

SMTP delivery feature set for CCM

02/07/08
version 0.1

1 Introduction and Notation

This note is a strawman proposal for an interoperability profile for using SMTP for the delivery of Cinema Control Messages (CCMs). Its purpose is to simplify implementation and promote early interoperability by specifying which SMTP features are required for this application, which features are optional and which features are prohibited. Defining interoperability profiles always leads to questions since standards may mandate support for features prohibited in the profile; the way around this is to say that interoperability is only assured if those features are not used.

2 General: Mode of Operation

"Embedded" SMTP servers. This profile primarily addresses message transport between an SMTP server inside the KDM provider network and another SMTP server inside the theater network, protected by firewall. The SMTP transfers run over a direct TCP connection across the Internet between the servers. These servers should be dedicated to this application; CCMs should not be sent to a general-purpose corporate e-mail server as the policies of such a server may not handle CCMs with an appropriate high-priority. These servers should be behind firewalls to protect them against denial of service attacks.

The profile is intended to support automated processing of KDM related messages. The following CCM message types are supported:

- KDMTransmission
- KDMZipTransmission [or other compression standard recommended by ISDCF]
- FLMTransmission
- StatusRequest
- StatusResponse [RRM]
- Exception

[Editor's note: the CCM has not yet been fully defined. I am assuming it will contain at least the above six message types].

Although this document only defines MTA behavior, it is assumed that there is a user agent function intimately related to the SMTP server.

3 Addressing.

3.1 SMTP to/from Internet addresses:

DNS subdomains would be used to address these servers. Example:
KdmSmtpl.AtlantaMultiplexA.mychain.com

In an exhibitor network, the local part of the e-mail address should be "DKMS" as indicated in [NATO]. Continuing the above example:
dkms@ KdmSmtpl.AtlantaMultiplexA.mychain.com

These are the addresses of the servers that take responsibility for ensuring that the message is processed by the appropriate target entity.

3.2 CCM to/from header address fields:

These must be more fully defined. For a KDMTransmission message, it makes sense to use the facility ID for the “to” field. In general, these would be the addresses of the target entity that must process the message; they may have only local significance within the computing domain of that entity.

4 Message Structure

The body of an SMTP message shall contain exactly 1 CCM message. *[However, multiple KDMs and multiple RRM s can be carried in a CCM message].* No other text should appear in the message body.

MIME encapsulation using multipart message bodies shall not be used. *[Editor's note: this should be revisited if it is required for authentication and/or encryption].*

Messages containing binary data or text data where whitespace must be preserved shall use base64 encoding.

5 SMTP basic protocol

This section discusses which SMTP commands are required and which should not be used. It also lists certain features which provide no added value in this application and should not be used. The commands themselves are defined in [SMTP].

The following commands are required:

MAIL FROM
RCPT TO
DATA
EHLO
QUIT

The following commands shall not be used:

VERFY
EXPN

The following header lines are required:

Return-path-line
Time-stamp-line

The use of explicit routing either in source or destination addressing is prohibited. It is assumed that the global DNS system [or local DNS for communication within a particular mail domain] can be used to locate the IP address of the destination SMTP server or of another server that will relay the message to the destination.

The timeouts defined in [SMTP] shall take the values defined in that document.

6 Internet Message Format

RFC2822 [IMF] specifies the general syntax for text messages sent by SMTP and serves as a base for more complex use of the protocol. In particular, it defines a number of header fields. To simplify interoperability, this section specifies the use of these header fields for this application.

The following header fields are required in each message and shall be used as indicated below:

orig-date:	the date and time the message was created; usually the time it was passed to the originating SMTP server.
from:	this field should only contain one address; that of the entity that pass the message to the originating SMTP server.
To:	only one address, as defined in the address section above.
message-id:	this must be globally unique.
in-reply-to:	this shall contain only one message ID (separate replies must be used to refer to different SMTP messages).
subject:	a text string identifying the type of CCM message in the message body.

The following header fields are optional:

reply-to:	this field can contain a list of entities to receive RRM's.
cc:	

The following header fields require further investigation to determine whether and how they should be used in this application:

"References" field, fields dealing with message retransmission.

The use of any header fields not mentioned in this profile is prohibited.

7 Authentication and encryption.

This complex subject requires more study and must be analyzed in the context of practical use cases. There are several possible approaches, which are not per se mutually exclusive:

TLS. Use of TLS is already mandated for certain intra-theatre communications by the DCI specification. Protecting SMTP sessions with TLS is well specified in [SMTP-TLS]. However, this only provides authentication and encryption between the SMTP client and the SMTP server. This is probably sufficient for the embedded SMTP server environment, but it does not provide end-to-end security in a store and forward environment. But it would not be suitable if messages were relayed through intermediate SMTP servers.

S/MIME. This is a mechanism for authentication and optionally encryption between the message creator and the message receiver. It is defined in [S/MIME] It is suitable for store and forward environments. It can use the same X.509 certificates used elsewhere in Digital Cinema. However, I am not sure how widely deployed it is or how available open-source software is for it.

PGP. This is probably the most widely deployed security mechanism in the open Internet, and the mime message format for is defined in [PGP/MIME]. However, PGP uses a different type of certificate.

8 References

[SMTP] RFC 2821. Simple Mail Transport Protocol.

[IMF] RFC 2822. Internet Message Format.

[NATO] NATO Digital Cinema System Requirements v2.0.

[S/MIME] RFC 3851. S/MIME 3.1 Message Specification.

[SMTP-TLS] RFC 3207. SMTP Service Extension for Secure SMTP over Transport Layer Security.

[PGP/MIME] RFC 2015. MIME security with OpenPGP.