Network Working Group
draft-irtf-asrg-cri-00.txt
Expires: <03-2004>

Eric Dean
Crystal Ball Inc.
Yakov Shafranovich
SolidMatrix Technologies, Inc.

Challenge / Response Interworking (CRI) Framework for Challenge / Response Email Systems

A working document of the Anti Spam Research Group (ASRG) of the Internet Research Task Force (IRTF)

Status of this Memo

Abstract

SMTP was designed simply to deliver email messages without authenticating sources or senders of email messages. In an effort to reduce spam on the Internet, Challenge/Response

("C/R") email systems were developed to provide a method for validating message origination for an intended recipient. This document defines a Challenge / Response Interworking ("CRI") protocol by proposing the use of SMTP extensions and MIME headers for interoperability of C/R systems. This document also defines a set of guidelines for continued use with existing non-CRI mail systems and clients.

Table of Contents

1. INTRODUCTION.

Challenge response systems attempt to authenticate senders and determine if each sender originated a message to an intended recipient. This document defines MIME headers and a SMTP extension for an interworking of challenge response systems while providing loose guidelines for user intervention.

There are various opportunities for a CRI protocol to possibly operate: via MIME headers, via DSNs as defined in [RFC-3464], via SMTP/ESMTP, and via the Message Tracking Protocol defined by the MSTRK WG. This note will address and define various approaches to CRI via these methods.

NOTE: This document is intended to evolve, based on comments from the Anti-Spam Research Group (ASRG) mailing list. It is certain that the current draft is incomplete and entirely possible that it is inaccurate. Hence, comments are eagerly sought, preferably in the form of suggested text changes, and preferably on the ASRG mailing list, at <asrg@ietf.org>.

NOTE: This protocol is experimental and is not suitable for wide spread deployment or production use.

1.1. Purpose.

This document proposes specific CRI methods intended to achieve the following objectives:

- Interoperability between CRI capable systems methods using MIME and SMTP while remaining transparent and non-conflicting to non-CRI capable systems.

- A messaging protocol method using defined headers for automatically handling challenge messages and responses

- Loop avoidance methods that prevent CRI systems from challenging challenge messages

- Exception handling for mailing lists or other systems so that lists do not receive challenge messages

- Guidelines for supporting software systems incompatible with CRI so that email is not disrupted and therefore CRI can be realistically deployed

NOTE: CRI is not an authentication method for email delivery nor security protocol.

1.2. CRI and Consent.

In [CHARTER] the spam problem is approached as one of consent:

"The definition of spam messages is not clear and is not consistent across different individuals or organizations. Therefore, we generalize the problem into "consent-based communication". This means that an individual or organization should be able to express consent or lack of consent for certain communication and have the architecture support those desires."

[CONSENT] further expands on this idea to define a full model for consent communications. Within the consent model (section 2.5, #2) a need is expressed for having "protocols for sharing CONSENT TOKENS". The CRI protocol is one such protocol which allows CRI systems to exchange CONSENT TOKENS. It is possible that the CRI protocol when further developed will become part of a full-fledged consent token exchange protocol. Therefore the CRI protocol should be treated as an experimental protocol not suitable for production use.

1.3. Definitions.

MTA - Mail Transfer Agent, usually an SMTP server
MUA - Mai User Agent, usually a client-side email program

2. CHALLENGE / RESPONSE INTERNETWORKING MODEL.

The challenge response model is based upon the following method:

a) The original sender sends a message to a recipient's MTA via SMTP.
b) Either the recipient's MTA or MUA produces a challenge message.
c) The resultant challenge message is sent to the original sender via SMTP.
d) If the sender's MTA supports CRI, then it may automatically respond to the challenge message. Otherwise, the challenge message will be forwarded to the original senderÆs MUA.
e) If the original sender's MUA supports CRI methods, then it may automatically respond to the challenge message.
f) In the event that neither the MTA or MUA that the sender is using support CRI, the challenge message should contain clear and legible instructions to the original sender instructing how to appropriately respond to the challenge request manually.
g) If the recipient's C/R system receives a response from the sender or his MTA/MUA, then the sender is considered valid

and the message is delivered. If no response is received within a pre-defined period of time, then the original message is disposed of in a implementation specific way.

