Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 5, 2016

A. Melnikov
Isode Ltd
G. Lunt
A. Ross
SMHS Ltd

October 3, 2015

Military Message Handling System (MMHS) over SMTP Profile
draft-melnikov-mmhs-profile-09

Abstract

A Military Message Handling System (MMHS) processes formal messages ensuring release, distribution, security, and timely delivery across national and international strategic and tactical networks. The MMHS Elements of Service have been defined as a set of extensions to the ITU-T X.400 (1992) international standards and are specified in STANAG 4406 Edition 2 or ACP 123.

This document specifies how a messaging service that meets these service definitions can be provided using the SMTP family of protocols. It defines a profile that can be used by those wishing to ensure that these services are provided.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

1.1. Overview

A Military Message Handling System (MMHS) processes formal messages ensuring release, distribution, security, and timely delivery across national and international strategic and tactical networks. The MMHS Elements of Service are defined as a set of extensions to the ITU-T X.400 (1992) international standards and are specified in STANAG 4406 Edition 2 or [ACP123]. This document specifies an MMHS Profile for how a comparable messaging service can be provided using Email Message Format [RFC5322], SMTP [RFC5321] and their extensions.

1.2. MMHS Profile Summary

This non-normative section provides a summary of the sections in this document that specifies the MMHS Profile; refer to the sections that follow for a normative specification of the MMHS Profile.

The fundamental purpose of STANAG 4406 Edition 2 or [ACP123] is to define a common message service to be provided between all participating organisations (or domains). STANAG 4406 Edition 2 and [ACP123] achieve this by defining the Military Messaging Elements of Service (EoS) that are required to be supported. [ACP123] defines EoS as 'abstractions that describe features of a system for which the user of that system has direct access'. Note for the purposes of this MMHS Profile a 'user' can be described as: an end user; an organisation (or domain); a Mail User Agent (MUA); a Mail Submission Agent (MSA); a Mail Transfer Agent (MTA); or, Mail Delivery Agent (MDA).

The MMHS Profile adopts the EoS defined in [ACP123].

Section 3 provides a developer-friendly summary (Section 3.2) and a detailed definition (Section 3.3, Section 3.4 and Section 3.5) that specifies:

- the mandatory and optional EoS to be supported in order to claim conformance to this MMHS Profile; and,

- the relevant IETF RFC Standard that provides the comparable EoS.

Section 4 describes generic security services independent of the mechanisms used to provide the security (Section 4.1) and profiles the use of Secure Multipurpose Internet Mail Extensions (S/MIME) protocols ([RFC5751], [RFC5652] and [RFC2634]) and DomainKeys Identified Mail (DKIM) Signatures ([RFC6376]) for implementing these security services (Section 4.2).

In order to implement an MMHS a number of components are typically deployed to support [ACP123]. The MMHS profile (defined in this document) identifies the requirements on the following SMTP MMHS components in order to claim conformance with the EoS specified in Section 3 and the security services specified in Section 4 (Note: additional SMTP extensions that provide additional SMTP functionality but do not have equivalent [ACP123] EoS are also included in these sections):

- Mail User Agent (Section 5);

- Mail Submission Agent (Section 6); and,

- o Mail Transfer Agent (Section 7);

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Elements of Service

3.1. Introduction

The military messaging elements of service are adopted from [ACP123].

Many of these elements of service are derived from the X.400 standards upon which [ACP123] is based.

Note that some of the X.400 elements of service do not have an equivalent in a SMTP messaging system. It is not the intention of this profile to define additional SMTP functionality and consequently a number of the military messaging elements of service are not supported by this profile.

Specifically, the physical delivery, conversion (implicit or explicit) and alternate recipient elements of service are not supported by this profile.

This profile adopts, where appropriate, header fields that are defined in [RFC2156] to support X.400 elements of service that support military messaging elements of service. [RFC2156] has already addressed the issue of conveying many of the X.400 elements of service within an SMTP messaging system.

3.2. Profile Support

Element of Service	ACP123 Reference	Support	SMTP Standard	Header Field or SMTP Parameter
Access Management (Section 3.3.1)	205a	MUST	[RFC4954], [RFC3207]	N/A
Content Type Indication	205b	MUST	[RFC6477], 3.2	MMHS-Extended-Au

(Section 3.3.2)				thorization-Info
Converted Indication (Section 3.3.3)	205c	N/A	N/A	N/A
Delivery Time Stamp Indication (Section 3.3.4)	205d	MUST	[RFC5322], 3.6.7	Received
MM Identification (Section 3.3.5)	205e	MUST	[RFC5322], 3.6.4	Message-ID
Message Identification (Section 3.3.6)	205f	MUST	[RFC3461], 4.4	ENVID
Non-delivery Notification (Section 3.3.7)	205g	MUST	[RFC3461], 4.1	NOTIFY=FAILURE
Original Encoded Information Types (Section 3.3.8)	205h	MAY	[RFC2156], 2.3.1.1	Original-Encoded-Information-Types
Submission Time Stamp Indication (Section 3.3.9)	205i	MUST	[RFC5322], 3.6.7	Received
Typed Body (Section 3.3.10)	205j	MUST	[RFC2045], 5	Content-Type
User/UA Capabilities Registration	205k	N/A	N/A	N/A

(Section 3.3.11)				
Alternate Recipient Allowed (Section 3.4.1)	206a	N/A	N/A	N/A
Alternate Recipient Assignment (Section 3.4.2)	206b	N/A	N/A	N/A
Authorizing Users Indication (Section 3.4.3)	206c	MUST	[I-D.melnikov-mmhs-authorizing-users]	MMHS-Authorizing-Users
Auto-forwarded Indication (Section 3.4.4)	206d	MAY	[RFC2156], 2.3.1.2	Autoforwarded
Blind Copy Recipient Indication (Section 3.4.5)	206e	MUST	[RFC5322], 3.6.3	Bcc
Body Part Encryption Indication (Section 3.4.6)	206f	N/A	N/A	N/A
Conversion Prohibited (Section 3.4.7)	206g	MAY	[RFC2156], 5.3.6	Conversion
Conversion Prohibition in Case of Loss of Information (Section	206h	MAY	[RFC2156], 5.3.6	Conversion-With-Loss

3.4.8)				
Cross Referencing Indication (Section 3.4.9)	206i	MAY	[RFC5322], 3.6.4	References
Deferred Delivery (Section 3.4.10)	206j	MAY	[RFC4865], 3.6.4	HOLDUNTIL
Deferred Delivery Cancellation (Section 3.4.11)	206k	N/A	N/A	N/A
Delivery Notification (Section 3.4.12)	206l	MUST	[RFC3461], 4.1	NOTIFY=SUCCESS
Designation of Recipient by Directory Name (Section 3.4.13)	206m	N/A	N/A	N/A
Disclosure of Other Recipients (Section 3.4.14)	206n	N/A	N/A	N/A
DL Expansion History Indication (Section 3.4.15)	206o	N/A	N/A	N/A
DL Expansion Prohibited (Section 3.4.16)	206p	N/A	N/A	N/A
Expiry Date	206q	MUST	[RFC2156], 2.3.1.2	Expires

Indication (Section 3.4.17)				
Explicit Conversion (Section 3.4.18)	206r	N/A	N/A	N/A
Forwarded MM Indication (Section 3.4.19)	206s	MUST	[RFC2046], 5.2	Content-Type: message/rfc822
Grade of Delivery Selection (Section 3.4.20)	206t	MUST	[RFC6758]	MT-Priority
Hold for Delivery (Section 3.4.21)	206u	N/A	N/A	N/A
Incomplete Copy Indication (Section 3.4.22)	206v	MAY	[RFC2156], 2.3.1.2	Incomplete-Copy
Language Indication (Section 3.4.23)	206w	MAY	[RFC3282], 2	Content-Language
Latest Delivery Designation (Section 3.4.24)	206x	MUST	[RFC2852], 4	BY
Multi-destination Delivery (Section 3.4.25)	206y	MUST	[RFC5321], 2.1	RCPT TO

Multi-part Body (Section 3.4.26)	206z	MUST	[RFC2046], 25.1.3	Content-Type: multipart/mixed
Non-receipt Notification Request Indication (Section 3.4.27)	206aa	MUST	[RFC3798], 2.1	Disposition-Notification-To
Obsoleting Indication (Section 3.4.28)	206ab	MAY	[RFC2156], 2.3.1.2	Supersedes
Originator Indication (Section 3.4.29)	206ac	MUST	[RFC5322], 3.6.2	Sender
Originator Requested Alternate Recipient (Section 3.4.30)	206ad	N/A	N/A	N/A
Prevent of Non-delivery Notification (Section 3.4.31)	206ae	MAY	[RFC3461], 4.1	NOTIFY=NEVER
Primary and Copy Recipients Indication (Section 3.4.32)	206af	MAY	[RFC5322], 3.6.3	To, Cc
Receipt Notification Request Indication (Section 3.4.33)	206ag	MUST	[RFC3798], 2.1	Disposition-Notification-To

Redirection Disallowed By Originator (Section 3.4.34)	206ah	N/A	N/A	N/A
Redirection of Incoming Messages (Section 3.4.35)	206ai	N/A	[RFC5228], 4.2? Maybe?	N/A
Reply Request Indication (Section 3.4.36)	206ab	N/A	[RFC5322] - no requesting mechanism	N/A
Replying MM Indication (Section 3.4.37)	206ak	MUST	[RFC2156], 3.6.4	In-Reply-To
Requested Preferred Delivery Method (Section 3.4.38)	206al	N/A	N/A	N/A
Subject Indication (Section 3.4.39)	206am	MAY	[RFC2156], 3.6.5	Subject
Use of Distribution List (Section 3.4.40)	206an	N/A	N/A	N/A
Primary Precedence (Section 3.5.1)	212a	MUST	[RFC6477], 3.8	MMHS-Primary-Precedence
Copy Precedence (Section 3.5.2)	212b	MUST	[RFC6477], 3.9	MMHS-Copy-Precedence

