           A Simple Mode of Facsimile Using Internet Mail

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Abstract

   This specification provides for "simple mode" carriage of facsimile
   data using Internet mail. Extensions to this document will follow.
   The current specification employs standard protocols and file formats
   such as TCP/IP, Internet mail protocols, Multipurpose Internet Mail
   Extensions (MIME), and Tagged Image File Format (TIFF) for Facsimile.
   It can send images not only to other Internet-aware facsimile devices
   but also to Internet-native systems, such as PCs with common email
   readers which can handle MIME mail and TIFF for Facsimile data. The
   specification facilitates communication among existing facsimile
   devices, Internet mail agents, and the gateways which connect them.

   This document is a revision of RFC 2305. There have been no
   technical changes.

1. Introduction

   This specification defines message-based facsimile communication over
   the Internet. It describes a minimum set of capabilities, taking
   into account those of typical facsimile devices and PCs that can
   generate facsimile data.

A G3Fax device has substantial restrictions due to specifications in
the standards, such as for timers. This specification defines a
profile for Internet mail, rather than creating a distinct "facsimile
over the Internet" service. The semantics resulting from the profile
are designed to be compatible with facsimile operation over the
general switched telephone network, so that gateways between
facsimile and Internet mail can operate with very high fidelity.

The reason for developing this capability as an email profile is to
permit interworking amongst facsimile and email users. For example,
it is intended that existing email users be able to send normal
messages to lists of users, including facsimile-based recipients, and
that other email recipients shall be able to reply to the original
and continue to include facsimile recipients. Similarly, it is
intended that existing email software work without modification and
not be required to process new, or different data structures, beyond
what is normal for Internet mail users. Existing email service
standards are used, rather than replicating mechanisms which are more
tailored to existing facsimile standards, to ensure this
compatibility with existing email service.

1.1. Services

A facsimile-capable device that uses T.4 [15] and the general
switched telephone network (GSTN) is called a "G3Fax device" in this
specification. An "IFax device" is an Internet-accessible device
capable of sending, receiving or forwarding Internet faxes. A
message can be sent to an IFax device using an Internet mail
address. A message can be sent to a G3Fax device using an Internet
mail address; the message MAY be forwarded via an IFax offramp
gateway.

1.2. Cases

This specification provides for communication between each of the
following combinations:

Internet mail   => Network printer
Internet mail   => Offramp gateway (forward to
                             G3Fax)
Network scanner   => Network printer
Network scanner   => Offramp gateway (forward to
                             G3Fax)
Network scanner   => Internet mail

1.3. Key Words

   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 [13].

2. Communication Protocols

   The set of conventions necessary to achieve facsimile-compatible
   service covers basic data transport, document data formats, message
   (document) addressing, delivery confirmation, and message security.
   In this section, the first 4 are covered. The remainder are covered
   in following sections, along with additional details for addressing
   and formats.

2.1. Transport

   This section describes mechanisms involved in the transport between
   IFAX devices.

2.1.1. Relay

   Data transfer MAY be achieved using standard Internet mail transfer
   mechanisms [1, 3]. The format of addresses MUST conform to the RFC
   821 <addr-spec> and RFC 822 <mailbox> Internet mail standards [1, 2,
   3].

2.1.2. Gateway

   A gateway translates between dissimilar environments. For IFax, a
   gateway connects between Internet mail and the T.4/GSTN facsimile.
   Gateways can service multiple T.4/GSTN facsimile users or can service
   only one. In the former case, they serve as a classic "mail transfer
   agent" (MTA) and in the latter as a classic "mail user agent" (UA).
   An onramp is a gateway which connects from T.4/GSTN facsimile to
   Internet mail. An offramp is a gateway which connects from Internet
   mail to T.4/GSTN facsimile. Behavior of onramps is out of scope for
   this specification.

This specification describes the Internet mail service portion of
offramp addressing, confirmation and failure notification. Details
are provided in later sections.