2.1. CRI Model Illustration.

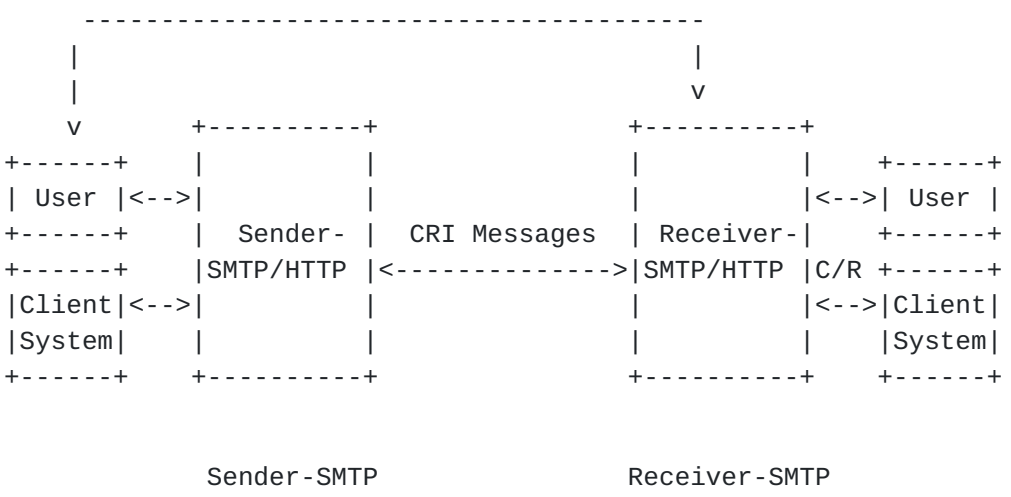

Figure 1. CRI Model.

2.2. Levels of C/R.

There are three basic levels of C/R systems, each one building upon the prior:

1. Sender verification - Attempt to verify whether the original sender's address is valid.
2. Message verification - Attempts to verify whether the original sender actually sent the original message.
3. Turing test - Attempts to verify whether the original sender is human or a machine.

Level 1 addresses an inherent loophole within SMTP that allows delivery of messages with invalid sender addresses. This level seeks to verify whether the sender's email address is valid. HOWEVER, there are several disadvantages with this approach outlines in [EMAIL-PATH]:

- o A spammer can use a valid email address that belongs to someone else
- o A spammer can use a valid domain name and set it to answer "yes" to all verification requests (but a valid domain name makes it easier to track down the spammers)
- o Can be abused by spammer to gather list of valid email addresses

Level 2 addresses some of these issues. With C/R systems, the intent is that sender will only respond to a C/R message

if they in fact sent that specific message. HOWEVER, there are several disadvantages to this approach outlined in [EMAIL-PATH]:

- Message can not be rejected at SMTP level so entire message HAS to be received and challenged, requiring more storage space
- Roaming users are unable to send email directly because they use their own disconnected mail server and message tracking information is not sent to centralized system for the domain
- This requires mail servers to have unified index of all messages that came through any of them

Level 3 ensures that the sender is actually a human being and not an automated spam system. This is done by a pseudo-Turing test usually involves having the sender respond to a puzzle that cannot be processed by a computer. However, since each of these kind of challenges must be responded to by a human being, no automatic system can be provided for responding to such challenges, unless the sender's system is trusted by the recipient to possess accurate information about the sender.

NOTE: Care must be taken designing pseudo-Turing tests so they support use by disabled individuals. For example, displaying a picture as a Turing test will shut out any blind individual.

3. DIFFERENT METHODS FOR CRI.

There are various methods available for CRI: RFC 822/2822 headers, Delivery Status Notification (DNS) messages, MIME headers, SMTP extension, and Message Tracking Protocol defined by the MSTRK WG. Here we will explain the advantages and disadvantages of different approaches.

- Using RFC 822/2822 headers would be the simplest approach. However, headers have a length limit and extending CRI to include digital signatures and certificates would be problematic. Therefore, RFC 822/2822 headers are not used except in conjunction with MIME.

