

Network Working Group  
Internet Draft  
Intended status: Standards Track  
Expires: November 24, 2009

S. Moonesamy  
May 25, 2009

SMTP Recipient Address Verification Using the Dynamic  
Delegation Discovery Service (DDDS)  
draft-moonesamy-smtp-vrfy-ddds-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

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 November 24, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the

---

IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

#### Abstract

This memo proposes a mechanism based on the Dynamic Delegation Discovery Service (DDDS) which can be used for the verification of SMTP recipient addresses.

## 1. Introduction

SMTP servers for a domain identified through higher numbered MX records are sometimes specifically targetted for mail delivery as they do not enforce the same policies for the domain. This can generate backscatter where the message is accepted by a SMTP server and bounced because the SMTP recipient address was rejected by a SMTP server further down in the delivery path, generally identified by a lower numbered MX record, to a mailbox that did not elect to receive the non-delivery notification message.

SMTP provides a VRFY command [[RFC5321](#)] to verify a user name. This command is generally disabled in SMTP server implementations for security reasons. Some SMTP clients get around that by doing a partial mail transaction without proceeding to the third step (DATA command). This document proposes a mechanism based on the Dynamic Delegation Discovery Service (DDDS) [[RFC3401](#)][[RFC3402](#)][[RFC3403](#)][[RFC3404](#)] where the local-part of a [RFC 5321](#) [[RFC5321](#)] address is associated with a Naming Authority Pointer (NAPTR) DNS Record Resource [[RFC3403](#)]. This mechanism can be used for the verification of SMTP recipient addresses.

Subaddressing is the practice of augmenting the local-part of an [RFC 5321](#) address with some "detail" information in order to give some extra meaning to that address. One common way of encoding "detail" information into the local-part is to add a "separator character sequence", such as "+", to form a boundary between the "user" (original local-part) and "detail" sub-parts of the address, much like the "@" character forms the boundary between the local-part and domain. The NAPTR Record Resource was chosen as it is a Record Resource (RR) that includes a a regular expression. That can be used to support subaddressing.

### 1.1. Comments

Comments and discussions about this draft can be directed to the

SMTP mailing list, ietf-smtp, maintained at imc.org.  
[RFC Editor: Please remove this subsection]

## 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 [[RFC2119](#)].

## 3. VRFY Application

The VRFY Application uses the NAPTR RR to map the local-part

S. Moonesamy

Expires November 2009

[Page 3]

---

Internet Draft

SMTP verification using DDDS

May 2009

of a [RFC 5321](#) address to a regular expression. SMTP servers can use the regular expression to verify local-part and "detail" of a [RFC 5321](#) address.

The maximum total length of a user name or other local-part, as defined in [RFC 5321](#), is 64 octets. It is important to note that domain labels are limited to 63 characters in length and the total length of the resulting string must be 255 octets or less [[RFC1035](#)]. For the purposes of this specification, the local-part of a [RFC 5321](#) address for the VRFY Application MUST be not be more than the limit defined for a domain label in [[RFC1035](#)].

### 3.1. Application Usage String

The application unique string is a [RFC 5321](#) address limited to 63 characters.

### 3.2. First Well Known Rule

The first known key is the local-part of the [RFC 5321](#) address. For example, postmaster@example.com would have "postmaster" as its first key.

### 3.3 Expected Output

The output of the First Well Known Rule for the VRFY Application is a regular expression. The "regexp" field is defined in [[RFC3402](#)] as consisting of a "delim-character", a POSIX Extended Regular



```
"!(user)$!!" . ; regexp replacement
)
```

The result of the extraction of the local-part of the [RFC 5321](#) address, user@example.com, is "user". The "separator character sequence" and "detail" are removed from the extracted string if subaddressing is used. The "user" (original local part) becomes the Application Usage String. The NAPTR RR to lookup is "user.\_vrfy.\_smtp.\_tcp.example.com.". The record returned is in the form:

```
user._vrfy._smtp._tcp.example.com. IN NAPTR
;; order pref flags service regexp replacement
   10    1    "u" "SMTP+VRFY" "!(user)$!!" .
```

The regular expression in the record is "!(user)\$!!". The "!" character is used to delimit the parts of the substitution expression. The replacement field is empty. There is a match when the regular expression is applied to the local-part and "detail" of the [RFC 5321](#) address being verified.

## [5.](#) Security Considerations

The SMTP VRFY command [[RFC5321](#)] is generally disabled in SMTP servers due to security considerations. It is recommended to use transaction level authentication such as Secret Key

Transaction Authentication for DNS (TSIG) [[RFC2845](#)] or access control mechanisms to restrict access to the DDDS database. Domain Name System Security Extensions (DNSSEC) [[RFC4033](#)] can be used to add data origin authentication and data integrity.

The amount of DNS queries generated by implementations can be substantial. Without the appropriate DNS infrastructure, that can cause a denial of service.

Regular expressions should be checked for sanity, not blindly passed.

## [6.](#) Internationalization Considerations

Non-ASCII characters in domain names are encoded using the

Internationalizing Domain Names in Applications specification  
[RFC3490].

## 7. IANA Considerations

The IANA maintains an Application Service Tag Registry for the S-NAPTR DDDS application defined in [RFC3958]. The IANA is advised that although the application defined in this document is not a S-NAPTR DDDS application, it defines a "SMTP+VRFY" value for the "services" field. That value should not be used in the Application Service Tag Registry for other applications.

## 8. Acknowledgements

The idea of using DNS for recipient address verification originated from David Skoll during a discussion about SMTP in May 2007.

## 9. References

### 9.1. Normative References

- [RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), November 1987.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC3402] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm", [RFC 3402](#), October 2002.
- [RFC3403] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", [RFC 3403](#), October 2002.

S. Moonesamy                      Expires November 2009                      [Page 6]

---

Internet Draft                      SMTP verification using DDDS                      May 2009

- [RFC3404] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI) Resolution Application", [RFC 3404](#), October 2002.
- [RFC5321] Klensin, J., "Simple Mail Transfer Protocol", [RFC 5321](#), October 2008.

### 9.2. Informative References

- [RFC2845] Vixie, P., Gudmundsson, O., Eastlake, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", [RFC 2845](#), May 2000.
- [RFC3401] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part One: The Algorithm", [RFC 3401](#), October 2002.
- [RFC3490] Faltstrom, P., Hoffman, P., and A. Costello, "Internationalizing Domain Names in Applications (IDNA)", [RFC 3490](#), March 2003.
- [RFC3958] Daigle, L. and A. Newton, "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)", [RFC 3958](#), January 2005.
- [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", [RFC 4033](#), March 2005.

Author's Address

S. Moonesamy  
76, Ylang Ylang Avenue  
Quatre Bornes  
Mauritius

Email: [sm+iETF@elandsys.com](mailto:sm+iETF@elandsys.com)