[MS-XLOGIN]: SMTP Protocol AUTH LOGIN Extension 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/default.mspx). 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.

Preliminary Documentation. This documentation is preliminary documentation for these protocols. Since the documentation may change between this preliminary version and the final version, there are risks in relying on preliminary documentation. To the extent that you incur additional development obligations or any other costs as a result of relying on this preliminary documentation, you do so at your own risk.

Tools. This protocol documentation is intended for use in conjunction with publicly available standard specifications and networking programming art, and assumes that the reader is either 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 a Licensee to develop an implementation. Licensees who have access to Microsoft programming tools and environments are free to take advantage of them.

Revision Summary			
Author	Date	Version	Comments
Microsoft Corporation	April 4, 2008	0.1	Initial Availability

Table of Contents

1 Introduction

This document specifies an authentication mechanism that is provided through the SMTP Service Extension for Authentication [RFC 4954] called AUTH LOGIN.

1.1 *Glossary*

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

Secure Sockets Layer (SSL)
Simple Mail Transfer Protocol (SMTP)

The following term is specific to this document:

Transport Layer Security (TLS): A security protocol that supports confidentiality and integrity of messages in client and server applications communicating over open networks. **TLS** supports server and, optionally, client authentication by using X.509 certificates (as specified in [X509]). **TLS** is standardized in the IETF TLS working group.

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.

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

[RFC4234] Crocker, D., Ed. and Overell, P., "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005, http://www.ietf.org/rfc/rfc4234.txt.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006, http://www.ietf.org/rfc/rfc4648.txt.

[RFC4954] Siemborski, R. and Melnikov, A., "SMTP Service Extension for Authentication", RFC 4954, July 2007, http://www.ietf.org/rfc/rfc4954.txt.

1.2.2 Informative References

[RFC4346] Dierks, T. and Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006, http://www.ietf.org/rfc/rfc4346.txt.

[SSL] A. Frier, P. Karlton, and P. Kocher, "The SSL Protocol Version 3.0", November 1996, http://wp.netscape.com/eng/ssl3/draft302.txt.

1.3 Protocol Overview (Synopsis)

Client applications that connect to the **Simple Mail Transfer Protocol (SMTP)** service can use a number of different authentication mechanisms. The SMTP Service Extension for Authentication [RFC4954] defines a service extension to SMTP as specified in [RFC2821], where a client SHOULD specify an authentication method to the server. AUTH LOGIN is one such authentication protocol for SMTP.

1.4 Relationship to Other Protocols

This specification defines an implementation of a protocol using [RFC4954].

1.5 Prerequisites/Preconditions

All prerequisites and preconditions are specified in [RFC2821] and [RFC4954].

1.6 Applicability Statement

This protocol extension does not change the way that [RFC4954] is used.

1.7 Versioning and Capability Negotiation

None.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

2 Messages

The following sections specify the AUTH LOGIN message syntax and how they are transported.

2.1 Transport

This protocol extension does not change the base transport specified by [RFC 4954].

2.2 Message Syntax

2.2.1 EHLO Response

Server support for the AUTH LOGIN extension is identified in the EHLO response per Section 3 of [RFC4954]. For example:

```
S: 220 smtp.example.com
C: EHLO client.example.com
S: 250-smtp.example.com  Hello client.example.com
S: 250 AUTH LOGIN
```

The server response of AUTH LOGIN as part of the responses to EHLO indicates support for AUTH LOGIN.

2.2.2 User Name and Password Values

The AUTH LOGIN extension transmits two values as part of the message sequence, a user name and a password. Each of these values is encoded using base64 per [RFC4648] before being transmitted. The values, before encoding, are defined as follows:

```
USERNAME = 1*CHAR

PASSWORD = 1*CHAR
```

2.2.3 AUTH LOGIN Command

Support for LOGIN authentication is through the AUTH command, per Section 4 of [RFC4954]. There are two forms for requesting LOGIN authentication, described in the following sections.

2.2.3.1 Simple AUTH LOGIN

To request LOGIN authentication, the client issues the AUTH command with the parameter LOGIN (AUTH_LOGIN_COMMAND):

```
AUTH LOGIN<CR><LF>
```

If AUTH LOGIN is not supported, the server responds with a 504 error message per section 4 of [RFC4954].

If AUTH LOGIN is supported on the server, the server responds with the AUTH_LOGIN_Username_Challenge:

```
334 VXNlcm5hbWU6<CR><LF>
```

The client then responds with the user name to be used for authentication, base64 encoded per [RFC4648]. For example, if the client's user name was "Charlie", the client would respond with the following Login_Username_Response:

```
       Q2hhcmxpZQ==<CR><LF>
```

The server then responds with the AUTH_LOGIN_Password_Challenge:

```
       334 UGFzc3dvcmQ6<CR><LF>
```

The client then responds with the password to be used for authentication, base64 encoded per [RFC4648]. For example, if the client's password was "password", the client would respond with the following Login_Username_Response:

```
       cGFzc3dvcmQ=<CR><LF>
```

If the authentication is successful, the server then issues a LOGIN_Succeeded_Response or a LOGIN_Failed_Response, corresponding to a 235 reply for success or a 535 reply for a failure, per [RFC4954].

2.2.3.2 AUTH LOGIN with User Name

To request LOGIN authentication, the client issues the AUTH command with the parameter LOGIN and the user name to be used for authenticatin, base64 encoded per [RFC4648].]. For example, if the client's user name was "Charlie", the client would initiate AUTH LOGIN as follows (AUTH_LOGIN_COMMAND_USER):

```
       AUTH LOGIN Q2hhcmxpZQ==<CR><LF>
```

If AUTH LOGIN is not supported, the server responds with a 504 error message per section 4 of [RFC4954].