- In [EMAIL-PATH] it is proposed to extend the message tracking protocol defined by the MSGTRK WG for the use of email path verification. However, since that protocol is not currently being used, this approach it not looked at. It is possible that future draft of the CRI proposal may include this approach.

- In [RFC-3464] a MIME format is defined for Delivery

Status Notifications (DSNs) that are intended to notify the sender of a message of any of several conditions: failed delivery, delayed delivery, successful delivery, or the gatewaying of a message into an environment that may not support DSNs. In our case, C/R falls under delayed delivery. However, one major issue that has been raised with using DSNs, is that they are intended for one-way notification and do no anticipate a response unlike C/R systems. Also, current systems often handle DSNs in a specific way and using CRI inside DSNs might break those assumptions. Therefore we are not considering the use of DSNs for CRI.

The remaining two methods are the ones that are defined in this document for CRI use. They are MIME headers and an SMTP extension. The reason for defining the SMTP extension is in order to reduce the storage space required for email by allowing CRI exchange to occur at SMTP level. However, the main method for CRI is defined in MIME headers, with the ESMTP method for use in systems that want to reduce storage space.

3.1. Using MIME for CRI.

This section discusses which MIME type and MIME headers will be used for CRI.

3.1.1. Using "multipart/report" MIME Type.

[RFC-3462] defines a MIME type called multipart/report to be used for reporting of mail system administrative messages and as a general "family" or "container" type for electronic mail reports of any kind. This MIME type defines three parts for every multipart/report message as follows:

1. First part provides a human readable message which is intended for humans only. In the CRI model, this would possibly contain the original message along with the instructions to the user for non-CRI compatible systems. This instruction should include a brief explanation of C/R and a hyperlink or an instruction for an acknowledgement or reply.

2. Second part provides a message to be used for CRI compatible machines with additional details for human beings. In the CRI model, this would contain the CRI MIME headers plus any additional information such as digital certificates, signatures, hashcash codes, etc.

3. Third part contains either the entire original message or portions of it such as headers.

There are several issues when using the multipart/report MIME type. First, not all email systems and clients handle this type. Second, it is intended for one way communications such as delivery failure notifications by the receiver's SMTP server and not necessarily intended for CRI. Third, if two C/R systems are communicating in regards to multiple users and messages, more than one machine readable part might be needed.

3.1.2. Defining a New "multipart/cri" MIME Type.

Another alternative would be defining a custom MIME type called such as "multipart/cri" patterned after the "multipart/report" MIME type which would provide the same three parts. It should be defined as follows:

MIME type name: multipart
MIME subtype name: cri
Required parameters: boundary
Optional parameters: none
Encoding considerations: 7bit should always be adequate
Security considerations: see section 5 of this memo

This MIME type would contain the following:

1. (required) A single human readable body with C/R instructions.
2. (required) Multiple machine-readable bodies (MIME type of message/cri).
3. (optional) Multiple optional bodies containing the original messages (either message/rfc822 or text/rfc822)

Multiple bodies are defined to allow C/R systems to communicate multiple challenges and responses in a single message.

The following MIME type, message/cri, will be defined for carrying CRI information:

MIME type name: message
MIME subtype name: cri
Optional parameters: none
Encoding considerations: 7bit should always be adequate
Security considerations: see section 5 of this memo

NOTE: Since CRI may become part of a larger consent protocol, it may use the MIME type defined for such protocol. In that case, this section will be deprecated.

3.2. MIME Headers for CRI.

This section will define various MIME headers that are used for CRI. We need to pass the following information:

- Sender's email address
- Receiver's email address
- Type of C/R message: challenge, response or informational
- C/R level desired: 1-sender, 2-message, or 3-turing test
- Challenge and response tokens
- Identification of the C/R systems
- How much time does the sender have to respond to the challenge
- If responded, how long the address will stay in the white list until challenged again
- Extensions

There are three different situations where headers are used:

- By the sender with the main message headers to indicate CRI parameters that can be used by the C/R system for the challenge. The CRI MIME is not used.
- By the C/R system in the challenge message with the CRI MIME type
- By the sender in the response message with the CRI MIME type

NOTE: Different token types may reference additional information that will be included in the body of the "message/cri" section.

