COMMON MESSAGING STRATEGY AND PROCEDURES

COMBINED COMMUNICATIONS-ELECTRONICS BOARD (CCEB)

MAY 2009

FOREWORD

1. The Combined Communications-Electronics Board (CCEB) is comprised of the five member nations, Australia, Canada, New Zealand, United Kingdom and United States and is the Sponsoring Authority for all Allied Communications Publications (ACPs). ACPs are raised and issued under common agreement between the member nations.

2. ACP 123(B), COMMON MESSAGING STRATEGY AND PROCEDURE, is an UNCLASSIFIED CCEB publication.

3. This publication contains Allied military information for official purposes only.

4. It is permitted to copy or make extracts from this publication.

5. This ACP is to be maintained and amended in accordance with the provisions of the current version of ACP 198.

THE COMBINED COMMUNICATION-ELECTRONICS BOARD
LETTER OF PROMULGATION

FOR ACP 123(B)

1. The purpose of this Combined Communication Electronics Board (CCEB) Letter of Promulgation is to implement ACP 123(B) within the Armed Forces of the CCEB Nations. ACP 123(B) COMMON MESSAGING STRATEGY AND PROCEDURE, is an UNCLASSIFIED publication developed for Allied use and, under the direction of the CCEB Principals. It is promulgated for guidance, information, and use by the Armed Forces and other users of military communications facilities.

2. ACP 123(B) is effective on receipt for CCEB Nations and when promulgated by the NATO Military Committee (NAMILCOM) for NATO nations and Strategic Commands.

EFFECTIVE STATUS

Publication	Effective for	Date	Authority
ACP 123(B)	CCEB	On Receipt	LOP

3. All proposed amendments to the publication are to be forwarded to the national coordinating authorities of the CCEB or NAMILCOM.

For the CCEB Principals

Paul Foster

P. FOSTER
Major, CF
CCEB Permanent Secretary

RECORD OF MESSAGE CORRECTIONS

Identification of Message Correction and Date, Time Group		Date Entered	By whom entered
DTG	Correction		

TABLE OF CONTENTS

TABLE OF FIGURES

CHAPTER 1
GENERAL

SECTION I
INTRODUCTION

101. The function of this document, Allied Communication Publication (ACP) 123, is to define the services, protocol, and procedures to support electronic messaging for Defense. In so doing the document expands on X.400 and defines the Military Messaging Elements of Service (EoS), procedures and protocols. Some guidelines for national implementation of the messaging systems are described. Minimal criteria to ease interoperability with existing systems through message and protocol gateways are presented. The aim of ACP 123 is to encapsulate all services, procedures, and protocols for all Allied X.400 messaging environments into one document.

BACKGROUND

102. This ACP was developed and coordinated under the auspices of the Combined Communications Electronics Board (CCEB) with the Allied Message Handling (AMH) International Subject Matter Experts (ISME) working group and the Messaging Task Force (MTF). The CCEB organized these groups to develop and deploy a common capability to provide interoperability among the Allies for Military Message (MM) traffic. The new common messaging strategy, which includes the definition of EoS and a corresponding set of procedures, is based on the 1992 version of the International Telegraph and Telephone Consultative Committee (CCITT)[1] X.400 Series of Recommendations.

103. This ACP identifies the service and protocol requirements necessary to ensure interoperability among Military Message Handling Systems (MMHS) for MM traffic that formally commits an organization and requires authorized release. This ACP specifically does not cover messaging between individuals. Gateway and transition issues between MMHS and other messaging systems are out of scope of this ACP. It defines the services that shall be provided and the protocols that shall be used by MMHS in the Application Layer of the Open Systems Interconnection (OSI) reference model. To ensure interoperability with North Atlantic Treaty Organization (NATO) members, this ACP was developed in close coordination with the NATO Consultation, Command and Control (C3) Board (NC3B, AC/322) Information Services Subcommittee (ISSC, SC/5) Core Enterprise Services Working Group (CESWG, WG/5). The CESWG is responsible for maintaining NATO Standardization Agreements (STANAGs) pertaining to military messaging services such as STANAG 4406.