If AUTH LOGIN is supported on the server, the server then responds with the AUTH_LOGIN_Password_Challenge:

```
       334 UGFzc3dvcmQ6<CR><LF>
```

The client then responds with the password to be used for authentication, base64 encoded per [RFC4648]. For example, if the client's password was "password", the client would respond with the following Login_Username_Response:

```
       cGFzc3dvcmQ=<CR><LF>
```

If the authentication is successful, the server then issues a LOGIN_Succeeded_Response or a LOGIN_Failed_Response, corresponding to a 235 reply for success or a 535 reply for a failure, per [RFC4954].

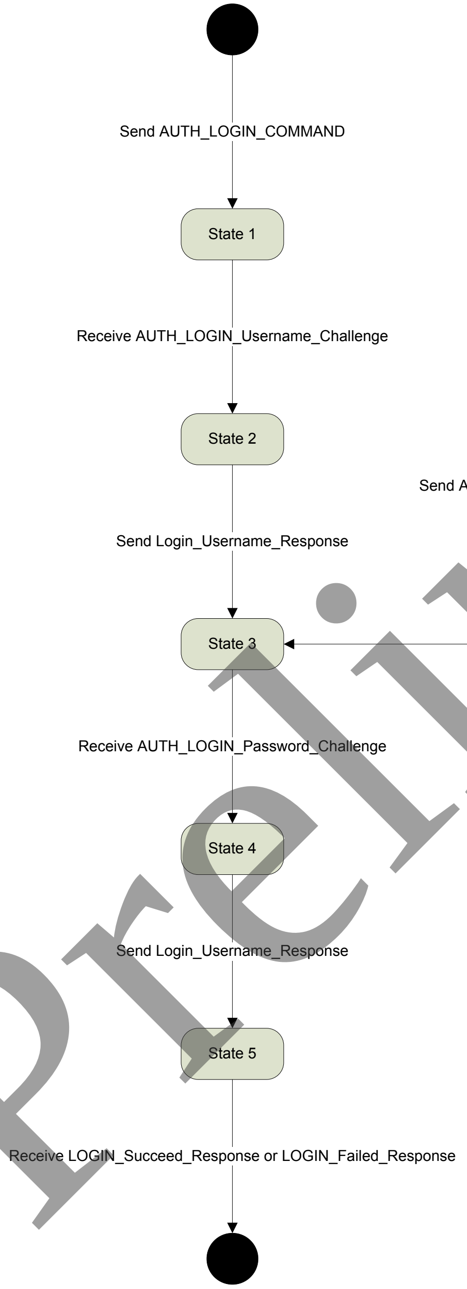
3 Protocol Details

The following sections specify details of the AUTH LOGIN protocol extension, including abstract data models and message processing rules.

3.1 Common Details

3.1.1 Abstract Data Model

The abstract data model shown in Figure 1 represents the sequence of messages described in the previous section.



Send AUTH_LOGIN_COMMAND
State 1
Receive AUTH_LOGIN_Username_Challenge
State 2
Send AUTH_LOGIN_COMMAND_USER
Send Login_Username_Response
State 3
Receive AUTH_LOGIN_Password_Challenge
State 4
Send Login_Username_Response
State 5
Receive LOGIN_Succeed_Response or LOGIN_Failed_Response

Figure 1: Abstract data model

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

This protocol does not change message processing events or sequencing rules of messages beyond that which is described if [RFC4954].

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

4 Protocol Examples

Following is an example of the use of the AUTH LOGIN protocol extension. The example demonstrates SMTP authentication using the AUTH LOGIN protocol.

```
S: 220 smtp.example.com
C: EHLO client.example.com
S: 250-smtp.example.com  Hello client.example.com
S: 250 AUTH LOGIN
C: AUTH LOGIN
S: 334 VXNlcm5hbWU6
C: Q2hhcmxpZQ==
S: 334 UGFzc3dvcmQ6
C: cGFzc3dvcmQ=
S: 235 authentication successful
```

In this example, a client connects to an SMTP server. The initial response by the server (“220 smtp.example.com”) is the greeting by the server. The client responds with the EHLO command, which is required to activate the extended command set. The server responds with, among other things, an indication of support for AUTH LOGIN. The client then issues the AUTH LOGIN command. The server responds with the first base64 encoded challenge. The client responds with “W2hhcmxpZQ==”, which is the base64 encoded name “Charlie”. The server then issues the second base64 encoded challenge and the client response with “cGFzc3dvcmQ=”, which is the base64 encoded password “password”. Successful authentication then results in a server response of 235.

5 Security

5.1 Security Considerations for Implementers

This protocol offers no inherent security mechanisms to protect the user credentials during authentication. Because of this, it is extremely important to only use this protocol when also using a secure communication channel such as **Secure Sockets Layer (SSL)** or Transport **Layer Security (TLS)**. Even if using SSL or TLS, the authentication credentials are available to the SMTP server, where it is possible that they could be recorded for future use. The recommendation, therefore, is to not use this protocol except in circumstances where no other option is available.

In environments where the use of TLS or other external security is mandated, the AUTH LOGIN advertisement SHOULD be suppressed until a secure channel is negotiated. TLS in particular exhibits this behavior where the SMTP session is restarted after TLS is negotiated and is explained in more detail in [RFC4346].

5.2 Index of Security Parameters

None.

6 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