Additional extension headers maybe defined by using the "X-" headers as per [RFC-2822].

3.2.1. Headers in the Initial Message.

CRI MIME Type is not used, the following required headers are passed:

- CRI-Message-Type: normally maybe either "challenge", "response" or "informational", here MUST BE set to "informational".
- CRI-Sender-Accept-Token: - lists types of token types the sender will accept

The following optional headers are passed:

- CRI-Sender-Agent: identifies the sender's C/R system
- CRI-Sender-Exempt: identifies that the sender desires to not receive a CRI message. i.e. mailing list

3.2.2. Headers in the Challenge Message.

The CRI MIME type IS used. There are two types of headers. Global headers are included as RFC 822/2822 headers with the main message headers. Sender specific headers are included

inside the "message/cri" message body.

The following headers are defined global for the entire C/R message and are required:

- o CRI-Reply-Until: how much time is given for response reply
- o CRI-Recipient-Accept-Token: lists types of tokens the recipient will accept

The following global headers are optional:

- o CRI-Recipient-Agent: identifies the receiver's C/R system
- o CRI-Whitelist-Until: until when will the sender will stay on the whitelist for

The following headers are specific per each sender and are required for each "message/cri" body:

- o CRI-Sender: the original sender of the original message, usually the RFC 822/2822 sender
- o CRI-Recipient: the original receiver of the message, usually the RFC 822/2822 receiver
- o CRI-Verification-Level: at the least must be "1" - sender, maybe also "2" - message, and "3" - human
- o CRI-Message-Type: maybe either "challenge", "response" or "informational", here set to either "challenge" or "informational".
- o CRI-Recipient-Accept-Type: lists types of tokens the recipient will accept
- o CRI-Token-Type: consists of token-type, same for ESMTP and MIME, see IANA section below
- o CRI-Token: - consists of the actual CRI token

3.2.3. Headers in the Response Message.

The CRI MIME type is used. The following optional global headers are passed as part of the main message headers:

- o CRI-Sender-Agent: identifies the sender's C/R system

The following headers are specific per each sender and are\ required for each "message/cri" body:

- o CRI-Sender: the original sender of the original message, usually the RFC 822/2822 sender
- o CRI-Recipient: the original receiver of the message, usually the RFC 822/2822 receiver
- o CRI-Verification-Level: at the least must be "1" - sender, maybe also "2" - message, and "3" - human
- o CRI-Message-Type: maybe either "challenge", "response" or "informational", here set to either "response" or "informational".
- o CRI-Token-Type: consists of token-type, same for ESMTP and MIME, see IANA section below
- o CRI-Token: - consists of the actual CRI token

3.3. CRI ESMTP EXTENSION.

SMTP Extensions are defined in [RFC-1869] and [RFC-2821]. The following service extension is hereby defined:

1) The name of the CRI ESMTP extension is "CRI".
2) The EHLO keyword value associated with this extension is "CRI".
3) Several optional parameters are allows with this EHLO keyword value. The first parameter is the verification level supported and is defined as follows:

   cri-level = SENDER / MESSAGE / HUMAN SP

   If no verification level is specified, then SENDER level is assumed. This is followed by a list of CRI extensions supported by the receiver's system separated by spaces as follows:

   cri-ext = EXT SP EXT SP EXT SP .... EXT = [ALPHA]

   If extensions are specified, then the level must be specified as well. Examples of extensions are digital signatures, hashcash, etc. An IANA registry will be established for registering CRI extensions. The CRI extension list is limited in line length in accordance with existing guidelines.
4) There are not additional verbs associated with this extension
5) New parameters are defined for the RCPT-TO and VRFY commands:

   CRI-TOKEN-TYPE=type; REQUIRED CRI-TOKEN=token; OPTIONAL
   For the DATA command: CRI-TOKEN-TYPE=type; OPTIONAL

   The CRI Token Type defines the token type, and the CRI token parameter carries the actual token. An IANA registry will be established for registering CRI extensions. Each token type will define whether it is carried in the CRI-TOKEN field or in the message body.

