The Cipher Mail Transport Protocol

Jonathan Moroney

July 5, 2016

Contents

1 CMTP Message

At the high level a Cipher Mail Message is broken into two classes. Envelope Data and Message Data. Envelope data is the plaintext used for routing a message and determining how to read it. Message data is the encrypted payload. Envelope information includes the sender and receiver, the version number, the log length and log body, the attachment count and attachment lengths, and the message length. All data is in network order on the wire. That is Big Endian. It is not strictly required that CMTP messages be stored on disk in Big Endian format, but it is highly advised. All reference code preserves the network data structure on disk. A high level view of the CMTP message can be seen in figure 1 with a scale in bytes.

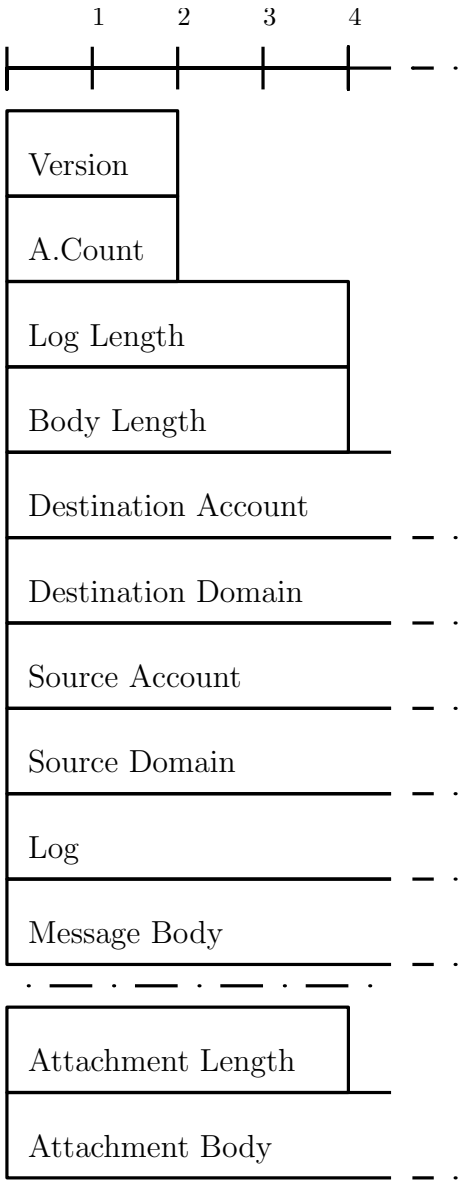

Figure 1: Message Diagram

1.1 Envelope Data

The envelope data is everything other than the message body and the attachment body. These fields are plaintext and used for routing and general message management. The fields in the message are

Version
: A four byte integer used to mark the version of the message structure. The type of cryptography in use is also defined by this number. This

document covers version 1.

Attachment Count
A four byte integer used to mark how many attachment fields follow.

Log Length
An eight byte integer (long) used to mark how many bytes are in the log field.

Body Length
An eight byte integer (long) used to mark how many bytes are in the message body field.

Destination Account
A null terminated utf-8 string used to denote the recipient account of the message. Max length is 256 bytes including the null terminator.

Destination Domain
A null terminated utf-8 string used to denote the recipient domain of the message. Max length is 256 bytes including the null terminator.

Source Account
A null terminated utf-8 string used to denote the sender account of the message. Max length is 256 bytes including the null terminator.

Source Domain
A null terminated utf-8 string used to denote the sender domain of the message. Max length is 256 bytes including the null terminator.

Log
Discussed in subsection 2.

Message Body
Discussed in subsection 3.

Attachment Length
An eight byte integer (long) used to mark how many bytes are in next attachment body.

Attachment Body
Discussed in subsection 3.

1.2 The Log

The Log is a simple structure of null terminated UTF-8 strings. The smallest possible log is a single null byte.

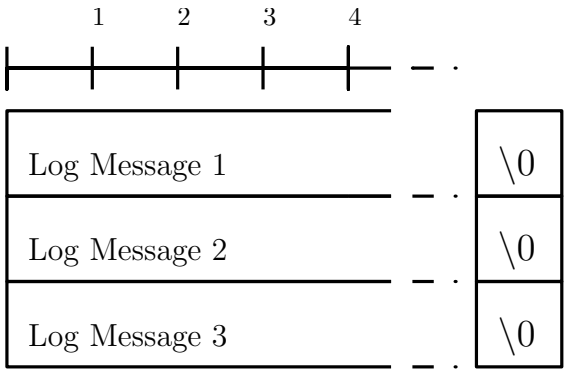

Figure 2: Log Diagram

1.3 The Message Body

The internals of the encrypted message body were designed to be feature compatible with current email implementations, ie. carbon copy, reply-to, and subject headers are all present. Additionally a 4 byte time-stamp is placed inside to provide a creation date record. The message body diagram follows.