Message Type (Section 3.5.3)	212c	MUST	[RFC6477], 3.10	MMHS-Message-Type
Exempted Addresses (Section 3.5.4)	212d	MAY	[RFC6477], 3.1	MMHS-Exempted-Address
Extended Authorization Info (Section 3.5.5)	212e	MAY	[RFC6477], 3.2	MMHS-Extended-Authorisation-Info
Distribution Code (Section 3.5.6)	212f	MAY	[RFC6477], 3.3	MMHS-Subject-Indicator-Codes
Message Instructions (Section 3.5.7)	212g	MAY	[RFC6477], 3.5	MMHS-Message-Instructions
Clear Service (Section 3.5.8)	212h	MAY	[RFC2634], 3 and [RFC7444]	eSSSecurityLabel, SIO-Label
Other Recipient Indicator (Section 3.5.9)	212i	MAY	[RFC6477], 3.11 3.12	MMHS-Other-Recipient-Indicator-To, MMHS-Other-Recipients-Indicator-CC
Originator Reference (Section 3.5.10)	212j	MAY	[RFC6477], 3.7	MMHS-Originator-Reference
Use of Address List (Section 3.5.11)	212k	N/A	N/A	N/A
Handling	213a	MAY	[RFC6477], 3.4	MMHS-

Instructions (Section 3.6.1)				Handling-Instructions
Pilot Forwarded (Section 3.6.2)	213b	N/A	N/A	N/A
Corrections (Section 3.6.3)	213c	N/A	N/A	N/A
ACP 127 Message Identifier (Section 3.6.4)	213d	MAY	[RFC6477], 3.13	MMHS-Acp127-Message-Identifier
Originator PLAD (Section 3.6.5)	213e	MAY	[RFC6477], 3.14	MMHS-Originator-PLAD
Codress Message Indicator (Section 3.6.6)	213f	MAY	[RFC6477], 3.6	MMHS-Codress-Message-Indicator
ACP 127 Notification Request (Section 3.6.7)	213g	N/A	N/A	N/A
ACP 127 Notification Response (Section 3.6.8)	213h	N/A	N/A	N/A
Access Control (Section 4.1.1)	Annex B, 7.1	MAY	TBD	TBD
Authentication of Origin (Section	Annex B, 7.2	MAY	[RFC5652], 5	SignedData

4.1.2)				
Non-repudiation of Origin (Section 4.1.3)	Annex B, 7.3	MAY	[RFC5652], 5	SignedData
Message Integrity (Section 4.1.4)	Annex B, 7.4	MUST	[RFC5652], 5	SignedData
Message Data Separation (Section 4.1.5)	Annex B, 7.5	MAY	[RFC5652], 6	EnvelopedData
Security Labels (Section 4.1.6)	Annex B, 7.6	MUST	[RFC2634], 3 and [RFC7444]	ESSSecurityLabel, SIO-Label
Non-repudiation of Receipt (Section 4.1.7)	Annex B, 7.7	MAY	[RFC2634], 2	ReceiptRequest
Secure Mailing Lists (Section 4.1.8)	Annex B, 7.8	MAY	[RFC2634], 4	MLExpansionHistory
Message Counter Signature (Section 4.1.9)	Annex B, 7.9	MAY	[RFC5652], 11.4	counterSignature
Certificate Binding (Section 4.1.10)	Annex B, 7.10	MAY	[RFC2634],	SigningCertificate
Compressed Data (Section 4.1.11)	Annex B, 7.11	MAY	[RFC3274]	CompressedData

3.3. Basic Elements of Service

3.3.1. Access Management

This element of service enables an Mail User Agent and an Mail Transfer Agent to establish access and manage information associated with access establishment. This includes the ability to identify and validate the identity of the other.

Strong authentication in the bind operation is mandatory. Strong authentication MUST be supported using SMTP Extension for Authentication [RFC4954] and SMTP Extension for Secure SMTP over TLS [RFC3207].

While the list of recommended authentication mechanisms used with SMTP Extension for Authentication would depend on operating environment and would change over time, some recommendations are provided here. For environment using X.509 certificates, use of SASL EXTERNAL [RFC4422] authentication mechanism is RECOMMENDED. For environment using Kerberos, use of SASL GSSAPI [RFC4752] authentication mechanism is RECOMMENDED. Support for SCRAM [RFC5802] is RECOMMENDED for environment using password based authentication.

3.3.2. Content Type Indication

This element of service enables an originating Mail User Agent to indicate the type of each submitted message. In most cases, the content type can be determined from the header fields that are present.

A Military Message MUST be indicated using the MMHS-Extended-Authorization-Info header field defined in [RFC6477].

Note that the Content Type Indication element of service is not supported by the MIME Content-Type header field defined in [RFC2045], even though they have a similar name. The MIME Content-Type header field is to describe only the data contained in the body of the message, and not the whole message itself.

3.3.3. Converted Indication

This element of service indicates to each recipient UA (i.e., on per-recipient basis) that the performed conversion on the Encoded Information Types (EITs) within a delivered message.

Security requirements and mechanisms may not allow conversion to take place within the MMHS.

However, messages entering the MMHS from a gateway (e.g., a civilian X.400 domain, an ACP 127 tactical gateway) may carry the converted indication.

The Converted Indication, if present, MUST use the X400-Received header field as defined in [RFC2156].

3.3.4. Delivery Time Stamp Indication

This element of service indicates to each recipient Mail User Agent (i.e., on a per-recipient basis), the date and time at which the Mail Transfer Agent delivered a message.

The delivery time stamp MUST be determined from the first Received header field, defined in [RFC5322], present in the message.

3.3.5. MM Identification

This element of service enables cooperating Mail User Agents to convey a globally unique identifier for each Military Message sent or received. This identifier is used in subsequent messages to identify the original Military Message.

A Military Message MUST be uniquely identified using the Message-ID header field defined in [RFC5322].

3.3.6. Message Identification

This element of service is used by Mail User Agents and the Mail Transfer Agents to refer to a previously submitted message in connection with other elements of service such as delivery and non-delivery notification.

Message Identification MUST be specified by the Mail User Agent using the ENVID parameter, as defined in [RFC3461]. The Mail Transfer Agent MUST return the message identification in the Original-Envelope-Id field of a message/delivery status as defined in [RFC3461].

3.3.7. Non-delivery Notification

This element of service allows a Mail User Agent to ask for the MTS to notify the originator if a submitted message was not delivered to the specified recipient Mail User Agent. The MMHS must, with a high degree of certainty, deliver a message to the intended recipient(s). If the system cannot deliver a message within a determined period of time , a non-delivery report will be returned to the originating Mail User Agent by the MMHS. The non-delivery report contains information

to enable it to be mapped to the appropriate message (i.e., the message identification), recipient information, as well as information about why the message could not be delivered.

Non-Delivery notifications MUST be generated in accordance with [RFC3461].

3.3.8. Original Encoded Information Types

This element of service enables the originating Mail User Agent to indicate the various formats of the bodyparts of a message.

The Original Encoded Information Types, if present, MUST use the Original-Encoded-Information-Types header field as defined in [RFC2156].

3.3.9. Submission Time Stamp Indication

This element of service enables the Message Transfer Agent to indicate to the originating Mail User Agent and each recipient Mail User Agent the date and time at which is which was submitted to the Message Transfer Agent.

The Submission Time Stamp Indication MUST be determined from the last Received header field, as defined in [RFC5322], present in the message. Note that this is distinct from the Date header field, defined in [RFC5322], which is more likely to be displayed by a receiving Mail User Agent but which indicates the date and time at which the originator of the message indicated that the message was complete and ready to submitted.

3.3.10. Typed Body

This element of service allows the nature and attributes of the body of the message to be conveyed along with the body.

The MMHS MUST support this element of service whereby:

- A Mail User Agent MUST support Multipurpose Internet Mail Extensions (MIME) [RFC2045], [RFC2046], [RFC2047], [RFC2049], [RFC2231] and [RFC3676]; and,

- A Mail Submission Agent MUST support SMTP Extension for 8-bit MIME transport [RFC6152].

3.3.11. User/UA Capabilities Registration

This element of service enables a MUA to indicate to the MMHS unrestricted use of any or all of the following capabilities with respect to received messages:

- the content type(s) of messages it is willing to accept;

- the maximum content length of a message it is willing to accept; and

- the Encoded Information Type(s) of messages it is willing to accept.

There is no current SMTP service that supports this element of service. Therefore this profile does not support this element of service.

However, this element of service MAY be supported by MUAs and other MMHS components that provide proprietary mechanisms (i.e Directory Services).

3.4. Optional Elements of Service

3.4.1. Alternate Recipient Allowed

This element of service enables an originating Mail User Agent to specify that the message being submiited can be redirected to an alternate recipient. Unless an originator specifically request that an alternate recipient be disallowed, all Military Messages will indicate that an alternate recipient is allowed.

There is no current SMTP service that supports allows the originator to disallow the redirection of a message to an alternate recipient. Therefore this profile does not support the Alternate Recipient Allowed element of service.

3.4.2. Alternate Recipient Assignment

This element of service enables a receiving Mail User Agent to be given the capability to have certain messages delivered to it for which there is not an exact match between the recipient address specified in the message and the valid addresses within the recipient domain. This service allows a message that would otherwise be undeliverable to be delivered to a "default mailbox" within the recipient domain.

There is no current SMTP service that supports allows the Alternate Recipient Assignment element of service. Therefore this profile does not support the Alternate Recipient Assignment element of service. Note that some Mail Transfer Agent products may provide propriertary mechanisms that support the element of service.

3.4.3. Authorizing Users Indication

This element of service allows the originator to indicate to the recipient the names or one or more persons who authorized the sending of the messages.

