The Cipher Mail Message Format

Jonathan Moroney

February 18, 2016

Contents

1 High level overview

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.

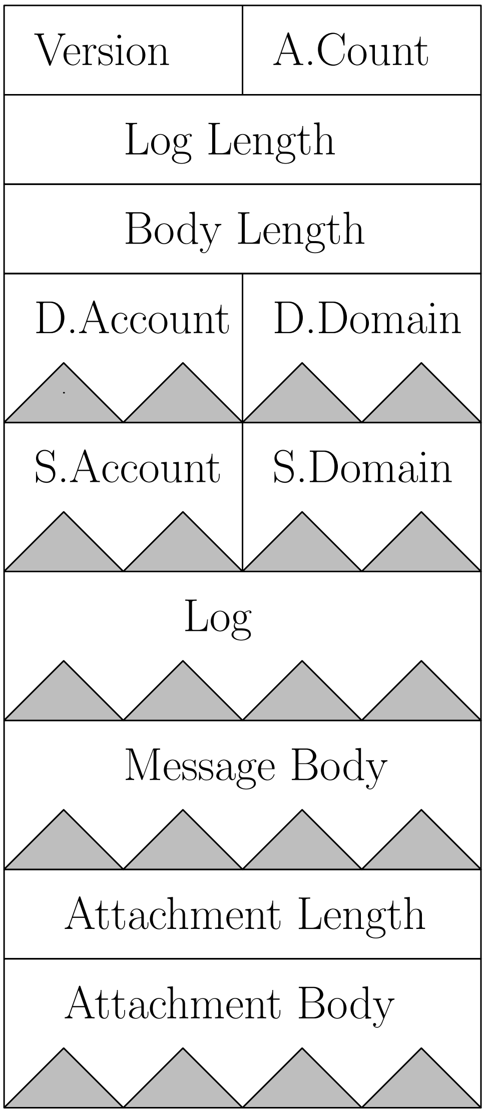

Figure 1: Cipher Mail Message Format

In figure 1 we see the a graphical overview of the message format. A single row is 8 bytes and a sawtooth bottom means variable length. Abreviations are:

1. A.Count = Attachment Count
2. D.Account = Destination Account
3. D.Domain = Destination Domain
4. S.Account = Source Account
5. S.Domain = Source Domain

1.1 Field Defenitions

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 255 bytes.

Destination Domain

A null terminated utf-8 string used to denote the recipient domain of the message. Max length is 255 bytes.

Source Account

A null terminated utf-8 string used to denote the sender account of the message. Max length is 255 bytes.

Source Domain

A null terminated utf-8 string used to denote the sender domain of the message. Max length is 255 bytes.

Log

Discussed in section II.

Message Body

Discussed in section III.

Attachment Length

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

Attachment Body

Discussed in section IV.

2 Log Structure

The log is simply defined as a collection of line feed terminated, utf-8 messages. The log is to be used by any entity processing the specific piece of mail and can be used for general status messages as well as for more critical issues.

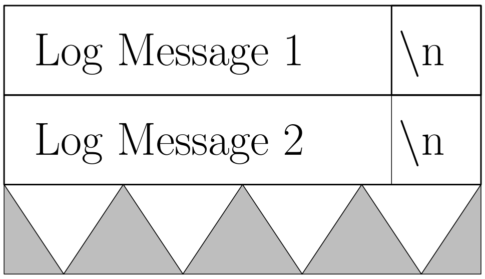

Figure 2: Cipher Mail Log Format

3 Message Body Structure

3.1 Internal Header

The internal header of a cipher mail message needs to contain a variable amount of information; A Subject line/field, a Reply To address, Carbon Copy addresses, and a Creation Date. As such the header itself is a variable length structure with each line item being a utf-8 string terminated by a null character. The ordering of the fields is Reply-To, Subject, Date, Carbon Copies. The carbon copies are username\0domain\0 and are terminated by a double null. ie. \0\0.

3.2 Internal Body

This section is simply a block of utf-8 encoded text. Any non-text data should be transmitted through attachments.

4 Attachment Structure

The Attachment is a simple structure. The first 255 bytes of the structure is reserved for the utf-8 file name and the rest of the structure is for actual file data. The file name should be null terminated unless it is using all 255 bytes for name data.