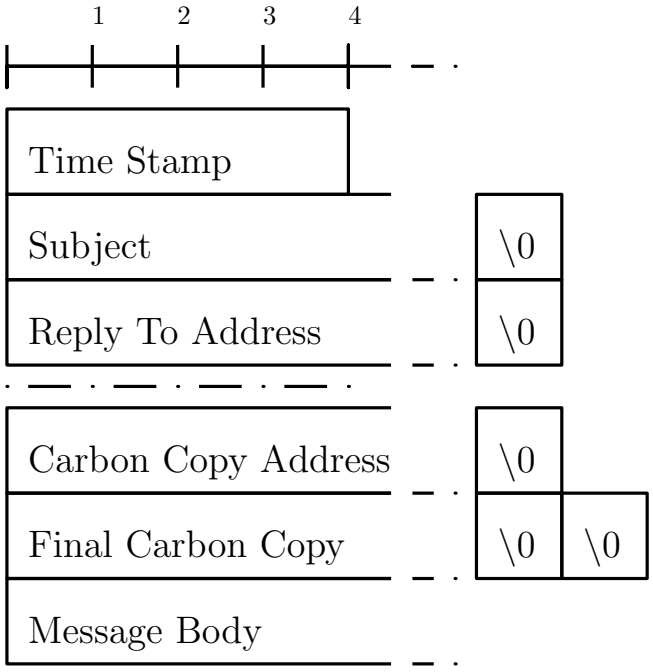

Figure 3: CMTP Message Internals

The only intricacy of the message body is the variable number of carbon copies. The last carbon copy is double null terminated while all other carbon

copies are single null terminated. It is perfectly valid to have no carbon copies at all and in this case there are simply two null characters following the reply-to null character. For clarity a diagram of the no carbon copy case is included.

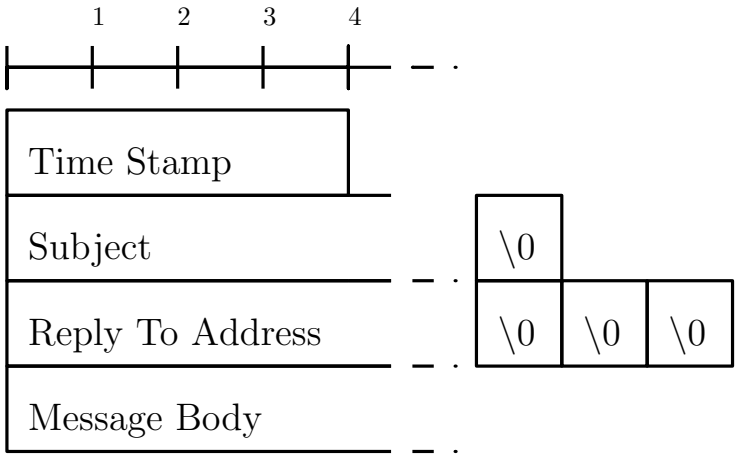

Figure 4: CMTP Message with no carbon copies

1.4 The Attachment Body

The attachment body is two parts. The first is the null terminated UTF-8 file name and the second is the attachment data itself.

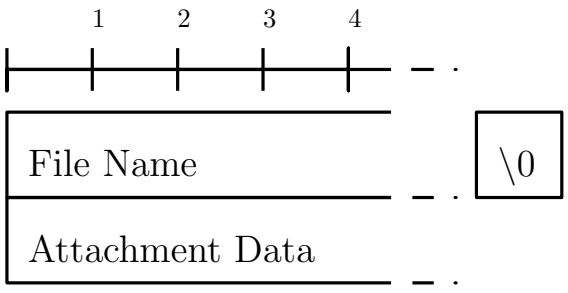

Figure 5: CMTP Attachment Internals

2 Xzibit key store

The Xzibit continues the trend of simple data structures with the following.

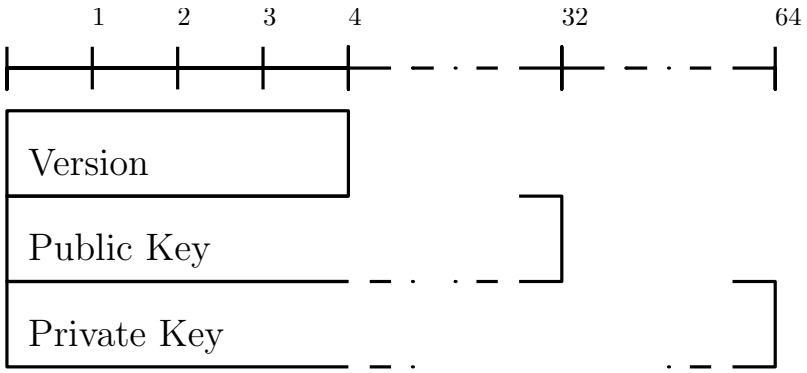

Figure 6: CMTP Xzibit Internals

In this diagram we see a version number which is an unencrypted integer and the two user keys which are encrypted using a symmetric cipher keyed from user input.