   One token is defined:
        Token Type: plain
        Token field used: YES
6) The following behavior changes are being made:

a. For the RCPT TO command, a 452 error code is defined which indicates that a challenge is being issued.
b. For the VRFY command, a requirement is added that it is issued after the MAIL FROM command when used in CRI.
c. For the VRFY command, after challenge is issued and successfully accepted, the QUIT command is used to end the

SMTP session.

d. For the VRFY command, the DATA command is used for transfer of very large tokens inside the message body.

3.4. Examples of CRI.

This section has some examples of how CRI would be used. They are for illustration purposes only.

3.4.1. MIME Example.

Sample CRI message from sender to the recipient with
both systems supporting CRI:

```
....
From: research@solidmatrix.com
To: asrg@irtf.org
Subject: test message
CRI-Message-Type: informational
CRI-Sender-Accept-Token: plain
CRI-Sender-Agent: CRI Tester 0.1
......
```

Sample CRI challenge message:

```
.....
From: challenger@irtf.org
To: research@solidmatrix.com
Subject: Challenge message
CRI-Reply-Until: Mon, 22 Sep 2003 15:16:26 -0400
CRI-Recipient-Accept-Token: plain
CRI-Recipient-Agent: CRI Tester 0.1
CRI-Whitelist-Until: Mon, 22 Sep 2003 15:16:26 -0400
Content-Type: multipart/cri; boundary="opopo54545/irtf.org"

--opopo54545/irtf.org

This is a challenge message. To verify, please go here:

www.irtf.org/asrg/verify/

--opopo54545/irtf.org
Content-Type: message/cri
CRI-Sender: research@solidmatrix.com
CRI-Recipient: asrg@irtf.org
CRI-Verification-Level: 1
CRI-Message-Type: challenge
CRI-Recipient-Accept-Type: plain
CRI-Token-Type: plain
CRI-Token: this is a challenge token

--opopo54545/irtf.org
```

....

Sample CRI response message:
.....
From: research@solidmatrix.com
To: challenger@irtf.org
Subject: Re: Challenge message
CRI-Sender-Agent: CRI Tester 0.1
Content-Type: multipart/cri; boundary="opopo54545/solidmatrix.com"

--opopo54545/irtf.org

This is a response message. The C/R token is: this is a challenge token

--opopo54545/solidmatrix.com
Content-Type: message/cri
CRI-Sender: research@solidmatrix.com
CRI-Recipient: asrg@irtf.org
CRI-Verification-Level: 1
CRI-Message-Type: response
CRI-Token-Type: plain
CRI-Token: this is a challenge token

--opopo54545/solidmatrix.com
.....