---

[1] Note that CCITT was recently reorganized into the International Telecommunications Union - Telecommunications Standardization Sector (ITU-T). The term CCITT is used here in the interest of maintaining clarity and continuity with references to existing CCITT documents.

104. Annex A is written in the structure and form of the 1992 X.400 series of recommendations, but contains only the changes and enhancements to the base documents necessary to support Military Messaging. Consequently, the numbering of paragraphs, figures, and tables in the annex may not appear to be sequential because the unchanged portions of the base documents are absent. Annex A has been harmonized with Annex A of NATO STANAG 4406, in order to ensure only one protocol definition for the support of the MM content type. Annexes B and E are similarly harmonized with NATO STANAG 4406.

EVOLUTION

105. ACP 123 is based on civilian international standards. The messaging capabilities that are provided by it are gradually being deployed through respective national programs in the CCEB nations. If any changes to this ACP are required due to the lessons learned from the deployed systems and their interconnections as described in ACP 145, then the CCEB MTF will change this ACP after formal review and coordination.

SCOPE

106. The fundamental purpose of ACP 123 is to define a common message service to be provided between all participating nations. This will be achieved by defining the EoS to be provided, the procedures they support, and a messaging strategy. By accomplishing these tasks, participating nations can achieve commonality of message formats[2] and protocols. This does not, however, preclude national differences for internal messaging.

107. Translation gateways may be required between ACP 123 domains and civilian Message Handling System (MHS) domains, and will be required between ACP 123 domains and older military messaging domains (e.g., ACP 127 and its supplements). Additionally, gateways at national boundaries may be necessary due to differences in cryptography or security management issues. Requirements for these gateways are outside the scope of ACP 123. However, by defining the services to be supported and a limited set of corresponding procedures, a consistent quality of service should be attained.

108. This ACP identifies the services and protocol requirements for interoperability between systems implementing the defined service. The focus is on the services to be provided. The procedures to ensure a consistent quality of service are also specified.

---

[2] The term Common Message Format is derived from the current messaging system (ACP 127) which contains a definition of where information is carried in a message. ACP 127 messages are a formatted sequence of characters whereas X.400 messages use a formatting technique to encode information in well-defined data structures. The phrase "Common Message Format" will not be used with ACP 123 because it is not applicable to X.400 messages.

The protocol elements used to convey the service information are also specified when the mechanism to provide the service has been agreed.

109. This ACP pertains primarily to the communication aspects of the messaging application. Local interfaces and requirements, such as the specifics of terminal display and local storage for archival purposes are not part of this publication, except where required to ensure interoperability. ACP 123 includes requirements for which information shall be displayed to the user, but the graphical display is outside the scope of this document.

110. ACP 123 is based on the 1992 CCITT X.400 Series of Recommendations[3] (henceforth referred to as X.400) and adopts the extensions documented in the NATO STANAG 4406. The ACP 123 contains enough information to be read alone by someone familiar with X.400 without duplicating the majority of the material contained in the X.400 Series of Recommendations. However, pointers to related information in X.400 are included for those readers requiring more details. Pointers to related material harmonized with STANAG 4406 refer to Annex A of this document, which contains military extensions to X.400. These extensions are presented in the form of a delta document to X.400.

111. ACP 123 defines the services required in an environment where messages are originated and received using ACP 123. Nations exchanging MMs using X.400 across national boundaries should follow the procedures described in this ACP 123 document. Annex A identifies some services and the related protocol fields that are only required for interworking with older military messaging systems (e.g., ACP 127 and ACP 128). Interworking with these older systems is outside the scope of this document. Origination of these transitional services is therefore not required as part of ACP 123. However, it is recognized that many of these same services will need to be addressed in a transition document.

