Network Working Group
Request for Comments: 4161
Category: Informational

K. Mimura
K. Yokoyama
T. Satoh
K. Watanabe
C. Kanaide
TOYO Communication Equipment
August 2005

Guidelines for Optional Services for Internet Fax Gateways

Status of This Memo

Copyright Notice

Abstract

To allow connectivity between the general switched telephone network facsimile service (GSTN fax) and the e-mail-based Internet Fax service (i-fax), an "Internet Fax Gateway" is required. This document provides guidelines for the optional functionality of Internet Fax Gateways. In this context, an "offramp gateway" provides facsimile data transmission from i-fax to GSTN fax; vice versa, an "onramp gateway" provides data transmission from GSTN fax to i-fax. The recommendations in this document apply to the integrated service including Internet Fax terminals, computers with i-fax software on the Internet, and GSTN fax terminals on the GSTN.

This document supplements the recommendation for minimal features of an Internet Fax Gateway. In particular, it covers techniques for dropping duplicated fax messages, automatic fax re-transmission, error, return notice, and log handling, and possible authorization methods by DTMF (Dual Tone Multi-Frequency) for onramp gateways.

1. Introduction

An Internet Fax Gateway can be classified as either an offramp gateway or an onramp gateway. This document provides guidelines for optional services and examples of Internet Fax Gateway operations. In particular, it covers techniques for dropping duplicated fax messages, automatic fax re-transmission, error, return notice, and log handling, and possible authorization methods by DTMF (Dual Tone Multi-Frequency) for onramp gateways.

A more detailed definition of onramps and offramps is provided in [1]. Recommended behaviors for Internet Fax Gateway functions are defined in [15].

This document provides recommendations only for the specific cases hereunder:

1) the operational mode of the Internet Fax is "store and forward", as defined in Section 2.5 of [1].

2) The format of image data is the data format defined by "simple mode" in [16].

This document does not apply to the gateway functions for "real-time Internet Fax", as described and defined in [18].

1.1. Key Words

The key words "MUST", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as described in [17].

2. Optional Services for an Offramp Gateway

2.1. Drop Duplicated GSTN Fax Transmission

Electronic mail transport agents (MTA) deliver an Internet Fax message into either the recipient's mailbox or an offramp gateway mailbox. Hence, the message is retrieved for further action, which in the case of the offramp gateway, will result in its delivery to the GSTN fax service.

The offramp gateway mailbox will thus receive all messages which the gateway will process, regardless of their final, distinct GSTN destinations. As such, addresses like

```
Fax=+12224567654@example.com
Fax=+38155234578@example.com
Fax=+3904567437777@example.com
```

will all end up in the offramp gateway mailbox corresponding to the "example.com" domain.

However, the handling of e-mail messages (including those of Internet Faxes) that contain more than one recipient, but are directed to the same final MTA, can be different, depending on the MTA configuration or features. A single message with multiple recipients in the SMTP envelope [19] is likely to be the most common case on the mail transport system, but it may happen that multiple copies of the same message are transmitted, one per recipient. Or it may happen that the final MTA is set to deliver a separate copy of the message per recipient into the final mailbox, supposing it is delivering messages to real mailboxes of distinct endusers.

Thus, it may happen that the offramp gateway receives multiple copies of the same Internet Fax message that is to be delivered to different GSTN destinations, which are listed together and repeatedly in the e-mail message headers [20] of the Internet Fax. In such cases, the offramp gateway SHOULD implement techniques to avoid duplicate or multiple transmission over GSTN of the same fax message to the same recipient.

Here are some possible, but non-exclusive, examples of these techniques.

2.1.1. SMTP Envelope Addresses Check

Using the SMTP [19] envelope destination address given in the "RCPT TO" field is usually the best technique to ensure that a received message is delivered to that address, and to avoid duplicate deliveries.

If the offramp gateway has the "RCPT TO" information still available during processing, then it MUST use it to determine the recipients over GSTN fax service.

2.1.2 Message-ID Check

If the SMTP "RCPT TO" information is not available (for example, in the case where the offramp gateway retrieves messages from its mailbox using either POP [21] or IMAP [22]), the message header "Message-ID" (see [20]) MAY be used to check if a message has already been processed, and hence avoid retransmission to all its GSTN recipients handled by the offramp gateway.

2.2. Error Handling

2.2.1. Recoverable Errors

Recoverable errors that happen during GSTN transmission are those where there is good chance that the error may not occur at the next attempt. This category includes "busy signal", "no line/carrier signal", etc.

For all these errors, the offramp gateway SHOULD re-queue the message and perform a retransmission attempt later on, as specified in Section 2.3.

2.2.2. Non-Recoverable Errors

If the error that occurs during GSTN transmission is likely non-recoverable, the offramp gateway SHOULD NOT attempt retransmission, and an error Message Delivery Notification (MDN) with appropriate error codes MUST be generated for the Internet Fax message sender. Examples of non-recoverable errors include paper-related errors (such as a jam, an empty tray, etc.) at a remote device, no response from a remote destination, voice response errors, data modem response errors, and stop event errors.