3.4.2. CRI ESMTP Examples.

Sample CRI ESMTP conversation from sender to the recipient with
both systems supporting CRI:
S: <wait for connection on TCP port 25>
C: <open connection to server>
S: 220 mail.ietf.org -- Welcome
C: EHLO solidmatrix.com
S: 250-mail.ietf.org
S: 250-HELP
S: 250 CRI SENDER PKI HASHCASH
C: MAIL FROM:<research@solidmatrix.com>
S: 250 OK.
C: RCPT TO:<asrg@irtf.org>
S: 250 asrg@irtf.org OK
C: RCPT TO: <someone@irtf.org>
S: 452 Unverified sender, issuing challenge, retry with CRI
token
.....
.....recipient connects to sender's MTA and issues challenge
.....
S: RCPT TO: <someone@irtf.org> CRI-TOKEN-TYPE=plain;
CRI-TOKEN=token;

```
C: 250 Sender approved for <someone@irtf.org>
C: DATA
S: 354 Send message, ending in CRLF.CRLF.
 ...
C: .
S: 250 OK
C: QUIT
S: 221 Goodbye

Recipient's MTA issuing a challenge with both systems supporting
CRI:
S: <wait for connection on TCP port 25>
C: <open connection to server>
S: 220 mail.solidmatrix.com -- Welcome
C: EHLO mail.irtf.org
S: 250-mail.solidmatrix.com
S: 250-HELP
S: 250 CRI SENDER PKI HASHCASH
C: MAIL FROM:<someone@irtf.org>
S: 250 OK.
C: VRFY:<research@solidmatrix.com> CRI-TOKEN-TYPE=plain;
CRI-TOKEN: token;
S: 250 CRI challenge accepted for <research@solidmatrix.com> OK
C: VRFY:<someone@solidmatrix.com> CRI-TOKEN-TYPE=plain;
CRI-TOKEN: token;
S: 550 Mailbox not found
C: QUIT
S: 221 Goodbye

Recipient's MTA issuing a challenge with both systems supporting
CRI and token carried in message body:
S: <wait for connection on TCP port 25>
C: <open connection to server>
S: 220 mail.solidmatrix.com -- Welcome
C: EHLO mail.irtf.org
S: 250-mail.solidmatrix.com
S: 250-HELP
S: 250 CRI SENDER PKI HASHCASH
C: MAIL FROM:<someone@irtf.org>
S: 250 OK.
C: VRFY:<research@solidmatrix.com> CRI-TOKEN-TYPE=big;
S: 250 CRI challenge accepted for <research@solidmatrix.com> OK
C: DATA CRI-TOKEN-TYPE=big;
S: Send data followed by  .÷
C: ... data ...
S: 250 Challenge token accepted for <research@solidmatrix.com>
C: QUIT
S: 221 Goodbye

Recipient's MTA issuing a challenge with sender's system not
supporting CRI:
```

```
S: <wait for connection on TCP port 25>
C: <open connection to server>
S: 220 mail.solidmatrix.com -- Welcome
C: EHLO mail.irtf.org
S: 250-mail.solidmatrix.com
S: 250-HELP
C: MAIL FROM:<someone@irtf.org>
S: 250 OK.
C: RCPT TO: <research@solidmatrix.com>
S: 250 OK
C: DATA
S: 354 Send mail data followed by CRLF
C: ...sends email challenge message ...
S: 250 Message accepted for delivery
C: QUIT
S: 221 Goodbye
```

4. Interoperability Considerations.

4.1. Loop Avoidance.

CRI systems should not issue challenge messages when C/R headers are present. CRI systems should not challenge messages with CRI-Message-Type: response or challenge. In order to maintain compatibility with non-CRI systems, it is recommended that each CRI system maintain stateful monitoring of challenge messages sent to original senders. For CRI systems that issue challenge messages, it is also recommended that each CRI system use a local systemwide user, such as cri@foo.com, for issuing challenges rather than preserving the original sender's email address as the sender of the challenge message. Doing so, allows for loop avoidance to be handled using double-bounce methods where appropriate. For client-based CRI software, loop avoidance may be handled using additional stateful means of tracking outgoing mail.

4.2. Mailing Lists.

Mailing lists may include CRI-Sender-Exempt headers to indicate that challenge messages should not be posted to the mailing list. Most mailing lists supply various headers to indicate that the messages has been sent from a mailing list. Such mailing list detection methods should result in suppressed challenge messages.

5. SECURITY CONSIDERATIONS.

CRI is not an authentication method for email delivery or security protocol. However, since certain methods of CRI may allow for address harvesting, care must be taken when CRI is

used.

6. PRIVACY CONSIDERATIONS.

Since C/R systems keep track of the senders email addresses, this raises privacy issues. In systems that use C/R level 2, copies of messages may be stored as well. Use of cryptography and checksums is encouraged.

7. IANA CONSIDERATIONS.

One IANA registry will be established for registering CRI token types. All additions to this registry require IESG approval. The following token type is defined in this note in the registry:

- Token Type: plain
- ESMTP Field use: Yes
- Description: plain text token
- Syntax: plain text [ALPHA]
- Additional Information: this is a plain text token which needs to be returned as is in the response message

The following application should be used when applying for a new CRI token type (send to <iana@iana.org>):

- Proposed token type name
- Whether the token is passed via the ESMTP CRI extension
- Token syntax
- Token description
- Any additional information that is needed to process this token by a C/R system

