

IETF ENUM Working Group
Internet Draft
Document: draft-ietf-enum-privacy-security-01.txt

Richard Shockey
NeuStar, Inc
John Morris
Center for
Democracy and
Technology
July 2003

Expires: January 2004

Privacy and Security Considerations in ENUM

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026 [1].

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026 except that the right to produce derivative works is not granted.

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/lid-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 January 1, 2004.

Copyright Notice

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

Abstract

Many individuals and groups have expressed concerns about the privacy and security of personal information to be contained in

implementations of ENUM. This document discusses some of the technical as well as security and privacy considerations national implementations of ENUM should consider.

This is a work in progress.

Discussion of this document is welcomed on the IETF ENUM mailing list.

General Discussion:enum@ietf.org
To Subscribe: enum-request@ietf.org
In Body: subscribe
Archive: ftp://ftp.ietf.org/ietf-mail-archive/enum/

Conventions used in this document

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 [RFC2119].

Table of Contents

- 1.0 INTRODUCTION.....3
- 2.0 THE RATIONALE FOR ENUM.....3
- 3.0 VIEWS OF ENUM.....4
 - 3.1 NUMBER TRANSLATION DATABASE.....4
 - 3.2 CALLED PARTY CONTROL OF ENUM ENABLED COMMUNICATIONS.....5
 - 3.3 CALLING PARTY CONTROL OF COMMUNICATIONS.....5
- 4.0 PROCEDURES FOR ENUM REGISTRATION.....6
- 5.0 SECURITY CONSIDERATIONS IN ENUM.....7
 - 5.1 SECURITY IN ENUM PROVISIONING.....7
 - 5.2 SECURITY OF THE DNS.....7
- 6.0 PRIVACY CONSIDERATIONS IN ENUM.....8
 - 6.1 PRIVACY CONCERNS INHERENT IN ENUM'S RELIANCE ON THE DNS...8
 - 6.1.1 CALLED PARTY VERSUS CALLING PARTY CONTROL.....8
 - 6.1.2 SIP AS A TOOL FOR ENABLING PRIVACY.....9
 - 6.1.3 THE USE OF REAL AND OR ALIAS NAMES.....10
 - 6.2 PRIVACY CONCERNS RAISED BY IMPLEMENTATION DECISIONS.....11
 - 6.2.1 PRIVACY OF REGISTRATION INFORMATION.....11
 - 6.2.2 OPT-IN NATURE OF ENUM.....12
 - 6.2.3 CONTROL OVER DATA IN ENUM RECORD.....13
- 7.0 FAIR INFORMATION PRACTICES.....13
- 8.0 REFERENCES.....14
- Acknowledgments.....16
 - Author's Addresses.....16

1.0 INTRODUCTION

Many individuals groups have expressed concerns about the privacy and data security implications of ENUM as it moves forward toward global deployment. For example, see [EPIC], [CLARKE], [CDT]. In that context there are several different views of what ENUM is, what it does, and how a global ENUM system may affect personal privacy and the security of data contained in the global ENUM system.

It is important to note that ENUM is first and foremost a system that works within the DNS. Specifically ENUM is a system that translates phone numbers [ITU-T] into Fully Qualified Domain Names that can be queried to return a specific set of data (URI's) in the form of NAPTR records [RFC 3403]. The global and distributed nature of the DNS means delegation and control can occur at any point within the FQDN. Many entities (service providers, enterprises and indeed some consumers) could control their own DNS servers for ENUM registered domain names.

As noted in [ENUM] and other documents, the utility of the DNS is essentially that it is open and globally accessible to any one on the Internet.

There are two forms of data required for the global ENUM system to work. First is the actual data to be entered into the DNS system -- the NAPTR records to be associated with an appropriate ENUM Fully Qualified Domain Name. Second is the data that will be required to maintain appropriate authentication, valid registration, administrative and technical contact for ENUM records stored in DNS servers. Both forms of data raise privacy and security issues.

The agreements between the IAB and the ITU over the management and control of the e164.arpa namespace [RFC 3026, RFC 3245] for those portions of the E.164 global numbering plan clearly articulates that the administration, management and control of the zones and administrative portions of the E.164 plan are nation-state issues governed by appropriate national laws and regulations, many of which have yet to be determined.