2.3. Automatic Re-Transmission Handling

An offramp gateway SHOULD implement a function that automatically tries to send facsimile data again if recoverable delivery failure occurs. If this function is implemented, then:

- the retry times and retry interval MAY be specified as options by the administrator of the offramp gateway;

- any error return notice SHOULD be sent only when the maximum number of retries has been completed without success;

- if transmission is suspended due to an error, then the subsequent transmission attempt SHOULD avoid retransmitting the pages already delivered successfully, if any.

2.4. Multiple Return Notice Handling

An offramp gateway can receive an Internet Fax for delivery to multiple GSTN recipients. If errors occur, which require the Internet Fax sender to be informed about them, or if the Internet Fax sender requested delivery notifications, then the offramp gateway has various ways to handle these multiple return notices:

1) An offramp gateway sends a return notice as soon as an error or a successful delivery occurs, per single GSTN recipient.

2) An offramp gateway gathers all information about the message, but sends a return notice only after all or a number of GSTN recipients have been handled (successfully or not).

If Case 2 is implemented, then the offramp gateway MAY also choose to send separate success and failure notices, or to limit the number of GSTN recipients handled per single return note (for example, no more than 10 recipients per return note).

2.5. Handling Transmission Errors for a Return Notice

When an offramp gateway fails in the transmission of a return notice, the Internet Fax Gateway SHOULD process the notice in either of the following ways:

1) The return notices SHOULD be re-queued, and delivery retried later. The number of retry attempts and the time interval between them MAY be a feature configured by the offramp gateway administrator. This is the preferred method to implement; however, if all the retransmission attempts fail, processing SHOULD continue as in Case 2.

2) If the gateway does not have enough capabilities to handle notice re-queuing, but has a log information preservation function, the error information SHOULD be recorded to a log, and processing SHOULD end. At this time, the administrator of the gateway system SHOULD be notified of these errors using a specific method (for example, by an e-mail message).

3) If the gateway does not even have a log information preservation function, the administrator SHOULD be notified about the failure (for example, via an e-mail message), and processing SHOULD end.

2.6. Offramp Gateway Log

An offramp gateway SHOULD have a function that keeps information listed as a log, either specific to the fax gateway or in a log file that exists locally on the gateway or remotely. If the fax gateway or the remote system are equipped with recording media, the log information SHOULD be saved as a log file. As a last resort, if no recording media are available, the log MAY be printed.

The information listed in the log MAY be the following:

- Date and time when the Internet Fax is received
- Sender address
- Recipient address(es)
- Start date and time of transmission over GSTN
- End date and time of transmission over GSTN
- Number of actually transmitted pages
- Number of actually transmitted bytes
- Fax resolution used
- Error codes/text that occurred during transmission
- Number of transmission attempts (retries)
- Date and time of transmission of the (eventual) delivery notice

3. Optional Services for an Onramp Gateway

3.1. Examples of User Authorization

An onramp gateway MAY have a user authorization function to confirm that the user is authorized to transmit a facsimile into the Internet fax service. For example, user authorization may be accomplished by getting a user ID and password received by DTMF, or via a local authorization table based on the GSTN caller-ID. The following subsections give some possible examples, but other methods are also possible.

3.1.1. Authorization via GSTN Caller-ID

The most simple method to authenticate and authorize a GSTN fax service user is to use the GSTN caller-ID. If available, in fact, the caller-ID is generated by the GSTN network service itself, and it is quite difficult to produce fake caller-IDs. In other words, the security related to this authentication method relies on the confidence that the GSTN caller-ID service is secure by itself.

The GSTN sender MAY be authorized via a lookup into a table managed by the onramp gateway administrator, via complete or partial (wildcard) matches.

3.1.2. Authorization via GSTN Fax "Station ID"

During the initial GSTN fax service negotiation, the sender fax can send various information to the onramp gateway, including the "station ID" alphanumeric string. This string MAY be used to transmit authentication and authorization information for subsequent lookup by the onramp gateway. Thus, user ID and an eventual password MAY be sent inside this string.

However, if used as the only authentication, this method is much less secure than the caller-ID one because the user of the calling GSTN station can decide which string to send, and the string travels in clear form over the GSTN. Given this security warning, this method allows more flexibility to the GSTN user: in fact, it is not tied to a single GSTN fax terminal, and authorization can be obtained from anywhere, provided the sender has the possibility to configure the "station ID" on the device being used.

A combination of caller-ID and station ID checks MAY, on the other hand, result in a greatly improved level of security.

3.1.3. Authorization via DTMF

An onramp gateway MAY implement the Authorization function by requesting that a user ID and password information are sent over GSTN via DTMF. For example, this function MAY be accomplished by requesting that the DTMF information is sent immediately after the connection over GSTN is established, before starting the GSTN fax negotiation; but other methods are also possible.