OVERVIEW

112. The messaging system employing ACP 123 EoS and related procedures will utilize internationally available messaging and directory service standards and protocols to provide a totally automated writer-to-reader messaging system. X.400 will be used for the exchange of messages. Because of the military environment, some additionally required extensions are specified by ACP 123. These additional requirements include security, a Military Messaging User Agent (MM-UA), a Military Messaging Message Store (MM-MS), and a new content type. X.500 will be used for the provision of directory services. Directory services should be provided to support messaging system functions. ACP 133 states the directory services for the Allied environment. It is recommended that directory services and protocols conform

[3] Seven recommendations form the 1992 X.400 Series of Recommendations: X.400, X.402, X.407, X.408, X.411, X.413, and X.420. Where appropriate, the specific recommendation will be referenced.

to ITU-T X.500 Series of Recommendations and support exchange of Lightweight Directory Access Protocol (LDAP) Data Interchange Format (LDIF) files.

113. MMs are composed of X.400 envelopes and Military content type(s). The envelope carries the information necessary for submission, transfer, and delivery of the message. The envelope is the same basic envelope as used in the civilian MHS. With the same envelope, commercial Message Transfer Systems (MTS) may be used to carry MMHS traffic. The content of the message is the information the originator wishes delivered to one or more recipients. The content of the message will be a MM content type, which is comprised of extensions to the X.420 International Standard. (See Figure 1-1.)