A second IANA registry will be define for registering ESMTP CRI extensions. All additions will require IESG approval. The following application should be used when applying for a new CRI ESMTP extension (send to <iana@iana.org>):

- Proposed extension name
- Information as to how this extension works
- Whether and how this extension changes the CRI protocol

8. ADDITIONAL INFORMATION.

8.1. References.

8.1.1. Normative References.

[RFC-821] Postel, J.; "Simple Mail Transfer Protocol"; STD 10, RFC 821; ISI/USC; August 1982

[RFC-822] Crocker, D.; "Standard For The Format Of ARPA Internet Text Messages"; STD 11, RFC 822; University of Delaware; August, 1982

[RFC-1049] Sirbu, M.; "Content-Type Header Field for Internet Messages"; STD 11, RFC 1049; CMU; March 1988.

[RFC-1869] Klensin, J., Freed, N., Rose, M., Stefferud, E. and Crocker, D.; "SMTP Service Extensions"; RFC 1869; MCI, Innosoft, Dover Beach Consulting, Network Management Associates, Brandenburg Consulting; November 1995

[RFC-2045] Borenstein, N., and Freed, N.; "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies"; RFC 1341; Innosoft, First Virtual; Nov 1996.

[RFC-2821] Klensin, J.; "Simple Mail Transfer Protocol"; RFC 2821; AT&T Laboratories; April, 2001.

[RFC-2822] Resnick, P.; "Internet Message Format"; RFC 2822; QUALCOMM Incorporated; April 2001.

8.1.2. Informative References.

[CHARTER] "Anti-Spam Research Group (ASRG) Charter", [http://www.irtf.org/charters/asrg.html], March 2003

[CONSENT] Shafranovich, Y,; "Consent Framework for Fighting Spam", SolidMatrix Technologies, Inc.; Version 0.0.2, July, 2003
[http://www.solidmatrix.com/research/asrg/asrg-consent-framework.html]

[EMAIL-PATH] Leibzon, W.; "Email Path Verification", March 2003
[http://www.elan.net/~william/asrg-emailpathverification-presentation.pdf]

[IPR] Shafranovich, Y.; "Intellectual Property Rights in Anti-Spam Technologies", SolidMatrix Technologies, Inc.; July 2003
[http://www.solidmatrix.com/research/asrg/asrg-ipr.html]

[RFC-3462] Vaudreuil, G; "The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages"; Lucent Technologies; January 2003

[RFC-3464] Moore, K. and Vaudreuil, G; "An Extensible Message Format for Delivery Status Notifications"; University of Tennessee, Lucent Technologies; January 2003

8.2. Acknowledgements.

A lot of information in this note has been based on the

discussions on the Anti-Spam Research Group (ASRG) mailing list. The authors would like to acknowledge the contributions of all members of the group.

8.3. IPR Information.

A list of IPR disclosures and related information may be found in [IPR]. The following IPR information is relevant to this document:

- In June of 2003 MailBlocks, Inc. disclosed to the ASRG that they may be in possession of IPR applicable to C/R systems. These constitute US Patents # 6,199,102 and # 6,112,227. MailBlocks, Inc. has stated that a licensing declaration will be provided later on.
- In June of 2003, TitanKey, Inc. disclosed to the ASRG that they may be in possession of IPR applicable to the CRI SMTP extension. These constitute multiple US and international patent applications. TitanKey, Inc. has stated that a licensing declaration will be provided later on.

8.4. Author(s) Addresses.

Eric Dean
Crystal Ball Inc.
eric@crystalballinc.com

Yakov Shafranovich
SolidMatrix Technologies, Inc.
research@solidmatrix.com
www.shaftek.org

8.5. Full Copyright Statement.

8.6. Document History.

v0.0.3 / YS / 07-23-2003 / Some editing and cleanup
v0.0.4 / YS / 09-22-2003 / Re-did the document, re-formatted, removed DSN section, expanded on IANA, security and privacy sections, added more references, added a section on consent, expanded the levels section, added a section on different approaches, section on MIME is expanded and required/optional parameters are added, renumbered sections, added IPR notices for MailBlocks and TitanKey