The Cipher Mail Transport Protocol

Jonathan Moroney

June 29, 2016

Contents

1 Command overview

The Cipher Mail Transport Protocol (CMTP) uses ASCII text for commands and replies. UTF-8 is used for user strings and domain strings where applicable. The commands used were chosen to be similar to SMTP commands without overlapping. Further the design of the CMTP commands enables

stateless server design. Null bytes are used as terminators for commands and parameters.

2 OHAI

OHAI is the 'HELO' of CMTP. It was chosen to conform with the 4 character limit of early SMTP implementations. By using a 4 character string which is unknown to SMTP,; CMTP should be able to gracefully coexist on the same ports as SMTP.

2.1 Parameters

None.

2.2 Replies

A reply to OHAI can either be success or failure. In the success case the respondent should reply with 'OHAI' followed by their CMTP server version string. Anything else is considered a failure.

3 MAIL

The MAIL command is used to pass a message and is followed by the CMTP message data structure. This data structure is self describing.

3.1 Parameters

The only parameter MAIL handles is a CMTP message.

3.2 Replies

On success a CMTP server replies with
SUCCESS[Sig][\0]
Where 'Sig' is the server signature of the message 'SUCCESS'. The message is followed by a null character.
On failure a CMTP server replies with
FAILURE[Sig][\0]
Where 'Sig' is the server signature of the message 'FAILURE'. The message is followed by a null character.

4 KEYREQUEST

The KEYREQUEST command is used to transfer user and server public keys. This command is what allows for the transparent encryption model of

CMTP.

4.1 Parameters

There are two parameters for KEYREQUEST; USER and DOMAIN. A null user refers to the server and a null domain refers to the local domain. Thus, a server receiving a keyrequest for null null would return its' own public key. Keyrequest always replies with the most recent key version available.

4.2 Replies

Success is when a key is available and car be returned to the requester. In this event the key is passed back in the following form.
[Version][PublicKey][Sig][\0]
Where 'Sig' is the server signature of the public key. The version number is four bytes and defines the length of both the public key and the signature. The server signature is always present even in the case when the server is distributing its' own public key.
Failure cases are handled with the generic failure message.
FAILURE[Sig][\0]
Where 'Sig' is the server signature of the message 'FAILURE'. The message is followed by a null character.

5 LOGIN

The LOGIN command facilitates private key distribution through the xzibit data structure.

5.1 Parameters

LOGIN takes a single parameter which is a null terminated UTF-8 string. This string is the user who wishes to retrieve their xzibit.
LOGIN[\0]USER[\0]

5.2 Replies

On success the CMTP server replies with
[UserXzibit][Sig][\0]
Where Sig is the server signature of the users' xzibit.
If the user has no xzibit then the user has not been added. In this case the CMTP server passes a generic failure message.
FAILURE[Sig][\0]

6 NOOP

The NOOP command is used as a way to test an active connection.

6.1 Parameters

NOOP takes no parameters.

6.2 Replies

A CMTP server should reply with its' version string in response to the NOOP command.

7 OBAI

OBAI is the inverse of the OHAI command and is used to terminate connections.

7.1 Parameters

OBAI takes no parameters.

7.2 Replies

There is no reply to to the OBAI command. The CMTP server should simply kill the active connection.