The Authorizing Users Indication element of service MUST be conformant with the Draft and Release using Internet Email specification [I-D.melnikov-mmhs-authorizing-users]. In addition, the Sender header field as defined in [RFC5322] (carrying the Originator Indication) MUST also be present in accordance with [RFC2156].

3.4.4. Auto-forwarded Indication

This element of service allows a recipient to determine that the body of an incoming Military Message contains a Military Message that has been auto-forwarded by an autonomous Mail Submission Agent. This is used to distinguish the incoming Military Message that contains a Military Message that was manually forwarded by the original recipient. If automatic forwarding of Military Messages is supported by a Mail Submission Agent, then the Auto-forwarded Indication MUST be supported on origination.

The Auto-forwarded Indication MUST use the Autoforwarded header field, as defined in [RFC2156].

3.4.5. Blind Copy Recipient Indication

This element of service enable the originator to provide the address of one or more additional intended recipients of the message being sent. These names are not disclosed to the primary, copy or other blind copy recipients. This service can be used to keep some recipient names and addressed hidden from other recipients. This service can be used to send a courtesy copy to drafters or reviewers of a message, when internal information, such as who drafted or reviewed the message, is not to be disclosed to the recipient(s). Separate copies of the mesage MUST be submitted to the Mail Transfer Agent for the open recipients (primary and copy recipients) and for each blind copy recipient. The messages sent to each of blind copy recipients MUST contain same MM Identification as the message sent to the open recipients.

The Blind Copy Recipient Indication MUST use the Bcc header field, as defined in [RFC5322].

3.4.6. Body Part Encryption Indication

This element of service allows the originator to indicate to the recipient that a particular body of the message has been sent encrypted.

There is no current SMTP service that supports allows the Body Part Encryption Indication element of service. Therefore this profile does not support the Body Part Encryption Indication element of service.

3.4.7. Conversion Prohibited

This element of service enables an originating Mail User Agent to instruct the Mail Transfer Agent that the implicit conversion of the military message should not be performed.

This element of service is not supported by an SMTP Mail Transfer Agent. A Mail User Agent MAY use the Conversion header field, as defined in [RFC2156] to control the conversion to an X.400 message at a MIXER gateway and further within the X.400 domain at X.400 Mail Transfer Agents.

3.4.8. Conversion Prohibition in Case of Loss of Information

This element of service enables and originating Mail User Agent to instruct the Mail Transfer Agent that the implicit conversion of the military message should not be performed, if such conversion would result in the loss of information.

This element of service is not supported by an SMTP Mail Transfer Agent. A Mail User Agent MAY use the Conversion-With-Loss header field, as defined in [RFC2156] to control the conversion to an X.400 message at a MIXER gateway and further within the X.400 domain at X.400 Mail Transfer Agents.

3.4.9. Cross Referencing Indication

This element of service allows the originator to associate the globally unique identifiers of one or more other messages with the message being sent. This enables the recipient's Mail User Agent, for example, to retrieve a copy of the referenced messages.

The Cross Referencing Indication MUST use the References header field, as defined in [RFC5322].

3.4.10. Deferred Delivery

This element of service enables an originating Mail User Agent to instruct the Mail Transfer Agent that a military message being submitted shall be delivered no sooner than a specified date and time. When this service is requested, it MUST be logged for audit and tracing purposes.

Deferred Delivery MUST be specified in accordance with [RFC4865].

3.4.11. Deferred Delivery Cancellation

This element of service enables an orginating MUA to instruct the MTA to cancel a previously submitted military message that contained a Deferred Delivery date and time.

Deferred Delivery Cancellation is not supported by this profile.

3.4.12. Delivery Notification

This element of service enables the originating MUA to request that the originating MUA be explicitly notified when a submitted military message has been successfully delivered to a recipient MUA. This notification is conveyed by a delivery report. The delivery report is related to the submitted message by means of a message identifier and includes the date and time of delivery. Receipt of a delivery report at the originating MUA results in the the generation of a delivery notification to the originator. In the case of multi-destination military messages, this service shall be selectable on a per recipient basis.

This element of service MUST be supported using the NOTIFY parameter of the ESMTP RCPT command with as value of SUCCESS, as defined in [RFC3461].

Note that while this element of service is selectable on a per recipient basis, an MUA MAY only allow it to be selected on a per message basis.

3.4.13. Designation of Recipient by Directory Name

This element of service enables an originating UA to use, on a per-recipient basis, a directory name in place of an individual recipient's address. This implies the support of a directory service. The directory name must be translated to an email address for delivery to take place. However, the directory lookup may take place at the MTA rather than at the MUA.

Designation of Recipient by Directory Name is not suppoted by this profile.

However the designation of a recipient by a directory name MAY be supported by a MUA that can retrieve an address from a directory service.

3.4.14. Disclosure of Other Recipients

This element of service enables the originating MTA to instruct the MTS to disclose the address of all other recipient of a multi-recipient military message to each recipient MUA, upon delivery of the message. The addresses disclosed are as supplied by the originating MUA or the results of address list expansion.

Disclosure of Other Recipients is not supported by this profile.

3.4.15. DL Expansion History Indication

This element of service provides information to a recipient about the DL(s) that resulted in the message being delivered to this recipient. This element of service also provides a mechanism to protect against potential nested DL looping.

DL Expansion History Indication is not supported by this profile.

The DL-Expansion-History header defined in [RFC2156] SHALL NOT be used. DL-Expansion-History header MAY be present in messages gatewayed from X.400.

3.4.16. DL Expansion Prohibited

This element of service allows an originating user to specify that if any of the recipient names can directly, or by reassignment, refer to a distribution, then no expansion of the distribution shall occur. Instead, a non-delivery notification shall be returned to the originating Mail User Agent.

DL Expansion Prohibited is not supported by this profile.

3.4.17. Expiry Date Indication

This element of service allows the originator to indicate to the recipient the date and time after which the message is considered invalid. The intent of this element of service is to state the originator's assessment of the current applicability of a message. If the Expiry Date Indication is present, it shall be displayed to the recipients(s) to indicate the time after which this message

should be longer be acted upon. It is left to the discretion of the recipient as to whether or not the message is discarded.

The Expiry Date Indication element of service SHALL use the Expires header field, as defined in [RFC2156].

3.4.18. Explicit Conversion

This element of service enables an originating MUA to request, on a per-recipient basis, that the MTA perform a specified Encoded Information Type conversion.

Explicit Conversion is not supported by this profile.

3.4.19. Forwarded MM Indication

This element of service allows a message, plus its delivery information to be sent as a body part inside another message. In a multi-part body the forwarded message may be one of serveral body parts of various types.

The Forwarded MM Indication element of service, if supported by the MMHS, SHALL use the Content-Type header field, as defined in [RFC2045] with the value "message/rfc822" and use the Content Type Indication , as defined in Section 3.3.2, within the headers of the embedded message.

Note that the Content-Type header field may be embedded within an outer "multipart/mixed" MIME body where, for example, the fowarding Military Message also includes delivery information, covering text or additional attachments.

3.4.20. Grade of Delivery Selection

This element of service enables an originating MUA to request that transfer through the MMHS take place at a selected priority. The time periods defined for each grade of delivery must be specified in an organisation (or domain) policy and bilaterally agreed between participating organisations (or domains).

The Grade of Delivery Selection element of service MUST be supported by the MMHS, using the MT-Priority header field, as defined in [RFC6758].

The Grade of Delivery Selection MT-Priority header field value MUST be derived from the Primary Precedence (Section 3.5.1) MMHS-Primary-Precedence [RFC6477] header field value.

The MMHS message may have no primary recipients (therefore no Primary Precedence); the Grade of Delivery Selection MT-Priority header field value MUST be derived from the Copy Precedence (Section 3.5.2) MMHS-Copy-Precedence [RFC6477] header field value.

The mapping between the Grade of Delivery Selection MT-Priority header field values and the Primary Precedence MMHS-Primary-Precedence header field values (and subsequently the Copy Precedence MMHS-Copy-Precedence header field values) MUST support the "STANAG4406" Priority Assignment Policy specified in [RFC6758] Appendix A.

The Grade of Delivery Selection MT-Priority doesn't have to be displayed to the recipient by the MUA, as an indication of the Grade of Delivery selection element of service is provided to the recipient MUA by the Primary and Copy Precedence.

3.4.21. Hold for Delivery

This element of service enables a recipient MUA to request that the MTA hold its MMHS messages and returning notifications for delivery until a later time. The MUA can indicate to the MTA when it is unavailable to take delivery of messages and notifications, and also, when it is again ready to accept delivery of messages and notifications from the MTA. The MTA can indicate to the MUA that messages are waiting due to the criteria the MUA established for holding messages. The MMHS message will be held until the maximum delivery time for that MMHS message expires, unless the recipient releases the hold prior to its expiry.

There is no current SMTP service that supports the Hold for Delivery element of service. Therefore this profile does not support this element of service.

However, this element of service MAY be partially supported by MTA products that provide proprietary mechanisms to schedule delivery times based on MMHS message size and MMHS message priority.

3.4.22. Incomplete Copy Indication

This element of service allows an originator to indicate that this MMHS message is an incomplete copy of a MMHS message with the same Message-ID header field in that one or more body parts or header fields of the original MMHS message are absent.

The Incomplete Copy Indication element of service MAY be supported by the MMHS, using the Incomplete-Copy header field, as defined in [RFC2156].

3.4.23. Language Indication

This element of service enables an originating MUA to indicate the language type(s) of a submitted message.

The Language Indication element of service MAY be supported by the MMHS, using the Content-Language header field, as defined in [RFC3282].

3.4.24. Latest Delivery Designation

This element of service enables an originating MUA to specify the latest time by which the MMHS message is to be delivered. If the MTA cannot deliver by the time specified, the MMHS message is canceled and a non-delivery report returned to the originating MUA.