2.1.3. Mailbox protocols

An offramp gateway that operate as an MTA serving multiple users
SHOULD use SMTP; a gateway that operates as a UA serving a single
mail recipient MAY use a mailbox access protocol such as POP [6] or
similar mailbox access protocols.

NOTE: An offramp gateway that relays mail based on addressing
information needs to ensure that it uses addresses supplied in the
MTA envelope, rather than from elsewhere, such as addresses listed in
the message content headers.

2.2. Formats

2.2.1. Headers

IFax devices MUST be compliant with RFC 2822 and RFC 1123, which
define the format of mail headers. The header of an IFax message
SHOULD include Message-ID and MUST include all fields required by [2,
3], such as DATE and FROM.

2.2.2. MIME

IFax devices MUST be compliant with MIME [4], except as noted in
Appendix A.

2.2.3. Content

The data format of the facsimile image is based on the minimum set of
TIFF for Facsimile [5], also known as the S profile.   Such facsimile
data are included in a MIME object by use of the image/TIFF sub-type
[12]. Additional rules for the use of TIFF for Facsimile, for the
message-based Internet facsimile application, are defined later.

2.2.4. Multipart

A single multi-page document SHOULD be sent as a single multi- page
TIFF file, even though recipients MUST process multipart/mixed
containing multiple TIFF files. If multipart content is present and
processing of any part fails, then processing for the entire message
is treated as failing, per [Processing failure] below.

2.3. Error Handling

2.3.1. Delivery failure

   This section describes existing requirements for Internet mail,
   rather than indicating special requirements for IFax devices.

   In the event of relay failure, the sending relay MUST generate a
   failure message, which SHOULD be in the format of a DSN [9].

   NOTE: Internet mail transported via SMTP MUST contain a MAIL FROM
           address appropriate for delivery of return notices. (See
           section 5.2.6.)

2.3.2. Processing Failure

   IFax devices with limited capabilities might be unable to process the
   content of a message. If this occurs it is important to ensure that
   the message is not lost without any notice. Notice MAY be provided
   in any appropriate fashion, and the exact handling is a local matter.
   (See Appendix A, second bullet.)

3. Addressing

3.1. Classic Email Destinations

   Messages being sent to normal Internet mail recipients will use
   standard Internet mail addresses, without additional constraints.

3.2. G3Fax Devices

   G3Fax devices are accessed via an IFAX offramp gateway, which
   performs any authorized telephone dial-up.

3.3. Address Formats Used by Offramps

   When a G3Fax device is identified by a telephone number, the entire
   address used for the G3fax device, including the number and offramp
   host reference MUST be contained within standard Internet mail
   transport fields, such as RCPT TO and MAIL FROM [1, 3]. The address
   MAY be contained within message content fields, such as <authentic>
   and <destination> [2, 3], as appropriate.

   As for all Internet mail addresses, the left-hand-side (local-part)
   of an address is not to be interpreted except by the MTA that is
   named on the right-hand-side (domain).

   The telephone number format SHOULD conform to [7, 8]. Other formats
   MUST be syntactically distinct from [7, 8].

4. Image File Format

   Sending IFax devices MUST be able to write minimum set TIFF files,
   per the rules for creating minimum set TIFF files defined in TIFF for
   Facsimile (the S profile) [5], which is also compatible with the
   specification for the minimum subset of TIFF-F in [14]. Receiving
   IFax devices MUST be able to read minimum set TIFF files.

   A sender SHOULD NOT use TIFF fields and values beyond the minimum
   subset of TIFF for Facsimile unless the sender has prior knowledge of
   other TIFF fields or values supported by the recipient. The
   mechanism for determining capabilities of recipients is beyond the
   scope of this document.

5. Security Considerations

5.1. General Directive

   This specification is based on use of existing Internet mail. To
   maintain interoperability with Internet mail, any security to be
   provided should be part of the of the Internet security
   infrastructure, rather than a new mechanism or some other mechanism
   outside of the Internet infrastructure.