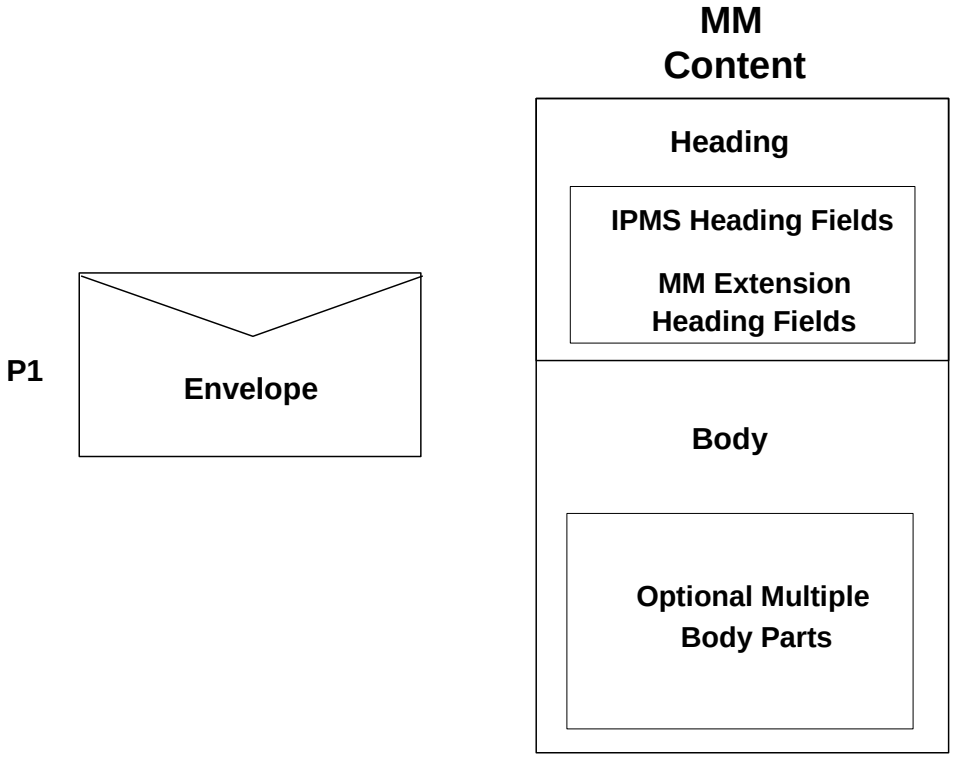


Figure 1-1 X.400/ACP 123 Message Structure

114. The MMHS will be composed of objects that perform message submission, transfer, and delivery and provide additional services; the MTS, which is comprised of Message Transfer Agents (MTAs), will support the transfer of MMs; MM-UAs will support the submission and delivery of MMs; optional Message Stores (MS) will assist an MM-UA in accepting delivery of messages when the MM-UA may not be available, and a Directory System to assist the MMHS and the messaging users themselves. These objects exchange information in the form of formatted Protocol Data Units (PDUs) exchanged over an OSI communication association. Each of the PDU formats constitutes an Application Layer protocol. There are three envelope protocols (or PDUs) used by X.400: P1, P3, and P7. The P1 protocol supports

communication between MTAs. The P3 protocol supports access to the MTS, and the submission and delivery of messages. The P7 protocol supports access to an MS by the MM-UA, and the indirect-submission and retrieval of messages. Content types, such as P772, are information objects that are conveyed with the various envelope protocols. (See Figure 1-2.)