The Latest Delivery Designation element of service MUST be supported by the MMHS as defined in the Deliver By SMTP extension [RFC2852].

3.4.25. Multi-destination Delivery

This element of service allows an originating MUA to specify that a message being submitted is to be delivered to more than one recipient MUA. This does not imply simultaneous delivery to all specified recipient MUAs.

The Multi-destination Delivery element of service is supported by the SMTP RCPT command as defined in [RFC5321].

3.4.26. Multi-part Body

This element of service allows an originator to send a message that is partitioned into several parts. The nature and attributes, or type, of each body part are conveyed along with the body part. This enables the multiple parts to be of different encoded information types.

The MMHS MUST support this element of service whereby:

o A Mail User Agent MUST support Multipurpose Internet Mail Extensions (MIME) [RFC2045], [RFC2046], [RFC2047], [RFC2049] and [RFC2231]; and,

o A Mail Submission Agent MUST support SMTP Extension for 8-bit MIME transport [RFC6152].

3.4.27. Non-receipt Notification Request Indication

This element of service allows the originator to ask, on a per-recipient basis, for notification if the MMHS message is deemed unreceivable by any of the recipients.

The Non-Receipt Notification Request Indication MUST be supported by the MMHS, using the Disposition-Notification-To header field as defined in [RFC3798].

In the case where the Non-Receipt Notification Request Indication element of service is required for a subset of the recipients the MSA MUST: submit a MMHS message to those recipients that a non-receipt notification is requested with a Disposition-Notification-To header field; and, submit a MMHS message(s) to those recipients that a non-receipt notification is not requested without a Disposition-Notification-To header field.

Note that while this element of service is selectable on a per recipient basis, an MUA MAY only allow it to be selected on a per message basis.

Note that this element of service will be supported in conjunction with the Receipt Notification Request Indication as profiled in Section 3.4.33.

3.4.28. Obsoleting Indication

This element of service allows the originator to indicate to the recipient that one or more previously sent MMHS messages are obsolete. The intention of this element of service is for the MUA to display to the user reading the original MMHS message that the original MMHS message is obsolete. It is the responsibility of the user for discarding the original MMHS message.

The Obsoleting Indication element of service MAY be supported by the MMHS, using the Supersedes header field, as defined in [RFC2156].

3.4.29. Originator Indication

The Originator Indication MUST use the MMHS-Authorizing-Users header field, as defined in [I-D.melnikov-mmhs-authorizing-users], when the Authorizing Users Indication is present in the message and the Sender header field, as defined in [RFC5322], when the Authorizing Users Indication is not present in the message.

This conditional use of different header fields is required to support interoperability with [ACP123] and [STANAG-4406] X.400 systems that utilise a MIXER compliant gateway, [RFC2156].

3.4.30. Originator Requested Alternate Recipient

This element of service enables the originating MUA to specify, for each intended recipient, one alternate recipient to whom the MTA can deliver the message, if delivery to the intended recipient is not possible. This service allows a MMHS message that would otherwise be delayed or non-delivered to be delivered to an alternative message recipient.

There is no current SMTP service that supports the Originator Requested Alternate Recipient element of service. Therefore this profile does not support this element of service. Note that some MTAs may provide propriertary mechanisms that support this element of service.

3.4.31. Prevention of Non-delivery Notification

This element of service enables an originating MUA to instruct a MTA not to return a non-delivery report to the originating MUA in the event that the message being submitted is judged undeliverable.

This element of service MUST be supported by the MMHS, using the NOTIFY parameter of the ESMTP RCPT command with as value of NEVER, as defined in [RFC3461].

Note that while this element of service is selectable on a per recipient basis, an MUA MAY only allow it to be selected on a per message basis.

3.4.32. Primary and Copy Recipients Indication

Primary and Copy recipients, within the MMHS, are known as action and information addressees, respectively. A primary recipient has a responsibility to act upon a delivered MMHS message, whereas a Copy recipient has been sent the MMHS message for information purposes only.

The Primary and Copy Recipients Indication element of service MUST be supported by the MMHS, using the To and Cc header fields, respectively, as defined in [RFC5322].

3.4.33. Receipt Notification Request Indication

This element of service allows the originator of a MMHS message to request, on a per-recipient basis, for notification when a particular MMHS message is received. The recipient MUA MUST prominently display the request for this element of service and permit the recipient to honour the request or reject the request.

The Receipt Notification Request Indication MUST be supported by the MMHS, using the Disposition-Notification-To header field as defined in [RFC3798].

In the case where the Receipt Notification Request Indication element of service is required for a subset of the recipients the MUA MUST: submit a MMHS message to those recipients that a receipt notification is requested with a Disposition-Notification-To header field; and, submit a MMHS message(s) to those recipients that a receipt notification is not requested without a Disposition-Notification-To header field.

Note that while this element of service is selectable on a per recipient basis, an MUA MAY only allow it to be selected on a per message basis.

Note that this element of service will be supported in conjunction with the Receipt Notification Request Indication as profiled in Section 3.4.27.

In the case where the MMHS supports S/MIME security services profiled in Section 4 the originating MUA MAY use the Non-repudiation of Receipt element of service as specified in Section 4.1.7.

3.4.34. Redirection Disallowed by Originator

This element of service enables an originating MUA to instruct the MTA that redirection should not be applied to a particular submitted MMHS message.

There is currently no SMTP service that supports this element of service. Therefore, the Redirection Disallowed by Originator element of service is not supported by this profile.

3.4.35. Redirection of Incoming Messages

This element of service enables a MUA to instruct the MTA to redirect incoming MMHS messages addressed to it, to another MUA or to an Address List (AL), for a specified period of time, or until revoked.

There is currently no SMTP service that supports this element of service. Therefore the Redirection of Incoming Messages element of service is not supported by this profile. However, note that some MTA and/or MDA products are able to enforce a local security policy supporting this element of service with proprietary mechanisms.

3.4.36. Reply Request Indication

This element of service allows the originator to request, on a per-recipient basis, that a recipient send a message in reply to the MMHS message that carries the request. The originator can also optionally specify the date by which any reply should be sent and the names of one or more users and ALs who the originator requests be included among the preferred recipients of any reply.

The Reply Request Indication element of service is not supported by this profile.

This element of service MAY be procedurally defined by a MMHS. Hence the Reply Request Indication MAY be supported by including the request within the body of the MMHS message.

Blind Copy recipients of the MMHS message, that includes support for this element of service within the message body, SHOULD be careful to consider the recipients of the reply MMHS message honoring the Blind Copy Recipient Indication element of service profiled in Section 3.4.5.

3.4.37. Replying MM Indication

This element of service allows the originator of a MMHS message to indicate to the recipients that the message is being sent in reply to another MMHS message.

The Replying MM Indication element of service MAY be supported by the MMHS, using the In-Reply-To header field as defined in [RFC5322].

3.4.38. Requested Preferred Delivery Method

This element of service allows an originator to request, on a per-recipient basis, the preference of method or methods of delivery.

Requested Preferred Delivery Method is not supported by this profile.

3.4.39. Subject Indication

This element of service allows the originator to indicate to the recipient(s) a user specified short description of the message.

The Subject Indication element of service MAY be supported by the MMHS, using the Subject header field as defined in [RFC5322].

3.4.40. Use of Distribution List

This element of service enables an origintaing MUA to specify, on a per-recipient basis, a Distribution List in place of all the individual recipients (users or nested DLs). The MTA will add the member of the list to the recipients and send it to those members. Support for this service shall be optional. Determination of where in the MMHS the DL expansion takes place may be the subject of national policy based upon security requirements. National policy may also dictate the preferential support of the Use of Address List (Section 3.5.11) and Exempted Addsresses (Section 3.5.4)Elements of Service instead of the Use of Distribution List Element of Service.

Use of Distribution List is not supported by this profile.

3.5. Military Elements of Service

This section profiles the MMHS Header Fields for use in the MMHS as specified in [RFC6477].

3.5.1. Primary Precedence

The MMHS-Primary-Precedence header field defined in [RFC6477] MUST be supported and included by the MMHS if the military message contains "To:" ("action") addresses.

3.5.2. Copy Precedence

The MMHS-Copy-Precedence header field defined in [RFC6477] MUST be supported and included by the MMHS if the military message contains "Cc:" or "Bcc:" ("information") addresses.

3.5.3. Message Type

The MMHS-Message-Type header field defined in [RFC6477] MUST be supported by the MMHS.

3.5.4. Exempted Addresses

The MMHS-Exempted-Address header field defined in [RFC6477] MAY be supported by the MMHS.

3.5.5. Extended Authorization Info

The MMHS-Extended-Authorisation-Info header field defined in [RFC6477] MUST be supported and included by the MMHS in a military message.

3.5.6. Distribution Code

The MMHS-Subject-Indicator-Codes header field defined in [RFC6477] MUST be supported by the MMHS.

3.5.7. Message Instructions

The MMHS-Message-Instructions header field defined in [RFC6477] MAY be supported by the MMHS.

3.5.8. Clear Service

This element of service indicates to the recipient that the military message containing classified information has been transmitted over non-secure communications links. This element of service, if permitted by the security policy, MAY be supported by using the printable string "CLEAR" in the privacy mark component of the security label (see Section 4.1.6) along with an appropriate security policy identifier. If this element of service is supported by the MMHS, the MUA MUST prominently display to the user that the military message has been transmitted over non-secure communication links.

3.5.9. Other Recipient Indicator

The MMHS-Other-Recipients-Indicator-To and MMHS-Other-Recipients-Indicator-CC header fields defined in [RFC6477] MAY be supported by the MMHS.

3.5.10. Originator Reference

The MMHS-Originator-Reference header field defined in [RFC6477] MAY be supported by the MMHS.

3.5.11. Use of Address List

The Address List Indication element of service is not supported by this profile.