2.0 THE RATIONALE FOR ENUM

Before a discussion of privacy and security issues raised by the global ENUM system, it is valuable to note why the IETF technical community developed ENUM, what applications it was designed to

serve and the implications of those applications for privacy and security issues.

Since telephone numbers are the global naming scheme for Public Switched Telephony, ENUM is designed to map phone numbers with the Internet DNS and its naming and addressing conventions (IP numbers and Domain Names). As such ENUM exists primarily to facilitate the interconnection of systems that rely on telephone numbers with those that use URI's to route transactions. Therefore in and of itself ENUM has no specific application value. It is only the applications themselves that are mapped to phone numbers that users direct interact with.

Many businesses and consumers are very comfortable with using telephone numbers for communications. The ITU developed E.164 numbering plan is a well organized and internationally recognized system that is essential to the proper functioning of the PSTN. Though it is clear that ENUM can and will be used for service routing of a variety applications, the principal focus of attention on ENUM application development has been focused on voice communications based on SIP [RFC 3261], the ITU developed H.323, and the general concept of convergence of the IP and PSTN networks.

ENUM is, consequently, part of the list of technologies developed in the IETF and the ITU that attempt to extend the functionality of IP based communications and reinvent the concept of telephony specifically.

3.0 VIEWS OF ENUM

Even within the technical community there are different views of what ENUM is and what it is designed to accomplish.

3.1 NUMBER TRANSLATION DATABASE

One view sees ENUM in the DNS as essentially a benign number translation database that exposes on the minimal subset of data necessary to establish a connection between two endpoints. This is the model we essentially have in the DNS now. DNS translates the URI concept such as `http://www.foobar.org` to IP number necessary for a client to find a server running HTTP. No other intervention by the DNS is necessary.

This is also the function of the DNS in E-mail where the DNS is used simply to locate an MX record for a SMTP server within a domain. No policy or personal information is exposed in the DNS beyond a host name.

This concept is roughly analogous to the concept of a Service Control Point within the architecture of the PSTN that provide routing data to a circuit switch based on the numeric input of a phone number.

The essential difference between the DNS and PSTN Service Control Points is that the DNS is a highly distributed database globally accessible to any device or network connected to the Internet and Service Control Points are a high specialized and restricted databases available only to uniquely authenticated and authorized PSTN network elements, such as Class 5 switches. Appropriate domain name holders can modify DNS entries while only authorized carriers can only modify data in PSTN Service Control points.

3.2 CALLED PARTY CONTROL OF ENUM ENABLED COMMUNICATIONS

An emerging view of ENUM is that it enables an advanced form of called party control of communications since it is presumed that the communications servers at the edge of network are under the administrative or operational control of called party. User control of those servers permits policy in some form to be directly applied to inbound communications irrespective of the wishes of the calling party.

This view is particularly relevant in the case of SIP based communication [PETERSON 1]. The classic SIP model is based on the use of proxies between end point client/user agents that can then negotiate information about each other in order to establish a session. The calling party has no need to discover the capabilities of the called parties end point since those are established during the signaling portion of a SIP session using the Session Description Protocol.

The called parties proxy can also be used to enforce policy (including privacy policy) about sessions, including how, when and from whom to establish sessions. The presumption of this model is that only the minimum information about location of the endpoint proxy is necessary to expose in the global DNS, since the proxies perform all other forms of session negotiation.

3.3 CALLING PARTY CONTROL OF COMMUNICATIONS

One other view of ENUM wishes to give the calling party the complete control over how they wish to contact someone else. The preference here is for the maximum amount of information exposed in the global DNS to permit the calling party the choice of contact methodology to the called party.

In this scenario all the various endpoints that a called party has under their control could be listed in the DNS with various hints as to their nature and function in the NAPTR enumservice field, such as E2U+sip,E2U+sms:tel, etc. [BRANDNER 1, BRANDNER 2]

The calling party's device or user agent could then parse the various NAPTR records and present the options for communication to the calling party.

```
$ORIGIN 4.3.2.1.6.7.9.8.6.4.e164.arpa.  
IN NAPTR 100 10 "u" "E2U+web:http"      "!^.*$!  
http:www.example.foo!"  
  
IN NAPTR 100 10 "u" "E2U+mms:tel;      " !^.*$!tel:+46987654321!"  
  
IN NAPTR 100 10 "u" "E2U+sip"  
"!^.*$!sip:patrik@barfoo.bar!"  
  
IN NAPTR 100 10 "u" "E2U+ifax:mailto"  
"!^.*$!mailto:patrik@mailco.foo!"
```

The calling party then selects the methodology for communication from that list.