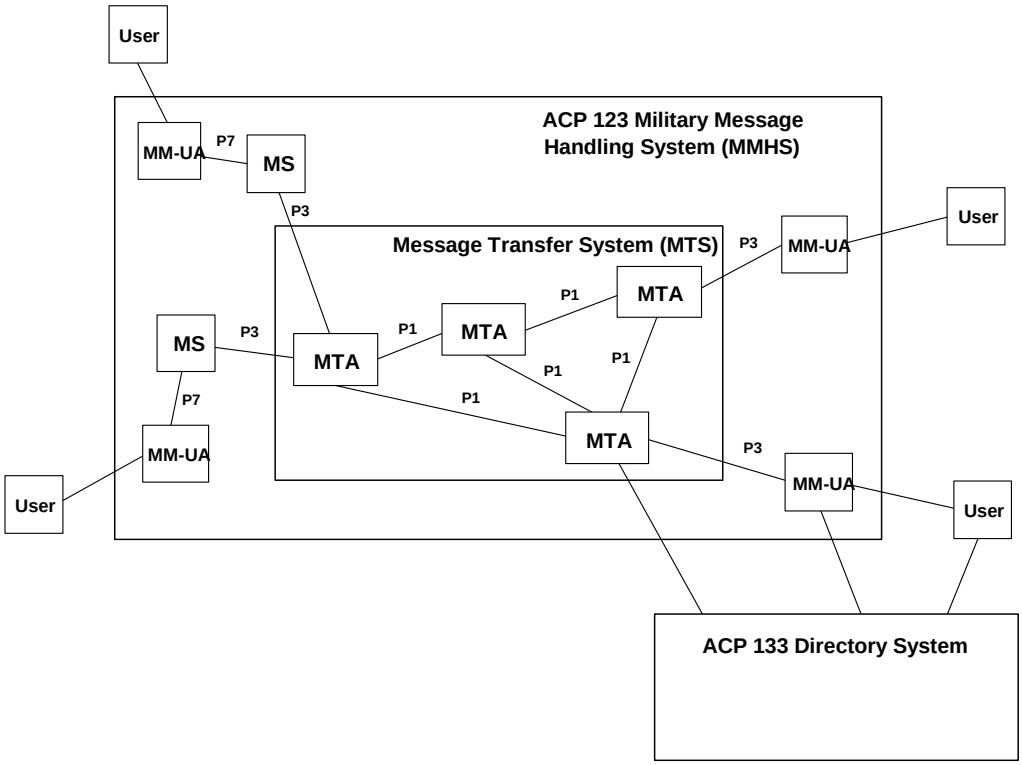


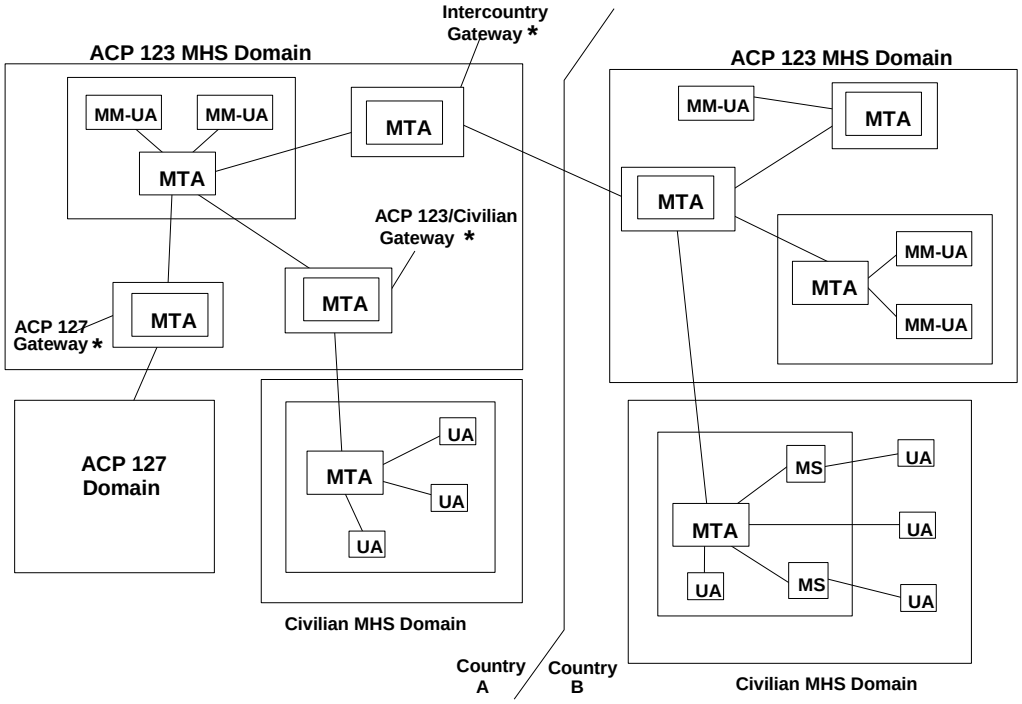
Figure 1-2 ACP 123 Messaging Environment

115. The MMHS Management Domains may be connected to Civilian MHS Management Domains by way of gateways. During transition from older military messaging systems, gateways between older MMHS domains (ACP 127) and ACP 123 domains may also be supported. Such gateways are not defined in this document. The ACP 123 Management Domain within a country may also connect to ACP 123 Management Domains in other countries. (See Figure 1-3.)

STRUCTURE OF THE DOCUMENT

116. This ACP is divided into five chapters. The first chapter (this chapter) outlines the background and scope of ACP 123 and provides an overview of the MMHS. The second chapter defines all the ACP 123 functions in terms of EoS. Chapter three describes specific requirements on each of the three MHS components; the MTS, MM-UA and MS. Chapter four defines policies and procedures associated with the military use of the services provided by MMHS. The fifth chapter defines two MM profiles: one for standard use, and a second for use with a Military Messaging System (MMS) in a restricted bandwidth environment.

117. Throughout the main body of this ACP the use of an italic font (e.g., *this is italics)* distinguishes the names of specific protocol elements cited from the X.400 syntax definition. These names are formatted according to Abstract Syntax Notation One (ASN.1) conventions. As such, these italicized names frequently contain unusual capitalization, hyphens, or missing spaces that are deliberate features of the ASN.1 name.



* = Note that these gateways are expected to be part of the overall system, but are not defined in this ACP.