5.2. Threats and Problems

   Both Internet mail and G3Fax standards and operational services have
   their own set of threats and countermeasures. This section attends
   only to the set of additional threats which ensue from integrating
   the two services. This section reviews relevant concerns about
   Internet mail for IFax environments, as well as considering the
   potential problems which can result of integrating the existing G3Fax
   service with Internet mail.

5.2.1. Spoofed Sender

   The actual sender of the message might not be the same as that
   specified in the Sender or From fields of the message content headers
   or the MAIL FROM address from the SMTP envelope.

   In a tightly constrained environment, sufficient physical and
   software controls may be able to ensure prevention of this problem.
   The usual solution is through encryption-based authentication, either
   for the channel or associated with the object, as discussed below.

It should be recognized that SMTP implementations do not provide
inherent authentication of the senders of messages, nor are sites
under obligation to provide such authentication. End-to-end
approaches such as S/MIME and PGP/MIME are currently being developed
within the IETF. These technologies can provide such authentication.

5.2.2. Resources Consumed by Dialout

In addition to the resources normally consumed for email (CPU cycles
and disk), offramp facsimile causes an outdial which often imposes
significant resource consumption, such as financial cost. Techniques
for establishing authorization of the sender are essential to those
offramp facsimile services that need to manage such consumption.

Due to the consumption of these resources by dialout, unsolicited
bulk email which causes an outdial is undesirable.

Offramp gateways SHOULD provide the ability to authorize senders in
some manner to prevent unauthorized use of the offramp. There are no
standard techniques for authorization using Internet protocols.

Typical solutions use simple authentication of the originator to
establish and verify their identity and then check the identity
against a private authorization table.

Originator authentication entails the use of weak or strong
mechanisms, such as cleartext keywords or encryption-based
data-signing, respectively, to determine and validate the identify
of the sender and assess permissions accordingly.

Other control mechanisms which are common include source filtering
and originator authentication. Source filtering entails offramp
gateway verification of the host or network originating the message
and permitting or prohibiting relaying accordingly.

5.2.3. GSTN Authorization Information

Confidential information about the sender necessary to dial a G3Fax
recipient, such as sender's calling card authorization number, might
be disclosed to the G3Fax recipient (on the cover page), such as
through parameters encoded in the G3Fax recipients address in the To:
or CC: fields.

Senders SHOULD be provided with a method of preventing such
disclosure. As with mechanisms for handling unsolicited faxes, there
are not yet standard mechanisms for protecting such information.

   Out-of-band communication of authorization information or use of
   encrypted data in special fields are the available non-standard
   techniques.

   Typically authorization needs to be associated to specific senders
   and specific messages, in order to prevent a "replay" attack which
   causes and earlier authorization to enable a later dial-out by a
   different (and unauthorized) sender. A non-malicious example of such
   a replay would be to have an email recipient reply to all original
   recipients -- including an offramp IFax recipient -- and have the
   original sender's authorization cause the reply to be sent.

5.2.4. Sender Accountability

   In many countries, there is a legal requirement that the "sender" be
   disclosed on a facsimile message. Email From addresses are trivial
   to fake, so that using only the MAIL FROM [1, 3] or From [2, 3]
   header is not sufficient.

   Offramps SHOULD ensure that the recipient is provided contact
   information about the offramp, in the event of problems.

   The G3Fax recipient SHOULD be provided with sufficient information
   which permits tracing the originator of the IFax message. Such
   information might include the contents of the MAIL FROM, From, Sender
   and Reply-To headers, as well as Message-Id and Received headers.

5.2.5. Message Disclosure

   Users of G3Fax devices have an expectation of a level of message
   privacy which is higher than the level provided by Internet mail
   without security enhancements.

   This expectation of privacy by G3Fax users SHOULD be preserved as
   much as possible.

   Sufficient physical and software control may be acceptable in
   constrained environments. The usual mechanism for ensuring data
   confidentially entail encryption, as discussed below.