3.6. Transition Elements of Service

3.6.1. Handling Instructions

The MMHS-Handling-Instructions header field defined in [RFC6477] MAY be supported by the MMHS only to support interoperability with ACP 127 systems.

3.6.2. Pilot Forwarded

The Pilot Forwarded element of service is not supported by this profile.

3.6.3. Corrections

The Corrections element of service is not supported by this profile.

3.6.4. ACP 127 Message Identifier

The MMHS-Acp127-Message-Identifier header field defined in [RFC6477] MAY be supported by the MMHS only to support interoperability with ACP 127 systems.

3.6.5. Originator PLAD

The MMHS-Originator-PLAD header field defined in [RFC6477] MAY be supported by the MMHS only to support interoperability with ACP 127 systems.

3.6.6. Codress Message Indicator

The MMHS-Codress-Message-Indicator header field defined in [RFC6477] MAY be supported by the MMHS only to support interoperability with ACP 127 systems.

3.6.7. ACP 127 Notification Request

The ACP 127 Notification Request element of service is not supported by this profile.

3.6.8. ACP 127 Notification Response

The ACP 127 Notification Response element of service is not supported by this profile.

4. Security Services

An MMHS MAY support security services. The security services specified in this profile are based on the Secure Multipurpose Internet Mail Extensions (S/MIME) protocols and DomainKeys Identified Mail (DKIM) Signatures specified in [RFC6376]. The S/MIME protocols Message Specification [RFC5751], Cryptographic Message Syntax [RFC5652] and Enhanced Security Services for S/MIME [RFC2634] specify a consistent way to securely send and receive MIME messages providing end to end integrity, authentication, non-repudiation and confidentiality. DKIM's primary purpose is to define an organization-level digital signature authentication framework for Internet email, using public key cryptography and using the domain name service as its key server technology. However, it is possible to administer DKIM to support user-level signature granularity. This section describes the generic security services and profiles the use of [RFC5751], [RFC5652], [RFC2634] and [RFC6376].

4.1. General Security Elements of Service

The general security services and implementation requirements for providing these security services for an MMHS are detailed below.

4.1.1. Access Control

The Access Control security service provides a means of enforcing the authorization of users to originate and receive messages. Access controls are performed in each MMHS domain in accordance with the security policy in force. MMHS systems MAY enforce their own native security policies, plus any other security policies that have been bilaterally agreed.

An MMHS providing the access control service MUST perform access control decisions based on comparing the sensitivity information conveyed in a security label (Section 4.1.6) with a user's authorizations.

4.1.2. Authentication of Origin

The Authentication of Origin security service provides assurance that the message was originated by the user indicated as the sender by digitally signing the message. However, it must be noted that the implementation of the MMHS security services is dependent upon the

security and assurance requirements that are to be met by those MMHS security services. As such, the identity of the signer of the MMHS message may be the user, the role the user is performing or the organization (or domain) the user belongs to.

If the MMHS provides security services it MUST support the Authentication of Origin service.

The MMHS SHOULD implement this service on origination supporting the SignedData content type (profiled in Section 4.2.1.2) to apply a digital signature to a MMHS message or, in a degenerate case where there is no signature information, to convey certificates.

Alternatively the MMHS MAY implement this service on origination supporting DKIM (profiled in Section 4.2.4) to apply a digital signature to a MMHS message.

On reception the MMHS MUST support verification of S/MIME and DKIM digital signatures.

4.1.3. Non-repudiation of Origin

The Non-repudiation of Origin security service provides the recipient with evidence that demonstrates, to a third-party, who originated the message, and will protect against any attempt by the message originator to falsely deny having sent the message. However, it must be noted that the implementation of the MMHS security services is dependent upon the security and assurance requirements that are to be met by those MMHS security services. As such, the identity of the signer of the MMHS message may be the user, the role the user is performing or the organization (or domain) the user belongs to.

If the MMHS provides security services it MUST support the Non-repudiation of Origin service.

The MMHS SHOULD implement this service on origination as profiled in Section 4.2.1.2.

Alternatively the MMHS MAY implement this service on origination supporting DKIM (profiled in Section 4.2.4) to apply a digital signature to a MMHS message.

On reception the MMHS MUST support verification of S/MIME and DKIM digital signatures.

4.1.4. Message Integrity

The Message Integrity security service provides a method of ensuring the content that was received by the recipient(s) is the same as that which was sent by the originator. However, it must be noted that the implementation of the MMHS security services is dependent upon the security and assurance requirements that are to be met by those MMHS security services. As such, the identity of the signer of the MMHS message may be the user, the role the user is performing or the organization (or domain) the user belongs to.

If the MMHS provides security services it MUST support the Message Integrity service.

The MMHS SHOULD implement this service on origination as profiled in Section 4.2.1.2.

Alternatively the MMHS MAY implement this service on origination supporting DKIM (profiled in Section 4.2.4) to apply a digital signature to a MMHS message.

On reception the MMHS MUST support verification of S/MIME and DKIM digital signatures.

4.1.5. Message Data Separation

The Message Data Separation security service protects against unauthorized disclosure of the message, and separates data contained in one message from that contained in another message. This service can help to enforce need to know restrictions, or enables multiple different user communities to share the same secure network. The service is independent of the network and systems transporting the message.

The MMHS MAY implement this service supporting the EnvelopedData content type (profiled in Section 4.2.1.3) to apply privacy protection to a message. A sender needs to have access to a public key for each intended message recipient to use this service. This content type does not provide authentication.

4.1.6. Security Labels

The Security Label security service provides a method for associating security labels with objects in the MMHS. This then allows a security policy to define what entities can handle messages containing associated security labels. The security label associated with a message MUST indicate the security policy to be followed along with the sensitivity, compartments, and other handling caveats

associated with the message. This service can be used for purposes such as access control or a source of routing information.

If the MMHS supports security services then the MMHS MUST implement this service as profiled in Section 4.2.5.

4.1.7. Non-repudiation of Receipt

The Non-repudiation of Receipt security service provides the originator with evidence that demonstrates, to a third-party, who received the message, and will protect against any attempt by the message recipient to falsely deny having received the message. This evidence is the signed receipt, which includes a digital signature and the certificates necessary to verify it.

The MMHS MAY implement this service supporting the ReceiptRequest attribute as specified in [RFC2634] Section 2.

4.1.8. Secure Mailing Lists

The Secure Mailing Lists security service allows a Mail List Agent (MLA) to take a single message, perform recipient-specific security processing, and then redistributes the message to each member of the Address List (AL) or Mail List (ML).

The MMHS MAY implement this service supporting the mlExpansionHistory attribute as specified in [RFC2634] Section 4.

4.1.9. Message Counter Signature

The Message Counter Signature security service allows multiple signatures to be applied to the original signature value in a sequential manner. Thus, the Message Counter-signature service allows supervising users or release authorities to countersign for an originator without invalidating the original signature.

The MMHS MAY implement this service supporting the countersignature attribute as specified in [RFC5652] Section 11.4.

4.1.10. Certificate Binding

The Certificate Binding security service allows for a certificate, which is sent with the message to be cryptographically bound to the message.

The MMHS MAY implement this service supporting the SigningCertificate attribute as specified in [RFC2634] Section 5. The SigningCertificate attribute SHOULD only contain the leaf end-user

certificate except where some prior agreement (possibly bilateral) exists to ensure that path validation is not adversely affected. Differing treatment in [RFC2634] Section 5.3, paragraph 3 avoids impact to path validation if only the leaf certificate is included.

4.1.11. Compressed Data

The Compressed Data security service reduces message size, which helps to protect MMHS availability and may provide an element of robustness in the event of denial of service attacks.

If the MMHS provides security services it MAY support the Compressed Data service.

The MMHS SHOULD include support for the Compressed Data content type on origination profiled in Section 4.2.1.4.

Alternatively the MMHS MAY support the application/zlib and application/gzip MIME media types on origination as defined in [RFC6713].

On reception the MMHS MUST support the Compressed Data content type, application/zlib media type and application/gzip media type.

4.2. Security Profile

This section profiles the use of the S/MIME protocols [RFC5751], [RFC5652] and [RFC2634] and DKIM protocol [RFC6376] for adding cryptographic services to the MMHS. The relevant sections of [RFC5751], [RFC5652], [RFC2634] and [RFC6376] are listed with further clarifications and amendments specific to the implementation of an MMHS conformant with this profile.

This security profile is aligned with the "Profile for the Use of the Cryptographic Message Syntax (CMS) and Enhanced Security Services (ESS) for S/MIME", [STANAG-4631].

In order for participating organisations (or domains) to obtain secure interoperability additional bilateral agreements on the labeling, cryptographic algorithms and Public Key Infrastructure (PKI) need to be achieved.

4.2.1. S/MIME Cryptographic Message Syntax Content Types

If the MMHS supports the S/MIME protocols for implementing the security services then the MMHS MUST support the Data, SignedData, EnvelopedData, and CompressedData content types as specified in [RFC5751].

In accordance with [RFC5652] ContentInfo MUST be supported to encapsulate the outer most SignedData or EnvelopedData content type. Conventions for inner wrappers MUST comply with [RFC5751].

The clarifications and refinements are as follows:

- The ContentInfo contentType field MUST be supported.

- The ContentInfo content field MUST be supported.

4.2.1.1. Data Content Type

The MMHS MUST use the id-data content type identifier to identify the "inner" MIME message content as specified in [RFC5751].

4.2.1.2. Signed-data Content Type

The signedData content type is specified in [RFC5652] Section 5, consisting of MIME content (identified by the id-data content type) and zero or more signature values.

4.2.1.2.1. SignedData Type

The MMHS MUST support the SignedData type as specified in [RFC5652] Section 5.1. The clarifications and refinements are as follows:

- The MMHS MUST support the EncapsulatedContentInfo type eContentType attribute. The value of the eContentType MUST be id-data unless the content is compressed according to Section 4.2.1.4.