4.0 PROCEDURES FOR ENUM REGISTRATION

Various national ENUM groups have emerged with the task of developing policies and procedures for administrating the ENUM system within their various jurisdictions. [See <http://www.itu.int/osg/spu/enum/index.html#trials>] Many of these forums have described a multi-tier model for ENUM registration and provisioning that will require some forms of personal data to be collected and stored as well as technical contact data on who is the responsible party for the management of the authoritative name servers that hold and manage ENUM records.

Many concepts and principals have been borrowed from domain name registration where there are three distinct parties to the transaction, Registrant, Registrar and Registry.

A Registrant in the global ENUM system is presumed to be the Telephone Number Holder or consumer. An ENUM Registrar is an administrative entity that assists Registrants in populating the global ENUM tree in e164.arpa by providing authentication and authorization functions, in order to preserve and protect both the interests of consumers and the global integrity of the E.164

numbering plan. The ENUM Registry is a national administrative entity that manages that portion of the E.164 namespace appropriate within e164.arpa (such as 6.4.e164.arpa for Sweden or 4.4.e164.arpa for the United Kingdom, or possibly a sub-namespace within a national namespace).

Various jurisdictions have different laws and regulations regarding data acquisition and the protection of data acquired from consumers (registrants). What those policies and procedures should be will ultimately be a national sovereign decision of the nation state managing their portion of the e164.arpa namespace.

5.0 SECURITY CONSIDERATIONS IN ENUM

Privacy is often viewed as an element of security, and thus the privacy considerations discussed below in Sections 6 and 7 are security considerations. This section security concerns in more traditional terms.

5.1 SECURITY IN ENUM PROVISIONING

Since the global ENUM system relies on the DNS and the protocol itself converts E.164 numbers into domain names there has been considerable discussion on how data is to be exchanged between the ENUM registrants, registrars and registries and how that data is protected.

For some time the IETF PROVREG working group has been developing a robust Extensible Provisioning Protocol [EPP] for the domain name industry. This protocol has within it several highly secure mechanisms for the exchange of data between the various Registrants, Registrars and Registries in the ENUM system.

This work could easily be adapted to the needs of ENUM, however there are a variety of highly secure protocols and technologies such as Simple Object Access Protocol (SOAP) that could provide similar capabilities.

5.2 SECURITY OF THE DNS

The security issues surrounding the DNS are well understood [DNSSEC-INTRO]. This has enormous implications for emerging national ENUM administrations. In particular a DNS request can be subject to man-in-the-middle attacks where the response from the DNS may be altered in transit. This has serious implications for the accuracy and authentication of responses from the DNS to ENUM formatted queries by applications.

The IETF has developed DNSSEC [DNSSEC-ROADMAP] to authenticate that the responses from the DNS are indeed from the zone for which they have been requested, however DNSSEC is still in early testing and deployment and has not been deployed in a large scale environment such as generic or country code Top Level Domain.[RFC 3130]

It is the consensus of the IETF ENUM Work group that the use of DNSSEC will become necessary as the protocol matures.

6.0 PRIVACY CONSIDERATIONS IN ENUM

ENUM raises a range of privacy concerns, both in its reliance on the DNS, and in decisions that will be made by each national authority that decides to implement ENUM. This section discusses both groups of concerns. Many of these concerns are raised by privacy principles called "fair information practices" These broad principles are briefly summarized below in Section 7.0.

6.1 PRIVACY CONCERNS INHERENT IN ENUM'S RELIANCE ON THE DNS

Because ENUM utilizes the global DNS to store information about how to contact individuals, and information stored in DNS records are freely accessible by any user on the Internet, ENUM inherently raises questions about user privacy. Although ENUM-like capability could have been designed without using the DNS, the robust and globally deployed nature of the DNS offered a means to develop and deploy ENUM without having to create a separate global information lookup system. Considerations raised by this reliance on the DNS are addressed below.

6.1.1 CALLED PARTY VERSUS CALLING PARTY CONTROL

As a technical matter, there is no reason to conclude that either the Called Party Control or Calling Party Control views of ENUM are right or wrong. There are clearly circumstances where consumers or businesses, for various reasons, might prefer each option.

