[MS-OXSMTP]: Simple Mail Transfer Protocol (STMP) Mail Submission Extensions Specification

Intellectual Property Rights Notice for Protocol Documentation

- **Copyrights.** This protocol documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the protocols, and may distribute portions of it in your implementations of the protocols or your documentation as necessary to properly document the implementation. This permission also applies to any documents that are referenced in the protocol documentation.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the protocols. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, the protocols may be covered by Microsoft's Open Specification Promise (available here: http://www.microsoft.com/interop/osp). If you would prefer a written license, or if the protocols are not covered by the OSP, patent licenses are available by contacting protocol@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. This protocol documentation is intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it. A protocol specification does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them.

Revision Summary			
Author	Date	Version	Comments
Microsoft Corporation	April 4, 2008	0.1	Initial Availability.
Microsoft Corporation	June 27, 2008	1.0	Initial Release.

Table of Contents

1 Introduction

The Simple Mail Transport Protocol (SMTP) Message Submission for Mail protocol, as specified in [RFC4409], profiles SMTP mechanisms specified in [RFC2821] and others to provide mail submission mechanisms for client mail systems. SMTP was originally defined to provide for mail transfer between mail servers. SMTP is now widely used as a message submission mechanism, where client messaging systems introduce new messages into the mail routing network.

This specification profiles [RFC4409], identifying the elements necessary to conform to Exchange Server protocols.

1.1 Glossary

The following terms are defined in [MS-OXGLOS]:

Mail User Agent (MUA)
Simple Mail Transfer Protocol (SMTP)

The following terms are specific to this document:

Message Submission Agent (MSA): A process that accepts messages from a **Mail User Agent (MUA)** and either delivers it or acts as a **Simple Mail Transfer Protocol (SMTP)** client to submit the messages to a **Message Transfer Agent (MTA)**.

Message Transfer Agent (MTA): An SMTP server that accepts mail from a **Mail Submission Agent (MSA)** or another **MTA** and delivers the mail or relays it to another **MTA**.

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as described in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

1.2.1 Normative References

[MS-OXGLOS] Microsoft Corporation, "Office Exchange Protocols Master Glossary", April 2008.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.ietf.org/rfc/rfc2119.txt.

[RFC4409] Gellens, R. and Klensin, J., "Message Submission for Mail", RFC 4409, April 2006, http://www.ietf.org/rfc/rfc4409.txt.

1.2.2 Informative References

[RFC2821] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001, http://www.ietf.org/rfc/rfc2821.txt.

[RFC821] Postel, J., "Simple Mail Transfer Protocol", RFC 821, August 1982, http://www.ietf.org/rfc/rfc821.txt.

1.3 Protocol Overview

[RFC4409] describes a profile of SMTP [RFC2821] and others that defines how clients submit mail to a server. This document specifies which parts of [RFC4409] are necessary for message submission.

1.4 Relationship to Other Protocols

This specification profiles [RFC4409] to define the protocol for message submission. [RFC4409] is based on SMTP as specified in [RFC2821].

1.5 Prerequisites/Preconditions

None.

1.6 Applicability Statement

This protocol is applicable to scenarios where clients will be submitting e-mail messages directly to a server.

1.7 Versioning and Capability Negotiation

This specification introduces no new versioning mechanisms beyond those that exist in SMTP.

Negotiation of SMTP options is part of [RFC4409]. The EHLO response indicates what capabilities are present on the server.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

2 Messages

2.1 Transport

None.

2.2 Message Syntax

None.

3 Protocol Details

This protocol describes the process for a client submitting e-mail messages to a **Message Transfer Agent (MTA)**. In [RFC4409], three components are described to represent the interaction: a **Mail User Agent (MUA)**, a **Message Submission Agent (MSA)**, and an MTA. These components describe an architecture, shown in Figure 1, where the MUA creates the message, the MSA picks it up and, via SMTP, submits it to the MTA for transmission to the recipient.