Figure 1-3 ACP 123 Management Domain Connections

118. Nine (9) annexes are included in this ACP. Annex A defines the MM content type and has been harmonized with the NATO STANAG 4406, in order to ensure only one protocol definition for support of the MM content type. Annex B defines the security solution for MMHS that has been harmonized with NATO STANAG 4406. Annex C is the profile for Common Unrestricted Messaging, which lists the MMHS requirements additional to those in ISO/IEC ISP 10611. Annex D is the content specific profile for the MM content, which lists procedural requirements on protocol elements an implementation shall support to claim conformance to the MM content type. Annex E defines an alternate protocol suite for MMHS that is suitable for a reduced-throughput or tactical domain, which has also been harmonized with STANAG 4406. Annex F is the profile general MS attributes, which lists the requirements for general MS attributes by MM-UA and MM-MS implementations. Annex G is the content specific profile for MM MS attributes, which lists the MM-specific attribute requirements that MM-UA and MM-MS implementations shall support. Annex H is an Information Object Implementation Conformance Statement

(IO-ICS) proforma that provides clear guidelines for implementors of what the mandatory and optional support for the protocol elements used to support the MM content type. This annex contains Appendix A, which can be filled out by an implementor to state exactly what support is claimed by a particular implementation. Annex I is a list of reference documents used in developing this ACP.

SECTION II
DEFINITION OF TERMS USED IN THIS PUBLICATION

DEFINITIONS

119. This section provides definitions for unique terms used in the rest of the document. Terms that are already adequately defined in the X.400 series base standards are not repeated in this section.

a. Abstract Syntax Notation One (ASN.1) – ASN.1 is the notation used to specify an abstract representation of the information conveyed by the protocol data units exchanged in X.400. (Defined in International Standards Organization [ISO] 8824.)

b. Access Unit (AU) – The AU is an origination or delivery end point that provides interconnection between non-ACP 123 compliant users of the MMHS and ACP 123 compliant users.

c. ACP 127 – ACP 127 is used in this document as a generic designator when referring to legacy military messaging systems that are based on ACP 127 and its supplements.

d. ADatP-3 – Allied Data Publication 3 – ADatP-3 refers to a class of military messages that have a pre-defined formatted text designed to convey information for commonly used and mission critical uses. Examples of ADatP-3 messages include Air Tasking Orders, and logistics reports.

e. Address List (AL) – An AL is a short hand method for addressing a predetermined list of recipients. An AL can be carried as an *ORName* on a recipient field or using the *address-list-indicator* military heading extension.

f. Copy Recipients – Copy recipients are those recipients of a message who are sent a message for information purposes only (information addressees).

g. CSP – Common Security Protocol – The CSP is an information object supported by ACP 120 to provide security services for the MMHS. Any message identified with the content type CSP is a Common Security Protocol message. ACP 120 is now treated as historical, but may still be employed nationally.

h. Directory Name – A directory name is a unique identifier for a record stored in a directory system. A directory name can be resolved by a directory system into a X.400 OR Address, a set of user capabilities, or other information. Implementation of a directory that is X.500 conformant is beyond the scope of this ACP. (See paragraphs 428-431.)

i. Dynamic – Dynamic behavior characterizes the constraints on the use of an element of protocol. Base standards normally define only minimal constraints on dynamic behavior in order to leave maximum flexibility to the user. Profiles may impose additional constraints, thus imposing additional requirements that exceed the base standard. The dynamic classifications used within this document are as follows:

(1) Optional – the referenced protocol element may be either present or absent at the discretion of the user (or implementation). This classification is the default requirement normally assigned by base standards. No dynamic constraints are implied. This classification is never explicitly included in classification tables because it is the default condition.

(2) Required (r) – the referenced protocol element shall be present in every instance of communication. Under most circumstances, absence of an element classified as *required* may be construed as a protocol violation. The term dynamic mandatory is sometimes used instead of dynamic required.