- The MMHS MUST support the EncapsulatedContentInfo type eContent attribute. The value of the eContent MUST contain the content to be signed. If the content is compressed using the compressed-data content type as defined in Section 4.2.1.4, the CompressedData.encapContentInfo.eContentType MUST be set to the id-data content type identifier of the compressed MIME content and the CompressedData.encapContentInfo.eContent MUST contain the MIME content to be compressed and protected by S/MIME.

- The MMHS MUST support X.509 version 3 certificates. An MMHS with high throughput MUST include certificates within the message. An MMHS with impoverished communications SHOULD NOT send certificates with the message.

- The MMHS MUST support the certificate profile and CRL profile specified in [RFC5280] [RFC6818].

- The MMHS MUST support X.509 version 3 certificate processing specified in [RFC5750].

4.2.1.2.2. SignerInfo Type

The SignerInfo type is specified in [RFC5652] Section 5.3 allowing the inclusion of unsigned and signed attributes along with a signature. The clarifications and refinements are as follows:

- The MMHS MUST support signed attributes. As a minimum the MMHS MUST support processing and handling of the following signed attributes: contentType ([RFC5751] Section 2.5.1); eSSSecurityLabel ([RFC2634] Section 3.2; messageDigest ([RFC5652] Section 11.2); signingTime ([RFC5751] Section 2.5.1); sMIMECapabilities ([RFC5751] Section 2.5.2); and, sMIMEEncryptionKeyPreference ([RFC5751] Section 2.5.3).

- The MMHS MUST support the conventions for using the Secure Hash Algorithm (SHA) message digest algorithms and signature algorithms as specified in [RFC5754] and [RFC5751].

- The MMHS MUST support both the SignerIdentifier type attributes issuerAndSerialNumber and subjectKeyIdentifier.

4.2.1.3. Enveloped-data Content Type

The envelopedData content type is specified in [RFC5652] Section 6, consisting of an encrypted MIME content (identified by the id-data content type) and encrypted content-encryption keys for one or more recipients.

4.2.1.3.1. EnvelopedData Type

The MMHS MUST support the EnvelopedData type as specified in [RFC5652] Section 6.1. The clarifications and refinements are as follows:

- The MMHS MUST support the EncryptedContentInfo type eContentType attribute. The value of the eContentType MUST be id-data unless the content is compressed according to Section 4.2.1.4.

- The MMHS MUST support the EncryptedContentInfo type eContent attribute. The value of the eContent MUST contain the content to be encrypted. If the content is compressed using the compressed-data content type as defined in Section 4.2.1.4, the CompressedData.encapContentInfo.eContentType MUST be set to the id-data content type identifier of the compressed MIME content and

the CompressedData.encapContentInfo.eContent MUST contain the MIME content to be compressed and protected by S/MIME.

- The MMHS MUST support the originatorInfo attribute if required by the key-management algorithm (refer to Section 4.2.1.3.1.1).

- The MMHS MUST support X.509 version 3 certificates. An MMHS with high throughput MUST include certificates within the message. An MMHS with impoverished communications SHOULD NOT send certificates with the message.

- The MMHS MUST support the certificate profile and CRL profile specified in [RFC5280] [RFC6818].

- The MMHS MUST support X.509 version 3 certificate processing specified in [RFC5750].

4.2.1.3.1.1. RecipientInfo Type

The RecipientInfo type is specified in [RFC5652] Section 6.2. The clarifications and refinements are as follows:

- The MMHS MAY support KeyTransRecipientInfo.

- The MMHS MUST support KeyAgreeRecipientInfo. The originatorKey attribute MUST be supported as the choice for the originator to specify the sender's key agreement public key.

- The MMHS MAY support KEKRecipientInfo.

- The MMHS MAY support PasswordRecipientinfo.

- The MMHS MAY support OtherRecipientInfo.

4.2.1.4. Compressed-Data Content Type

The MMHS MUST support the compressedData content type as specified in [RFC3274].

4.2.1.4.1. CompressedData Type

In the cases where the MMHS uses compressedData, it MUST only be used once for every message and MUST only be used around the content of the innermost security wrapper.

4.2.2. S/MIME Triple Wrapping

If the MMHS supports S/MIME protocols for providing the security services (defined in this profile) the MMHS MUST support military messages that are triple wrapped or signed only. A triple wrapped message is one that has been signed, then encrypted, then signed again. The signers of the inner and outer signatures may be different entities or the same entity. If a military message is triple wrapped, the SignedData and EnvelopedData wrappers MUST follow the specifications described in Section 4.2.1.2 and Section 4.2.1.3 of this profile, respectively.

4.2.3. Organisation to Organisation Security

The implementation of the MMHS security services is dependent upon the security and assurance requirements that are to be met by those MMHS security services. As such, the identity of the signer of the MMHS message may be the user, the role the user is performing or the organization the user belongs to. If the MMHS supports S/MIME protocols for providing the security services (defined in this profile) and the MMHS is providing organisation to organisation security services then the MMHS MUST support Domain-based signing using S/MIME as specified in [I-D.melnikov-smime-msa-to-mda].

4.2.4. DKIM Digital Signatures

DKIM [RFC6376] defines an organization-level digital signature authentication framework for Internet email, using public key cryptography and using the domain name service as its key server technology. However, it is possible to administer DKIM to support user-level signature granularity. This profile specifies the use of DKIM defined in [RFC6376] for providing an alternative security mechanism to S/MIME to deliver the Authentication of Origin (Section 4.1.2), Non-repudiation of Origin (Section 4.1.3) and Message Integrity (Section 4.1.4) security services to the MMHS. However, the implementation of DKIM is dependent upon the security and assurance requirements that are to be met by the MMHS security services. An MMHS MAY implement DKIM (to apply digital signatures for the MMHS message header fields and message body) to meet those security and assurance requirements based on one of the following use cases:

1. Share the organization signing identity (identified by the Signing Domain Identifier (SDID)) private key for signing the MMHS message. The MMHS message is digitally signed by the organization MSA component. This profile does not provide end to end security services. This profile supports organization to

organization Authentication of Origin, Non-repudiation of Origin and Message Integrity security services.

2. Share the organization signing identity private key for signing the MMHS message. The email address of the MMHS message originator can be specified as the Agent or User Identifier (AUID). The semantics for performing per-user identity differentiation with this approach MUST be agreed out-of-band and is outside the scope of this MMHS profile. The MMHS message is digitally signed by the organization MSA component. This profile does not provide end to end security services. This profile supports organization to organization Authentication of Origin, Non-repudiation of Origin and Message Integrity security services.

3. Generate per-user public/private key pairs where the public key is published to distinct subdomains (of the organization domain). The MMHS message is signed with the user's private key and the signing identity is identifiable by the user's subdomain value in the SDID. The MMHS message is digitally signed by the MUA. This profile supports end to end Authentication of Origin, Non-repudiation of Origin and Message Integrity security services.

4. Generate per-user public/private key pairs where the public key is published to a unique resource record under the organization domain. The MMHS message is signed with the user's private key and the signing identity is identifiable by the domain value in the SDID and the unique resource record identified by the selector value. The MMHS message is digitally signed by the MUA. This profile supports end to end Authentication of Origin, Non-repudiation of Origin and Message Integrity security services.

To provide organization to organization security services: the recipient MUA SHOULD support DKIM digital signature verification or the MUA MUST support the Authentication-Results header field as specified in [RFC7601] according to the security policy; and the organization border MTA (or MDA) MUST support DKIM digital signature verification and output the verification results (according to the security policy) to the Authentication-Results header field compliant with [RFC7601].

To provide end to end security services the recipient MUA MUST support DKIM digital signature verification specified in [RFC6376].

DKIM does not provide confidentiality security services.

4.2.5. Security Labels

If the MMHS supports S/MIME protocols for implementing security services then the MMHS MUST support on origination the ESSSecurityLabel specified in Section 3 of [RFC2634]. The MMHS MUST support the security-policy-identifier, security-classification, privacy-mark and security-categories attributes of the ESSSecurityLabel. The MMHS MAY support the Equivalent Security Labels EquivalentLabels as specified in [RFC2634] Section 3.4.

An MMHS MAY on origination support the SIO-Label header field as specified in [RFC7444].

On reception the MMHS MUST support the ESSSecurityLabel and SIO-Label. In the case where a military message contains a SIO-Label and an ESSSecurityLabel the MMHS MUST assert that the policy conveyed in both are the same and that the sensitivity, compartments, and other handling caveats that can be conveyed in both are the same.

4.2.6. Message Header Fields

By default, [RFC5751] secures MIME message body parts, excluding the message header fields. If the MMHS implements S/MIME security services then the MMHS SHOULD provide a mechanism for securing the message header fields. [RFC5751] includes a mechanism for protecting the header fields where the whole message is wrapped in a message/rfc822 MIME media type. However, this approach can be problematic for non-S/MIME aware MUAs and does not provide a mechanism for signing a subset of message header fields.

If the MMHS provides security services this profile requires that the MMHS MUST support the protection for the integrity and authenticity of MMHS message header fields.

The MMHS MUST support the mechanism for protecting the header fields as defined in [RFC5751] based on the considerations specified in [I-D.melnikov-smime-header-signing] and/or the MMHS MUST support DomainKeys Identified Mail (DKIM) Signatures profiled in Section 4.2.4 for digitally signing the MMHS message header fields.

In the case of DKIM for digitally signing the MMHS message header fields a subset or all of the MMHS message header fields MAY be digitally signed. The MMHS message headers that are required to be digitally signed are to be specified in the security policy being enforced, however a recommended set of MMHS message headers that are to be digitally signed (if present) are listed below (note that if a header field is absent, DKIM will provide protection from insertion of the header field):

- From

- Reply-To

- Subject

- Date

- To, Cc, Bcc

- Sender

- Expires

- Supersedes

- Message-ID

- In-Reply-To, References

- SIO-Label

- MMHS-Primary-Precedence, MMHS-Copy-Precedence, MMHS-Message-Type, MMHS-Extended-Authorisation-Info, MMHS-Authorizing-Users

- MT-Priority

DKIM does not provide confidentiality security services.

