3. Web Service Registration with 'https:'

Enumservice Name: "web"

Enumservice Type: "web"

Enumservice Subtype: "https"

URI Scheme: 'https:'

Functional Specification:

This Enumservice indicates that the resource identified by the associated URI scheme is capable of being a source of information, which can be contacted by using TLS or the Secure Socket Layer protocol.

Note that the kind of information retrieved can be manifold. Usually, contacting a resource by an 'https:' URI [12] provides a document. This document can contain many different kinds of information, such as audio, video, or executable code. Thus, one cannot be more specific about what information to expect when contacting the resource.

Security Considerations:

There are no specific security issues with this 'Enumservice'. However, the general considerations of Section 5 apply.

Intended Usage: COMMON

Authors:

Rudolf Brandner, Lawrence Conroy, Richard Stastny (for author contact detail, see the Authors' Addresses section)

Any other information the author deems interesting:

None

4. FT Service Registration

Enumservice Name: "ft"

Enumservice Type: "ft"

Enumservice Subtype: "ftp"

URI Scheme: 'ftp:'

Functional Specification:

This Enumservice indicates that the resource identified by the associated URI scheme is a service usable in the manner specified for ftp: in RFC 1738 [10], for instance, file retrieval.

Security Considerations:

There are no specific security issues with this 'Enumservice'. However, the general considerations of Section 5 apply.

Intended Usage: COMMON

Authors:

Rudolf Brandner, Lawrence Conroy, Richard Stastny (for author contact detail, see the Authors' Addresses section)

Any other information the author deems interesting:

None

5. Security Considerations

As used by ENUM, DNS is a global, distributed database. Thus any information stored there is visible to anyone anonymously. Although this is not qualitatively different from publication in a telephone directory, it does expose the data subject to having "their"

information collected automatically without any indication that this has been done, or by whom.

Data harvesting by third parties is often used to generate lists of targets for unrequested information; in short, it is used to address "spam". Anyone who uses a Web-archived mailing list is aware that the volume of "spam" email they receive increases when they post to the mailing list; publication of a telephone number in ENUM is no different and may be used to send "junk faxes" or "junk SMS", for example.

Many mailing list users have more than one email address and use "sacrificial" email accounts when they post to these lists to help filter out unrequested emails. This is not so easy with published telephone numbers; the PSTN E.164 number assignment process is much more involved, and usually a single E.164 number (or a fixed range of numbers) is associated with each PSTN access. Thus, providing a "sacrificial" phone number in any publication is not possible.

Due to the implications of publishing data on a globally accessible database, as a principle the data subject MUST give explicit informed consent when data is published in ENUM.

In addition, the data subject should be made aware that, due to storage of such data during harvesting by third parties, removal of the data from publication will not remove any copies that have been taken; in effect, any publication may be permanent.

However, regulations in many regions will require that the data subject can at any time request that the data is removed from publication, and that consent for its publication is explicitly confirmed at regular intervals.

The user SHOULD be asked to confirm opening a web page or starting an ftp session (particularly if the ftp client is configured to send the user's email address as an "anonymous" user password).

Using a web:http or ft:ftp service is not secure, so the user should apply the same caution when entering personal data as they would do if using a client application started with any other method. Although this is not a feature of ENUM or these Enumservices, the ENUM-using application on the end system may appear different from the user's "normal" browser, so the user SHOULD receive an indication of whether their communication is secured.

As evaluating a web page can involve execution of embedded (or linked) content that may include executable code, evaluating a web URL involves risks. If automatic evaluation of a web link were to be used, the querying user would be exposed to risks associated with that automatic download and execution of content. Thus, the client MUST ask the querying user for confirmation before evaluating the web URL; the client MUST NOT download and evaluate the web content automatically.

An analysis of threats specific to the dependence of ENUM on the DNS, (threats against which are covered in [14]) and the applicability of DNSSEC [13] to these, is provided in RFC 3761 [2].

6. IANA Considerations

The IANA has registered Enumservice 'web' and 'ft' per the registration process defined in the ENUM specification [2].

7. References

7.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Faltstrom, P. and M. Mealling, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 3761, April 2004.

[3] ITU-T, "The International Public Telecommunication Number Plan", Recommendation E.164 , May 1997.

[4] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[5] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS", RFC 3401, October 2002.

[6] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm", RFC 3402, October 2002.

[7] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", RFC 3403, October 2002.

[8] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI)", RFC 3404, October 2002.

[9] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures", BCP 65, RFC 3405, October 2002.

[10] Berners-Lee, T., Masinter, L., and M. McCahill, "Uniform Resource Locators (URL)", RFC 1738, December 1994.

[11] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[12] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

7.2. Informative References

[13] Arends, R. and et al., "Protocol Modifications for the DNS Security Extensions", Work in Progress.

[14] Atkins, D. and R. Austein, "Threat Analysis of the Domain Name System (DNS)", RFC 3833, August 2004.

Authors' Addresses

Rudolf Brandner
Siemens AG
Hofmannstr. 51
81359 Munich
Germany

Phone: +49-89-722-51003
EMail: rudolf.brandner@siemens.com

Lawrence Conroy
Siemens Roke Manor Research
Roke Manor
Romsey
United Kingdom

Phone: +44-1794-833666
EMail: lwc@roke.co.uk

Richard Stastny
Oefeg
Postbox 147
1103 Vienna
Austria

Phone: +43-664-420-4100
EMail: richard.stastny@oefeg.at

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.