5.2.6. Non Private Mailboxes

   With email, bounces (delivery failures) are typically returned to the
   sender and not to a publicly-accessible email account or printer.
   With facsimile, bounces do not typically occur. However, with IFax,
   a bounce could be sent elsewhere (see section [Delivery Failure]),
   such as a local system administrator's account, publicly-accessible
   account, or an IFax printer (see also [Traffic Analysis]).

5.2.7. Traffic Analysis

   Eavesdropping of senders and recipients is easier on the Internet
   than GSTN. Note that message object encryption does not prevent
   traffic analysis, but channel security can help to frustrate attempts
   at traffic analysis.

5.3. Security Techniques

   There are two basic approaches to encryption-based security which
   support authentication and privacy:

5.3.1. Channel Security

   As with all email, an IFax message can be viewed as it traverses
   internal networks or the Internet itself.

   Virtual Private Networks (VPN), encrypted tunnels, or transport layer
   security can be used to prevent eavesdropping of a message as it
   traverses such networks. It also provides some protection against
   traffic analysis, as described above.

   At the current time various protocols exist for performing the above
   functions, and are only mentioned here for information. Such
   protocols are IPSec [17] and TLS [18].

5.3.2. Object Security

   As with all email, an IFax message can be viewed while it resides on,
   or while it is relayed through, an intermediate Mail Transfer Agent.

   Message encryption can be used to provide end-to-end encryption.

   At the current time two protocols are commonly used for message
   encryption and are only mentioned here for information. The two
   protocols are PGP-MIME [16] and S/MIME [19].

6. References

6.1. Normative References

   [1] Klensin, J., Editor, "Simple Mail Transfer Protocol", RFC 2821,
        April 2001.

   [2] Resnick, P., Editor, "Internet Message Format", RFC 2822, April
        2001.

   [3] Braden, R., "Requirements for Internet hosts - application and
        support", STD 3, RFC 1123, October 1989.

   [4] Borenstein, N. and N. Freed, "Multipurpose Internet Mail
        Extensions (MIME) Part Five: Conformance Criteria and Examples",
        RFC 2049, November 1996.

   [5] Buckley, R., Venable, D., McIntyre, L., Parsons, G., and J.
        Rafferty, "File Format for Internet Fax", RFC 3949, November
        2004.

   [6] Myers, J. and M. Rose, "Post Office Protocol - Version 3", STD
        53, RFC 1939, May 1996.

   [7] Allocchio, C., "Minimal GSTN address format for Internet mail",
        RFC 3191, October 2001.

   [8] Allocchio, C., "Minimal fax address format for Internet mail",
        RFC 3192, October 2001.

   [9] Moore, K., and G. Vaudreuil, "An Extensible Message Format for
        Delivery Status Notifications", RFC 3464, January 2003.

   [10] Freed, N. and N. Borenstein, "Multipurpose Internet Mail
        Extensions (MIME) Part Two: Media Types", RFC 2046, November
        1996.

   [11] Moore, K. "MIME (Multipurpose Internet Mail Extensions) Part
        Three: Message Header Extensions for Non-ASCII Text", RFC 2047,
        November 1996.

   [12] Parsons, G. and J. Rafferty, "Tag Image File Format (TIFF) -
        image/tiff MIME Sub-type Registration", RFC 3302, September
        2002.

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

6.2. Informative References

   [14] Parsons, G. and J. Rafferty, "Tag Image File Format (TIFF) -- F
        Profile for Facsimile", RFC 2306, March 1998.

   [15] ITU-T (CCITT), "Standardization of Group 3 facsimile apparatus
        for document transmission", ITU-T (CCITT), Recommendation T.4.

   [16] Callas, J., Donnerhacke, L., Finney, H., and R. Thayer, "OpenPGP
        Message Format", RFC 2440, November 1998.

   [17] Kent, S. and R. Atkinson, "Security Architecture for the
        Internet Protocol", RFC 2401, November 1998.