A variety of businesses and enterprises may wish to expose and individually characterize the maximum number of contact points in the global DNS order, to facilitate communications by calling parties in the most convenient means available.

Consumers, however, will probably prefer that information about them is masked or aliased in the DNS, in order to benefit from

advanced IP communications, while preserving personal preferences and privacy.

What is important is ENUM and the global ENUM system is flexible enough to permit either approach, and the choice of either methodology should be based on the informed consent of the user. No implementation of ENUM should preclude or inhibit the use of either the Called Party Control or the Calling Party Control models.

6.1.2 SIP AS A TOOL FOR ENABLING PRIVACY

As described above in Section 3.2, the Called Party Control model offers ENUM users the ability to exert control over what information is provided through the ENUM system. Critical to this model of ENUM is technology such as the Session Initiation Protocol, SIP, which can be used as a tool to greatly enhance the privacy of information accessed through an ENUM transaction.

Traditional telephony relies on essentially "stupid" endpoints such as traditional telephone instruments and "intelligence" in the network embodied in Class 5 switches at the core of the PSTN. These switches, typically controlled by service providers, provide all of the advanced applications consumers have come to expect.

Services such as Do Not Disturb, Call Forwarding, Call Screening can only be enabled by these switches under the administrative control of service providers. As a globally closed system, call signaling and transport in the PSTN are tightly bound together, the exact opposite of the architectural design of the Internet. [RFC 1958]

SIP as an application technology at the edges of the Internet reverses the PSTN control model. SIP endpoints and proxies are assumed to be "intelligent" and configurable by network administrators.

SIP through the use of advanced Call Processing Language techniques can be quickly and easily programmed to provide Class 5 like features without the intervention of the call transport mechanism.

The Called Party Control model of ENUM, therefore, relies on and will promote the broad deployment of applications such as SIP that give consumers direct control over their communications options, and more generally allow the user to control who accesses personal information about the user.

6.1.3 THE USE OF REAL AND OR ALIAS NAMES

Even with the Called Party Control models some information is necessarily exposed in the global DNS, but important steps can be taken to reduce the disclosure of personal information in the DNS records themselves. In order to establish a session between two endpoints it is necessary to describe that endpoint as a form or URL. However, it not necessary nor is it a requirement to use personally identifying information to establish a successful end-to-end SIP connection. If this information is exposed is only because an end user chooses to do so by configuration of their proxy.

The classic form of NAPTR record for SIP looks much like this.

```
$ORIGIN 4.3.2.1.6.7.9.8.6.4.e164.arpa.
IN NAPTR 100 10 "u" "E2U+sip"
"!^.*$!sip:patrik.faltstrom@example.foo!"
```

One alternative method of achieving the same result without exposing a real name or other form of Personally Identifying Information is to use various forms of aliases. The following are example of a highly constrained, but equally valid, ENUM SIP response. In the first case the identification of the SIP endpoint is configured using an alias convention
"sip:e164number@userdomain.foo"

```
$ORIGIN 4.3.2.1.6.7.9.8.6.4.e164.arpa.
IN NAPTR 100 10 "u" "E2U+sip"    "!^.*$!sip:4689761234@example.foo!"
```

OR

```
$ORIGIN 4.3.2.1.6.7.9.8.6.4.e164.arpa.
IN NAPTR 100 10 "u" "E2U+sip"    "!^.*$!sip:anon5613@example!"
```

Where the user name "anon5616" is randomly selected.

Notice that the ENUM query only returns from the global DNS information that a SIP proxy for the user "4689761234" or "anon5616" exists within the domain example.foo. No personal information is exposed in the global DNS other than the phone number or anonymous alias used to create the FQDN query.

From the perspective of the SIP proxy, if properly configured, there is no functional difference between
sip:patrik.faltstrom@example.foo and sip:4689761234@example.foo
or sip:anon5651@example.foo. All three could accurately describe a unique SIP aware client or user agent.

These examples illustrate a particular view of what is necessary to establish a connection between two parties. That one name can be an alias to something else well understood in Internet engineering terms. For instance it is very easy to give out a e-mail address foobar@domain.us that can be automatically forwarded to a different email address rich.shockey@example.biz.