5. Requirements on Mail User Agents

5.1. Standards Compliance

A Mail User Agent (MUA) compliant with this specification MUST support

1. Internet Message Format [RFC5322].

2. Multipurpose Internet Mail Extensions (MIME) [RFC2045] [RFC2046] [RFC2047] [RFC2049] [RFC2231]. In particular they must be able to generate, display and process of message/rfc822, multipart/mixed and text/plain media types. Additionally, the ability to decode application/zlib and application/gzip media types on receipt as defined in [RFC6713] and support for format=flowed text/plain media type parameter [RFC3676].

3. Parsing, processing and having the ability to generate MMHS header fields specified in [RFC6477].

4. The ability to specify priority on origination, in particular the ability to insert MT-Priority header field [RFC6758] into messsages to be sent.

5. Parsing and processing of multipart/report media type for the Reporting of Mail System Administrative Messages [RFC6522] containing message/delivery-status [RFC3464] and Message Disposition Notification (MDN) [RFC3798].

6. The ability to request an MDN and the ability to generate an MDN in response to a request [RFC3798].

7. The ability to indicate message language using the Content-Language header field, as defined in [RFC3282].

8. The ability to select message expiration date when composing a message (using the Expires header field [RFC2156]) and display whether a message is expired or not upon receipt.

9. Use of SMTP extension for Delivery Status Notifications [RFC3461], in particular support for NOTIFY, RET and ENVID parameters.

10. Use of the Deliver By SMTP extension [RFC2852] for specifying the Latest Delivery date for a message.

11. If supporting S/MIME for security services: the ability to send and receive signed and encrypted S/MIME messages [RFC5652] [RFC5751].

12. If supporting S/MIME for security services: the ability to send and receive ESS Security Labels [RFC2634].

13. If supporting DKIM for security services: support DKIM digital signature verification specified in [RFC6376] or support the Authentication-Results header field as specified in [RFC7601] according to the security policy.

14. Support for SIO-Label header field [RFC7444] on receipt.

MUA can also take advantage of SMTP extensions advertised by MSAs (see Section 6).

5.2. Audit Trail and Logging

Storage of audit data by the MUA is required to support security monitoring, accountability, and tractability of messages to the source. This information will be used to provide accountability and

support for any required tracer actions. All stored audit data shall be maintained for at least ten (10) days. Data will be recorded and stored at each MUA to provide an audit capability for messages that are submitted and received. The following table indicates which audit information is required at a minimum to be logged by the MUA for submitted and received messages. Policy may require longer retention periods and additional information be stored. The integrity of audit logs must be protected.

Submitted Messages	Delivered/Received Messages
Authorizing Users Indication, Extended Authorization Info, MM Identification, Message Identification, Delivery/Non-delivery Notification, Receipt/Non-receipt Notification Request Indication, Primary/Copy Precedence, Primary and Copy Recipients Indication, Blind Copy Recipient Indication, Non-Repudiation of Receipt, Security Labels, Message Type	Extended Authorization Info, MM Identification, Message Identification, Originator Indication, Primary/Copy Precedence, Security Labels, Delivery Timestamp Indication

6. Requirements on Mail Submission Agents

6.1. Standards Compliance

In addition to the list of requirements specified in [RFC6409], an Mail Submission Agent (MSA) compliant with this specification MUST support:

1. SMTP Extension for Authentication [RFC4954]. For environment using X.509 certificates, SASL EXTERNAL [RFC4422] authentication mechanism must be supported. For environment using Kerberos, SASL GSSAPI [RFC4752] authentication mechanism must be supported. For environment using password based authentication, SASL SCRAM [RFC5802] must be supported.

2. SMTP Extension for Secure SMTP over TLS [RFC3207].

3. SMTP Service Extension for Returning Enhanced Error Codes [RFC2034].

4. Deliver By SMTP Service Extension [RFC2852].

5. SMTP extension for Message Transfer Priorities. [RFC6710] "STANAG4406" Priority Assignment Policy MUST be advertised in the EHLO response. The MSA MUST be able to handle the MT-Priority header field as specified in [RFC6758].

6. SMTP extension for for Delivery Status Notifications [RFC3461].

7. SMTP Extension for 8-bit MIME transport [RFC6152].

8. SMTP Extension for Message Size Declaration [RFC1870].

9. SMTP Extension for Command Pipelining [RFC2920].

10. SMTP Extensions for Transmission of Large and Binary MIME Messages [RFC3030].

11. Support Draft & Release procedure using the MMHS-Authorizing-Users header field [I-D.melnikov-mmhs-authorizing-users].

12. If supporting S/MIME for security services: the ability to sign and/or encrypt S/MIME messages on bahalf of the originating domain as specified in [I-D.melnikov-smime-msa-to-mda].

13. If supporting DKIM for security services: support DKIM digital signature generation as specified in [RFC6376].

The following SMTP extensions are OPTIONAL to support in MSAs compliant with this specification:

1. SMTP Submission Service Extension for Future Message Release [RFC4865].

6.2. Audit Trail and Logging

Storage of audit data by the MSA is required to support security monitoring, accountability, and traceability of messages to the source. This information will be used to provide accountability and support for any required tracer actions. All stored audit data shall be maintained for at least ten (10) days. Data will be recorded and stored at each MSA to provide an audit capability for messages that are delivered and submitted. The following table indicates which audit information is required at a minimum to be logged by the MSA for delivered and submitted messages. Policy may require longer retention periods and additional information be stored. The integrity of audit logs must be protected.

Submitted Messages
MM Identification, Message Identification, Submission Timestamp Indication, Priority

7. Requirements on Mail Transfer Agents

7.1. Standards Compliance

A Mail Transfer Agent (MTA) compliant with this specification MUST support

1. SMTP Service Extension for Returning Enhanced Error Codes [RFC2034].

2. Deliver By SMTP Service Extension [RFC2852].

3. SMTP extension for Message Transfer Priorities [RFC6710]. "STANAG4406" Priority Assignment Policy MUST be advertised in the EHLO response. The MTA MUST be able to handle the MT-Priority header field as specified in [RFC6758].

4. SMTP extension for for Delivery Status Notifications [RFC3461].

5. SMTP Extension for 8-bit MIME transport [RFC6152].

6. SMTP Extension for Message Size Declaration [RFC1870].

7. SMTP Extension for Command Pipelining [RFC2920].

8. SMTP Extensions for Transmission of Large and Binary MIME Messages [RFC3030].

Additionally border MTAs in originating domains MUST support

1. Enforcement of correct Draft & Release procedure using the MMHS-Authorizing-Users header field [I-D.melnikov-mmhs-authorizing-users].

2. If supporting S/MIME for security services: the ability to sign and/or encrypt S/MIME messages on bahalf of the originating domain as specified in [I-D.melnikov-smime-msa-to-mda].

3. If supporting DKIM for security services: support DKIM digital signature generation as specified in [RFC6376].

4. If supporting S/MIME for security services: enforcement of correctness of ESS Security Labels [RFC2634].

5. Enforcement of correctness of security labels in SIO-Label header field [RFC7444].

6. SMTP Extension for Secure SMTP over TLS [RFC3207].

7. SMTP Extension for Authentication [RFC4954].

Additionally border MTAs in receiving domains MUST support

1. If supporting S/MIME for security services: the ability to verify and/or decrypt S/MIME messages on behalf of the receiving domain as specified in [I-D.melnikov-smime-msa-to-mda].

2. If supporting DKIM for security services: support DKIM digital signature verification as specified in [RFC6376].

3. Support for the Authentication-Results header field generation as specified in [RFC7601] if required by the security policy.

4. If supporting S/MIME for security services: enforcement of correctness of ESS Security Labels [RFC2634].

5. Enforcement of correctness of security labels in SIO-Label header field [RFC7444].

6. SMTP Extension for Secure SMTP over TLS [RFC3207].

7. SMTP Extension for Authentication [RFC4954].

7.2. Audit Trail and Logging

Storage of audit data by the MTA is required to support security monitoring, accountability, and tracability of messages to the source. This information will be used to provide accountability and support for any required tracer actions. All stored audit data shall be maintained for at least ten (10) days. Data will be recorded and stored at each MTA to provide an audit capability for messages that are sent and received. The following table indicates which audit information is required at a minimum to be logged by the MTA for inbound and outbound messages. Policy may require longer retention periods and additional information be stored. The integrity of audit logs must be protected.

Inbound Messages	Outbound Message
MM Identification, Message Identification, Submission Timestamp Indication, Priority, Time of Transfer In*	MM Identification, Message Identification, Submission Timestamp Indication, Priority, Time of Transfer Out*

* MTAs operating in a relay capacity are responsible for logging the marked attributes.

8. IANA Considerations

This document doesn't ask for any action from IANA.

9. Security Considerations

This document specifies an MMHS Profile for a comparable messaging service to STANAG 4406 Edition 2 or [ACP123] provided using Internet Electronic Mail, SMTP and their extensions, S/MIME and DKIM.

The MMHS Profile is not defining new protocol, therefore no new security concerns are raised that are not already captured by Email [RFC5322], MIME [RFC2045], S/MIME [RFC5751], DKIM [RFC6376], ESS [RFC2634] and SIO-Label [RFC7444] in general.

10. References

10.1. Normative References

[RFC2033] Myers, J., "Local Mail Transfer Protocol", RFC 2033, DOI 10.17487/RFC2033, October 1996, <http://www.rfc-editor.org/info/rfc2033>.

