

# The Cipher Mail Transport Protocol Interface

Jonathan Moroney

April 28, 2016

## Contents

<b>1</b>	<b>Command Overview</b>	<b>1</b>
1.1	OHAI . . . . .	1
1.2	MAIL . . . . .	1
1.3	KEYREQUEST <USER> <DOMAIN> . . . . .	2
1.4	NOOP . . . . .	2
1.5	LOGIN <USER> . . . . .	2
1.6	OBAI . . . . .	2
<b>2</b>	<b>General Responses</b>	<b>3</b>

## 1 Command Overview

The Cipher Mail Transport Protocol (CMTP) uses a text based, command/reply interface similar to that of the Simple Mail Transport Protocol (SMTP). The commands for CMTP have been designed to make stateless implementation easy. All commands are ASCII strings terminated by a null character (`\0`). ASCII is used over utf-8 for commands as each ASCII character corresponds to one byte.

### 1.1 OHAI

The OHAI command is in place to prevent SMTP clients from seeing a CMTP server as a valid SMTP server. Conveniently OHAI is four characters long which should mean even the oldest SMTP client should fail in a defined way when attempting to connect to a CMTP server.

### 1.2 MAIL

The MAIL command is a stand alone command which servers only to tell the CMTP server that a message is to follow. The CMTP message is self describing in length so that a server knows when it has received the entire thing. Subsequently no state is needed in order to pass a message.

### 1.3 KEYREQUEST <USER> <DOMAIN>

The KEYREQUEST command takes at least one parameter and at most two. The user parameter is required while the domain parameter is not. Each parameter is null terminated. In the case that the domain parameter is not present the CMTTP server should assume that the user is local to it. The reply format is

[Version][UserPublicKey][\0][ServerSigOfKey][\0].

Errors and messages use a similar reply format but with the Version = 0 which corresponds to the plaintext crypto case

[Version][Message][\0][ServerSigOfMessage][\0].

In this way delays and 'no key' messages can be passed back to the client. Currently the only error message is

#### KEYNOTAVAILABLE

Used as a reply if requested key does not exist. On the wire this looks like [Version][KEYNOTAVAILABLE][\0][ServerSigOfMessage][\0]

### 1.4 NOOP

The NOOP command exists because SMTP has a NOOP command. This may be removed if a better reason for existence cannot be found.

### 1.5 LOGIN <USER>

The LOGIN command takes one parameter and returns an encrypted copy of the users xzibit. The xzibit is the encrypted private key for the user. If authentication is desired a user reply can be implemented which has the user encrypt their exhibit with the server's public key and forwards that back to the server. This is currently not implemented. Version one defines the reply as

[Version][XzibitLength][Xzibit][ServerSigofXzibit] Field lengths are as follows.

- Version: 4 bytes
- XzibitLength: 4 bytes
- Xzibit: Length defined by XzibitLength. XzibitLength\*(1 byte).
- ServerSigofXzibit: Defined by crypto version. In version 1 signatures are 64 bytes long.

### 1.6 OBAI

The OBAI command is in place to terminate a connection. Connections may terminate for other reasons (time outs, tcp connection breaking, etc...), but OBAI allows for a graceful exit.

## 2 General Responses

There are two general responses that follow the general message structure.

### **SUCCESS**

Used to indicate that a command was received and processed. [SUCCESS][\0][ServerSigOfMessage][\0]

### **FAILURE**

Used to indicate that a command was received and not processed. [FAILURE][\0][ServerSigOfMessage][\0]