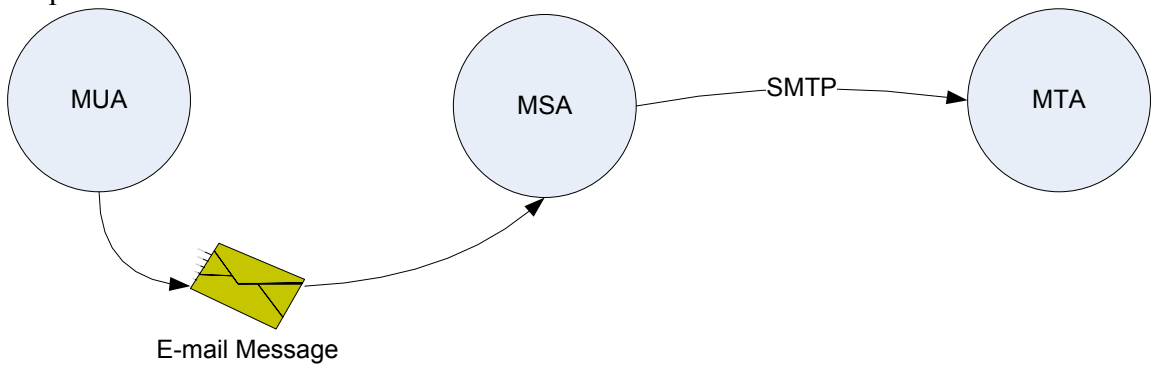

Figure 1: Message transmission

Most modern e-mail clients combine the MUA and the MSA, such that there is no perceptible handoff between the MUA and MSA functions. As a result, the MSA provides SMTP client capabilities while the MTA provides the SMTP server capabilities. This protocol only covers the path between the MSA and the MTA. Thus the profile of [RFC4409] provided is broken into two roles – the client and the server – where the client performs SMTP submissions and the server accepts the SMTP submissions. Aspects of [RFC4409] that describe the interaction between the MUA and the MSA are specifically excluded from this protocol.

3.1 Client Details

The MUA/MSA process is the client. The MUA functionality is used to acquire or create the message and the MSA functionality performs an SMTP client submission. The client, therefore, only acts as an SMTP client; it does not have the ability to receive messages via SMTP as an SMTP server.

The client protocol for message submission conforms to [RFC4409] except as identified in the following table.

Section	Description
3.1	The client SHOULD submit messages on port 587, port 25 or any port that a site chooses for message submission.
3.2	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.
3.3	The client SHOULD authenticate using mechanisms defined in [RFC2554]. The client SHOULD use AUTH LOGIN or AUTH NTLM.
4.1	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.
4.2	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.
4.3	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.
5.1	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.
5.2	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.
6	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.
7	The client SHOULD support DSN, AUTH, and STARTTLS. AUTH SHOULD be supported as specified in section 3.3 of this table.
8	This section is not included in the client profile because the MUA and MSA functionality are integrated into the same process.

3.1.1 Abstract Data Model

None.

3.1.2 Timers

None.

3.1.3 Initialization

None.

3.1.4 Higher-Layer Triggered Events

None.

3.1.5 Message Processing Events and Sequencing Rules

None.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

3.2 Server Details

The server component of message submission conforms to [RFC4409] except as identified in the following table.

Section	Description
3.1	The server SHOULD allow messages to be submitted on port 587, port 25, or any port that a site chooses for message submission.
3.2	The server SHOULD offer authenticate mechanisms as defined in [RFC2554].
3.3	The server SHOULD offer authenticate mechanisms as defined in [RFC2554]. The client SHOULD offer AUTH LOGIN or AUTH NTLM.
4.1	The server SHOULD respond with a 550 or a 554 for error conditions.
4.2	The server SHOULD respond with a 550 or a 554 for error conditions.
4.3	The server SHOULD require client authentication. If the server does not require client authentication, the server MUST NOT issue an error response to an unauthenticated MAIL command.
7	The server SHOULD implement DSN, AUTH, and STARTTLS. The server SHOULD offer AUTH LOGIN and AUTH NTLM.

3.2.1 Abstract Data Model

None.

3.2.2 Timers

None.

3.2.3 Initialization

None.

3.2.4 Higher-Layer Triggered Events

None.

3.2.5 Message Processing Events and Sequencing Rules

None.

3.2.6 Timer Events

None.

3.2.7 Other Local Events

None.

4 Protocol Examples

None.

5 Security

5.1 Security Considerations for Implementers

None.

5.2 Index of Security Parameters

Security parameters for message submission authentication are described in [RFC4409].

Appendix A: Office/Exchange Behavior

The information in this specification is applicable to the following versions of Office/Exchange:

- Office 2003 with Service Pack 3 applied
- Exchange 2003 with Service Pack 2 applied
- Office 2007 with Service Pack 1 applied
- Exchange 2007 with Service Pack 1 applied

Exceptions, if any, are noted below. Unless otherwise specified, any statement of optional behavior in this specification prescribed using the terms SHOULD or SHOULD NOT implies Office/Exchange behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies Office/Exchange does not follow the prescription.

Index