3.2. Onramp Gateway Log

An onramp gateway SHOULD have a function that keeps information listed as a log, either specific to the fax gateway or in a log file that exists locally on the gateway or remotely. If the fax gateway or the remote system are equipped with recording media, the log information SHOULD be saved as a log file. As a last resort, if no recording media are available, the log MAY be printed.

The information listed in the log MAY be the following:

- Start date and time of transmission from GSTN
- End date and time of transmission from GSTN
- Number of actually received pages
- Number of actually received bytes
- Fax resolution used
- Sender address (if available)
- Recipient address(es)
- Date and time when the Internet Fax is sent
- Error codes/text that occurred during Internet Fax transmission
- Number of transmission attempts (retries)
- Date and time of transmission of the (eventual) delivery notice

4. Security Considerations

Refer to Section 3.1 ("User Authorization") for authentication for an onramp gateway. In particular, sending user IDs and passwords in clear, as described in Section 3.1.2, can pose high security risks, and thus is NOT RECOMMENDED.

S/MIME [2][11][12][13][14] and OpenPGP [3][10] can also be used to encrypt an Internet Fax message. A signed or encrypted message is protected while transported along the network; however, when a message reaches an Internet Fax Gateway, either onramp or offramp, this kind of protection cannot be applied anymore. In this situation, security must rely on trusted operations of the gateway itself. A gateway might have its own certificate/key to improve security operations when sending Internet Faxes, but, as with any gateway, it breaks the end-to-end security pattern of both S/MIME and OpenPGP.

Other security mechanisms, like IPsec [4][5][6][7][8] or TLS [9] also do not ensure a secure gateway operation.

Denial-of-service attacks are beyond the scope of this document. Host compromise caused by flaws in the implementation is beyond the scope of this document.

5. Acknowledgments

Thanks to Claudio Allocchio (Consortium GARR, Italy) for its final review of this document, and for contributing the authorization and security sections of this document.

6. References

6.1. Informative References

[1] Masinter, L., "Terminology and Goals for Internet Fax", RFC 2542, March 1999.

[2] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004.

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

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

[5] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[6] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, September 2001.

[7] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[8] Thayer, R., Doraswamy, N., and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.

[9] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 3546, June 2003.

[10] Elkins, M., Del Torto, D., Levien, R., and T. Roessler, "MIME Security with OpenPGP", RFC 3156, August 2001.

[11] Rescorla, E., "Diffie-Hellman Key Agreement Method", RFC 2631, June 1999.

[12] Ramsdell, B., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling", RFC 3850, July 2004.

[13] Ramsdell, B., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", RFC 3851, July 2004.

[14] Hoffman, P., "Enhanced Security Services for S/MIME", RFC 2634, June 1999.

6.2. Normative References

[15] Mimura, K., Yokoyama, K., Satoh, T., Kanaide, C., and C. Allocchio, "Internet Fax Gateway Requirements", RFC 4160, August 2005.

[16] Toyoda, K., Ohno, H., Murai, J., and D. Wing, "A Simple Mode of Facsimile Using Internet Mail", RFC 3965, December 2004.

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

[18] "Procedures for real-time Group 3 facsimile communication over IP networks", ITU-T Recommendation T.38, June 1998.

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

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

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

[22] Crispin, M., "Internet Message Access Protocol - Version 4rev1", RFC 3501, March 2003.

Authors' Addresses

Katsuhiko Mimura
TOYO Communication Equipment CO., LTD.
2-1-1 Koyato, Samukawa-machi, Koza-gun
Kanagawa-pref., Japan

Fax: +81 467 74 5743
EMail: mimu@miyabi-labo.net

Keiichi Yokoyama
TOYO Communication Equipment CO., LTD.
2-1-1 Koyato, Samukawa-machi, Koza-gun
Kanagawa-pref., Japan

Fax: +81 467 74 5743
EMail: keiyoko@msn.com

Takahisa Satoh
TOYO Communication Equipment CO., LTD.
2-1-1 Koyato, Samukawa-machi, Koza-gun
Kanagawa-pref., Japan

Fax: +81 467 74 5743
EMail: zsatou@t-ns.co.jp

Ken Watanabe
TOYO Communication Equipment CO., LTD.
2-1-1 Koyato, Samukawa-machi, Koza-gun
Kanagawa-pref., Japan

Fax: +81 467 74 5743
EMail: knabe@ad.cyberhome.ne.jp

Chie Kanaide
TOYO Communication Equipment CO., LTD.
2-1-1 Koyato, Samukawa-machi, Koza-gun
Kanagawa-pref., Japan

Fax: +81 467 74 5743
EMail: icemilk77@yahoo.co.jp

Full Copyright Statement

Intellectual Property

Acknowledgement

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