Current discussion in the IETF ENUM WG have explored the concept of indirect resolution to all forms of communications, not just SIP, through the use of presence servers or a concept called a "service resolution service". [PETERSON 2] Once again the called party who is registering their phone number in the global ENUM system would then have control of how he or she could be contacted by any method, on any device, by means of configuring in that presence or SRS service only that data that they choose to expose to persons wishing to contact them. The calling party in this scenario would first executing a query to DNS to find the presence server or SRS and based on locally controlled policy the server would return the options available.

```
$ORIGIN 0.0.6.2.3.3.5.2.0.2.1.e164.arpa.  
IN NAPTR 100 10 "u" "E2U+pres" "!.^.*$!pres:jon.peterson@foobar.foo!"
```

This represents a more robust and expansive concept of presence where a presence server or SRS would not automatically reveal or display the physical or network presence of an individual or the services under the called parties control but becomes a point of control for how, why when and where presence and a form of communication session might be established.

6.2 PRIVACY CONCERNS RAISED BY IMPLEMENTATION DECISIONS

The above privacy concerns arise because of ENUM's reliance on the DNS system. This section instead discusses concerns that may (or may not) arise in national implementations of ENUM. These considerations are offered to reduce possible privacy-harming impacts that could arise in ENUM implementations.

6.2.1 PRIVACY OF REGISTRATION INFORMATION

Unlike the ICANN administered domain name industry, the global ENUM system has no requirement for a central WHOIS registry of registrants. There is, however, a strong need to be able to locate technical contact information concerning an ENUM record.

Unlike with the domain name system, ENUM URLs could not possibly contain trademarked or other potentially disputed names. More generally, ENUM records do not, in and of themselves, provide ANY "ultimate" service to any Internet users. All that an ENUM record does is to provide pointers to one or more references to other services available over the Internet. If anyone (such as an intellectual property holder, for example) needs to contact the owner of one a service that is referenced in an ENUM record, they can use the URL/URI of the referenced service to locate the relevant party.

For these reasons, there is little reason to require that the identity of the holder of an ENUM record be disclosed in a WHOIS-like system.

In contrast, there is value in linking technical contacts with particular ENUM records. Because the ENUM system depends on the security and stability of DNS servers to function properly, it is prudent and necessary that technical contact data for these servers be widely available to network administrators so that they can be contacted in the event there is a technical problem with aspects of the DNS under their management and control.

A discussion of the various problems with the current WHOIS protocol is beyond the scope of this document. The IETF CRISP working group [<http://www.ietf.org/html.charters/crisp-charter.html>] is developing requirements [CRISP-REQ] for a next generation WHOIS like protocol that may offer a more appropriate solution to the ENUM environment.

6.2.2 OPT-IN NATURE OF ENUM

With both the Called Party Control model of ENUM, and especially with the Calling Party Control model, some degree of personal contact information is exposed in the global DNS. It is important that information regarding end telephone users NOT be imported on a blanket or wholesale basis into the ENUM/DNS system. Users should have a choice of whether to have any information about them listed in the publicly-available DNS.

Such an approach will, for example, reasonably preserve the ability of end users to maintain an "unlisted" telephone number, even using VoIP technology. Assuming users are given a choice about enrolling in the ENUM system, a user could forego the benefits of ENUM in favor of directly providing (for example) a SIP address of record to trusted family members and associates.

6.2.3 CONTROL OVER DATA IN ENUM RECORD

Because as noted some degree of personal contact information is exposed in the global DNS, it is important that the ENUM registrants be provided effective and efficient control over that information. It is also important that ENUM registrants fully understand the privacy implications of placing information in the global DNS.

The flip side of effective user control over ENUM records is that only authorized users should be able to control the content of ENUM records. This issue is briefly discussed as a security consideration above.

7.0 FAIR INFORMATION PRACTICES

As guiding principles, consumer privacy protection in many parts of the world is based on "fair information practices," which were authoritatively detailed in [OECD] by the Organization for Economic Co-operation and Development. The principles should be considered in any implementation of ENUM. Fair information practices include the following principles:

- * Notice and Consent - before the collection of data, the data subject should be provided: notice of what information is being collected and for what purpose and an opportunity to choose whether to accept the data collection and use. In Europe, data collection cannot proceed unless data subject has unambiguously given his consent (with exceptions).

- * Collection Limitation - data should be collected for specified, explicit and legitimate purposes. The data collected should be adequate, relevant and not excessive in relation to the purposes for which they are collected.