[RFC2034] Freed, N., "SMTP Service Extension for Returning Enhanced Error Codes", RFC 2034, DOI 10.17487/RFC2034, October 1996, <http://www.rfc-editor.org/info/rfc2034>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3461] Moore, K., "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)", RFC 3461, DOI 10.17487/RFC3461, January 2003, <http://www.rfc-editor.org/info/rfc3461>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <http://www.rfc-editor.org/info/rfc5321>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <http://www.rfc-editor.org/info/rfc5322>.

[RFC6409] Gellens, R. and J. Klensin, "Message Submission for Mail", STD 72, RFC 6409, DOI 10.17487/RFC6409, November 2011, <http://www.rfc-editor.org/info/rfc6409>.

[RFC1870] Klensin, J., Freed, N., and K. Moore, "SMTP Service Extension for Message Size Declaration", STD 10, RFC 1870, DOI 10.17487/RFC1870, November 1995, <http://www.rfc-editor.org/info/rfc1870>.

[RFC2852] Newman, D., "Deliver By SMTP Service Extension", RFC 2852, DOI 10.17487/RFC2852, June 2000, <http://www.rfc-editor.org/info/rfc2852>.

[RFC2920] Freed, N., "SMTP Service Extension for Command Pipelining", STD 60, RFC 2920, DOI 10.17487/RFC2920, September 2000, <http://www.rfc-editor.org/info/rfc2920>.

[RFC3030] Vaudreuil, G., "SMTP Service Extensions for Transmission of Large and Binary MIME Messages", RFC 3030, DOI 10.17487/RFC3030, December 2000, <http://www.rfc-editor.org/info/rfc3030>.

[RFC4865] White, G. and G. Vaudreuil, "SMTP Submission Service Extension for Future Message Release", RFC 4865, DOI 10.17487/RFC4865, May 2007, <http://www.rfc-editor.org/info/rfc4865>.

[RFC6152] Klensin, J., Freed, N., Rose, M., and D. Crocker, Ed., "SMTP Service Extension for 8-bit MIME Transport", STD 71, RFC 6152, DOI 10.17487/RFC6152, March 2011, <http://www.rfc-editor.org/info/rfc6152>.

[RFC4954] Siemborski, R., Ed. and A. Melnikov, Ed., "SMTP Service Extension for Authentication", RFC 4954, DOI 10.17487/RFC4954, July 2007, <http://www.rfc-editor.org/info/rfc4954>.

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, DOI 10.17487/RFC3207, February 2002, <http://www.rfc-editor.org/info/rfc3207>.

[RFC6477] Melnikov, A. and G. Lunt, "Registration of Military Message Handling System (MMHS) Header Fields for Use in Internet Mail", RFC 6477, DOI 10.17487/RFC6477, January 2012, <http://www.rfc-editor.org/info/rfc6477>.

[RFC6710] Melnikov, A. and K. Carlberg, "Simple Mail Transfer Protocol Extension for Message Transfer Priorities", RFC 6710, DOI 10.17487/RFC6710, August 2012, <http://www.rfc-editor.org/info/rfc6710>.

[RFC6758] Melnikov, A. and K. Carlberg, "Tunneling of SMTP Message Transfer Priorities", RFC 6758, DOI 10.17487/RFC6758, October 2012, <http://www.rfc-editor.org/info/rfc6758>.

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <http://www.rfc-editor.org/info/rfc2045>.

[RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, DOI 10.17487/RFC2046, November 1996, <http://www.rfc-editor.org/info/rfc2046>.

[RFC2047] Moore, K., "MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text", RFC 2047, DOI 10.17487/RFC2047, November 1996, <http://www.rfc-editor.org/info/rfc2047>.

[RFC2049] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples", RFC 2049, DOI 10.17487/RFC2049, November 1996, <http://www.rfc-editor.org/info/rfc2049>.

[RFC2231] Freed, N. and K. Moore, "MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations", RFC 2231, DOI 10.17487/RFC2231, November 1997, <http://www.rfc-editor.org/info/rfc2231>.

[RFC3676] Gellens, R., "The Text/Plain Format and DelSp Parameters", RFC 3676, DOI 10.17487/RFC3676, February 2004, <http://www.rfc-editor.org/info/rfc3676>.

[RFC6713] Levine, J., "The 'application/zlib' and 'application/gzip' Media Types", RFC 6713, DOI 10.17487/RFC6713, August 2012, <http://www.rfc-editor.org/info/rfc6713>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC6818] Yee, P., "Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 6818, DOI 10.17487/RFC6818, January 2013, <http://www.rfc-editor.org/info/rfc6818>.

[RFC2634] Hoffman, P., Ed., "Enhanced Security Services for S/MIME", RFC 2634, DOI 10.17487/RFC2634, June 1999, <http://www.rfc-editor.org/info/rfc2634>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <http://www.rfc-editor.org/info/rfc5652>.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, DOI 10.17487/RFC5751, January 2010, <http://www.rfc-editor.org/info/rfc5751>.

[RFC5754] Turner, S., "Using SHA2 Algorithms with Cryptographic Message Syntax", RFC 5754, DOI 10.17487/RFC5754, January 2010, <http://www.rfc-editor.org/info/rfc5754>.

[RFC5750] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling", RFC 5750, DOI 10.17487/RFC5750, January 2010, <http://www.rfc-editor.org/info/rfc5750>.

[RFC3274] Gutmann, P., "Compressed Data Content Type for Cryptographic Message Syntax (CMS)", RFC 3274, DOI 10.17487/RFC3274, June 2002, <http://www.rfc-editor.org/info/rfc3274>.

[RFC3464] Moore, K. and G. Vaudreuil, "An Extensible Message Format for Delivery Status Notifications", RFC 3464, DOI 10.17487/RFC3464, January 2003, <http://www.rfc-editor.org/info/rfc3464>.

[RFC6522] Kucherawy, M., Ed., "The Multipart/Report Media Type for the Reporting of Mail System Administrative Messages", STD 73, RFC 6522, DOI 10.17487/RFC6522, January 2012, <http://www.rfc-editor.org/info/rfc6522>.

[RFC3798] Hansen, T., Ed. and G. Vaudreuil, Ed., "Message Disposition Notification", RFC 3798, DOI 10.17487/RFC3798, May 2004, <http://www.rfc-editor.org/info/rfc3798>.

[RFC3282] Alvestrand, H., "Content Language Headers", RFC 3282, DOI 10.17487/RFC3282, May 2002, <http://www.rfc-editor.org/info/rfc3282>.

[RFC5228] Guenther, P., Ed. and T. Showalter, Ed., "Sieve: An Email Filtering Language", RFC 5228, DOI 10.17487/RFC5228, January 2008, <http://www.rfc-editor.org/info/rfc5228>.

[RFC7601] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", RFC 7601, DOI 10.17487/RFC7601, August 2015, <http://www.rfc-editor.org/info/rfc7601>.

[RFC2156] Kille, S., "MIXER (Mime Internet X.400 Enhanced Relay): Mapping between X.400 and RFC 822/MIME", RFC 2156, DOI 10.17487/RFC2156, January 1998, <http://www.rfc-editor.org/info/rfc2156>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <http://www.rfc-editor.org/info/rfc6376>.

[RFC7444] Zeilenga, K. and A. Melnikov, "Security Labels in Internet Email", RFC 7444, DOI 10.17487/RFC7444, February 2015, <http://www.rfc-editor.org/info/rfc7444>.

[RFC4422] Melnikov, A., Ed. and K. Zeilenga, Ed., "Simple Authentication and Security Layer (SASL)", RFC 4422, DOI 10.17487/RFC4422, June 2006, <http://www.rfc-editor.org/info/rfc4422>.

[RFC4752] Melnikov, A., Ed., "The Kerberos V5 ("GSSAPI") Simple Authentication and Security Layer (SASL) Mechanism", RFC 4752, DOI 10.17487/RFC4752, November 2006, <http://www.rfc-editor.org/info/rfc4752>.

[RFC5802] Newman, C., Menon-Sen, A., Melnikov, A., and N. Williams, "Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms", RFC 5802, DOI 10.17487/RFC5802, July 2010, <http://www.rfc-editor.org/info/rfc5802>.

[ACP123] CCEB, , "Common Messaging Strategy and Procedures", ACP 123, May 2009.

[I-D.melnikov-mmhs-authorizing-users]
Melnikov, A., "Draft and Release using Internet Email", draft-melnikov-mmhs-authorizing-users-08 (work in progress), June 2015.

[I-D.melnikov-smime-msa-to-mda]
Melnikov, A., "Domain-based signing and encryption using S/MIME", draft-melnikov-smime-msa-to-mda-04 (work in progress), March 2014.

[I-D.melnikov-smime-header-signing]
Melnikov, A., "Considerations for protecting Email header with S/MIME", draft-melnikov-smime-header-signing-02 (work in progress), April 2015.

10.2. Informative References

[RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598, DOI 10.17487/RFC5598, July 2009, <http://www.rfc-editor.org/info/rfc5598>.

[STANAG-4406]
NATO, , "STANAG 4406 Edition 2: Military Message Handling System", STANAG 4406, March 2005.

[STANAG-4631]
NATO, , "STANAG 4631 Edition 1: Profile for the Use of the Cryptographic Message Syntax (CMS) and Enhanced Security Services (ESS) for S/MIME", STANAG 4631, June 2008.

Appendix A. Acknowledgements

Many thanks for input provided by Steve Kille and David Wilson.

Authors' Addresses

Alexey Melnikov
Isode Ltd
5 Castle Business Village
36 Station Road
Hampton, Middlesex TW12 2BX
UK

EMail: Alexey.Melnikov@isode.com

Graeme Lunt
SMHS Ltd
Bescar Moss Farm
Bescar Lane
Ormskirk L40 9QN
UK

EMail: graeme.lunt@smhs.co.uk

Alan Ross
SMHS Ltd
Bescar Moss Farm
Bescar Lane
Ormskirk L40 9QN
UK

EMail: alan.ross@smhs.co.uk