   [18] Hoffman, P., "SMTP Service Extension for Secure SMTP over
        Transport Layer Security", RFC 3207, February 2002.

   [19] Ramsdell, B., "S/MIME Version 3 Message Specification", RFC
        2633, June 1999.

7. Acknowledgements

   This specification was produced by the Internet Engineering Task
   Force Fax Working Group, over the course of more than one year's
   online and face-to-face discussions. As with all IETF efforts, many
   people contributed to the final product.

   Active for this document were: Steve Huston, Jeffrey Perry, Greg
   Vaudreuil, Richard Shockey, Charles Wu, Graham Klyne, Robert A.
   Rosenberg, Larry Masinter, Dave Crocker, Herman Silbiger, James
   Rafferty.

Appendix A: Exceptions to MIME

    * IFax senders are not required to be able to send text/plain
      messages (RFC 2049 requirement 4), although IFax recipients are
      required to accept such messages, and to process them.

    * IFax recipients are not required to offer to put results in a file.
      (Also see 2.3.2.)

    * IFax recipients MAY directly print/fax the received message rather
      than "display" it, as indicated in RFC 2049.

Appendix B: List of edits to RFC 2305

```
+----+----------+------------------------------------------------+
| No.| Section  |              Edit  July 27, 2001               |
+----+----------+------------------------------------------------+
| 1. |Copyright | Updated copyright from "1998" to "1999,2000"    |
|    |Notice    |                                                |
+----+----------+------------------------------------------------+
| 2. |SUMMARY   | Changed the phrase "over the Internet" to      |
|    |          |                   "using Internet mail"        |
+----+----------+------------------------------------------------+
| 3. |5         | Changed the paragraphs regarding to the        |
|    |          | following references to make them very         |
|    |          | non-normative.                                 |
|    |          |  "OpenPGP Message Format", RFC 2440            |
|    |          |  "Security Architecture for the IP", RFC 2401  |
|    |          |  "SMTP Service Extensions for Secure SMTP over |
|    |          |   TLS", RFC 2487                               |
|    |          |  "S/MIME Version 2 Message Specification",     |
|    |          |   RFC 2311                                     |
+----+----------+------------------------------------------------+
| 4. |REFERENCES| Removed the following references because they   |
|    |          | are non-normative                              |
|    |          |  "SMTP Service Extensions for Delivery Status  |
|    |          |   Notifications", RFC 1891                     |
|    |          |  "Internet Message Access Protocol", RFC 2060  |
+----+----------+------------------------------------------------+
| 5. |REFERENCES| Separated REFERENCES to the normative and       |
|    |          | non-normative                                  |
+----+----------+------------------------------------------------+
| 6. |Appendix  | Changed the phrase from "NOT REQUIRED" to       |
|    | A        | "not required"                                 |
+----+----------+------------------------------------------------+
| 7. |Appendix  | Added "Appendix B  List of edits to RFC 2305"  |
+----+----------+------------------------------------------------+
```

Authors' Addresses

   Kiyoshi Toyoda
   Panasonic Communications Co., Ltd.
   4-1-62 Minoshima Hakata-ku
   Fukuoka 812-8531 Japan

   Fax: +81 92 477 1389
   EMail: toyoda.kiyoshi@jp.panasonic.com

   Hiroyuki Ohno
   National Institute of Information and Communications Technology
   4-2-1, Nukui-Kitamachi, Koganei, Tokyo,
   184-8795, Japan

   Fax: +81 42 327 7941
   EMail: hohno@ohnolab.org

   Jun Murai
   Keio University
   5322 Endo, Fujisawa
   Kanagawa 252 Japan

   Fax: +81 466 49 1101
   EMail: jun@wide.ad.jp

   Dan Wing
   170 W. Tasman Drive
   San Jose, CA 95134 USA

   Phone: +1 408 525 5314
   EMail: dwing@cisco.com

Full Copyright Statement

Intellectual Property

Acknowledgement