- * Use/Disclosure Limitation - data should be used only for the purpose for which it was collected and should not be used or disclosed in any way incompatible with those purposes.

- * Retention Limitation - data should be kept in a form that permits identification of the data subject no longer than is necessary for the purposes for which the data were collected.

- * Accuracy - the party collecting and storing data is obligated to ensure its accuracy and, where necessary, keep it up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete are corrected or deleted.

* Access - a data subject should have access to data about himself, in order to verify its accuracy and to determine how it is being used.

* Security - those holding data about others must take steps to protect its confidentiality.

8.0 REFERENCES

1. [RFC2916bis] Faltstrom, P.& Mealling, M. "The E.164 to URI DDDS Applications", draft-ietf-enum-rfc2916bis-06.txt, (work in progress), May 2003
2. [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997
3. [ITU-T], "The International Public Telecommunication Number Plan", Recommendation E.164, May 1997.
4. [RFC3026] Blaine, R. "Liaison to IETF/ISOC on ENUM" RFC 3026, January 2001
5. [RFC 3403] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Four: The URI Resolution Application", RFC 3403 October 2002.
6. [PETERSON1] Peterson, J. et al, "Using ENUM for SIP Applications", draft-ietf-sipping-el64.02.txt, (work in progress), October 2002
7. [BRANDNER 1] Brandner, R. et.al." Registration for enumservices of group messages", draft-ietf-enum-msg-00.txt, (work in progress) June 2003
8. [BRANDNER 2] Brandner, R. et.al." Registration for enumservices web and ft", draft-ietf-enum-webft-00.txt, (work in progress) June 2003
9. [DNSSEC-INTRO] Arends, R., "DNS Security Introduction and Requirements", draft-ietf-dnsext-dnssec-intro-05.txt, (work in progress) February 2003

10. [RFC 3130] Lewis, E. "Notes from the State-Of-The-Technology: DNSSEC" RFC 3130, June 2001
11. [RFC 1958] Carpenter, B. Editor "Architectural Principals of the Internet", RFC 1958 June 1996
12. [RFC 3245] Klensin, J. Editor "The History and Context of Telephone Number Mapping (ENUM) Operational Decisions: Informational Documents Contributed to ITU-T Study Group 2 (SG2)", RFC 3245, March 2002
13. [PETERSON2] Peterson, J "Enumservice Registration for Presence Services", draft-peterson-enum-pres-00.txt, (work-in-progress) February 2003
14. [RFC 3130] Lewis, E. "Notes from the State-Of-The-Technology: DNSSEC" RFC 3130, June 2001
15. [PROVREG] Hollenbeck, S. "Extensible Provisioning Protocol", draft-ietf-provreg-epp-09.txt, (work in progress) September 2003
16. [CRISP-REQ] Newton, A. "Cross Registry Internet Service Protocol (CRISP) Requirements", draft-ietf-crisp-requirements-05.txt, (work in progress) May 2003
17. [DNSSEC-ROADMAP] Rose, S. "DNS Security Document Roadmap", draft-ietf-dnsext-dnssec-roadmap-07.txt (work in progress) Feb 2003
18. [CLARKE] Clarke, R. "ENUM - A Case Study in Social Irresponsibility," March 2003,
<http://www.anu.edu.au/people/Roger.Clarke/DV/enumISOC02.html>
19. [EPIC] Electronic Privacy Information Center, "EPIC Comments on Privacy Issues in ENUM Forum 11-01-02 Unified Document," November 2002,
<http://www.epic.org/privacy/enum/enumcomments11.02.html>
20. [CDT] Center for Democracy & Technology, "ENUM: Mapping Telephone Numbers onto the Internet - Potential Benefits with Public Policy Risks," April 2003,
<http://www.cdt.org/standards/enum/030428analysis.pdf>

Acknowledgments

The original suggestion for this document came from Allison Mankin and Scott Bradner.

Author's Addresses

Richard Shockey
NeuStar, Inc
46000 Center Oak Plaza
Sterling, VA 20166 USA
Phone: +1 571 434 5651
Email: richard.shockey@neustar.biz

John B. Morris, Jr.
Director, Internet Standards, Technology & Privacy Project
Center for Democracy and Technology
1634 I Street NW, Suite 1100
Washington, DC 20006 USA
Email: jmorris@cdt.org
<http://www.cdt.org>

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 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.