(3) Excluded (x) – the referenced protocol element shall never be present in any instance of communication. Under most circumstances, presence of an element classified as *excluded* may be construed as a protocol violation or other error (e.g., security violation). The term dynamic prohibited is sometimes used instead of dynamic excluded.

j. Elements of Service (EoS) – EoS are abstractions that describe features of a system for which the user of that system has direct access. In some cases, the "user" of the system may be another system. For example, the MMS is a consumer of the services provided by the MTS. The X.400 recommendation defines EoS as functional units for the purpose of segmenting and describing message handling features. EoS do not necessarily relate to protocol elements (see clause 1.II.119.x) on a one-to-one basis.

k. Formal Military Message – A formal military message is a message sent on behalf of an organization, in the name of that organization, that establishes a formal commitment on the part of that organization, and that has been formally released in accordance with the policies of the originating nation.

l. Gateway – Gateway is generic term that covers both AUs and translation gateways.

m. MM – Military Message – The MM is an information object supported by ACP 123 that is used to convey messages between military organizations. Any message identified with the content type P772 is a Military Message.

n. MM-AU – Military Messaging Access Unit – The MM-AU is a functional object that links another communication system to the MTS within an MMHS.

o. MM-MS – Military Messaging Message Store – The MM-MS is a functional object that provides an organization or subscriber with capabilities for military message storage and retrieval. It provides a user with indirect submission capabilities and accepts delivery of MMs on behalf of that user. An MM-MS is an X.400 MS that supports retrieval of messages based on the MM-specific MS attributes.

p. MM-UA – Military Messaging User Agent – The MM-UA is a functional object that allows an organization or subscriber to engage in military message handling. An MM-UA is an X.400 User Agent (UA) that can generate and receive MMs.

q. MMHS – Military Message Handling System – The MMHS is the messaging system defined by ACP 123. The purpose of MMHS is to convey MMs among military organizations and individuals. This document addresses only MMHS in the context of MM traffic that has been approved for release between military organizations.[4]

r. MMS – Military Messaging Service – The MMS is a service that provides electronic messaging to staff units and authorized individual users (i.e., message release authorities) in military organizations. The MMS fulfills established military requirements for messaging systems.

s. MS – Message Store – The MS is an optional functional object that provides users with capabilities for message storage and retrieval. It provides a user with indirect submission and accepts delivery of messages on behalf of the user.

t. Plain Language Address Designator (PLAD) – A PLAD is an abbreviated or non-abbreviated activity (organization) title with associated geographical location. The PLAD is used in ACP 127 message addressing.

[4] Guidelines for individual traffic shall be clarified in supplements or by bilateral agreements.

u. Precedence – Precedence is a labeled value that reflects the originator's determination of the relative message importance and thereby determines the required speed of service and its associated message handling by the recipient(s).

v. Primary Recipients – Primary recipients are those recipients of a message who have the responsibility to act on the delivered message (action addressees).

w. Priority – Priority is a labeled value that reflects the required speed of service for a message. It is synonymous with the Grade of Delivery selection in the message transfer service.

x. Protocol Elements – Protocol elements are well-defined data structures that are transmitted between open systems to exchange information. The collection of all such protocol elements used for a particular communication is known as the abstract syntax. Protocol elements do not necessarily relate to EoS (see clause 1.II.119.j) on a one-to-one basis. Protocol elements are sometimes called "protocol fields", "fields", or "sub-fields".

y. Routing Indicator (RI) – The RI is a group of letters assigned to identify a station within a tape relay network. The RI facilitates the routing of traffic, indicates the status of the station, and may indicate its geographical area. (Routing Indicators are composed in accordance with the Routing Indicator Plan described in the ACP 121 series. RIs are used to define the network address of a Communications Center (COMCEN) serving one or more organizations. It is used for routing purposes in ACP 127 messaging).

z. Static – Static behavior characterizes the capability of an implementation to support (i.e., generate, decode or process) an element of protocol. Base standards normally define what constitutes support for a particular element. Base standards normally classify static support requirements for particular protocol elements according to several standardized classifications. Profiles may also impose additional static requirements on elements that the base standard classifies as optional. The static classifications used within this document are as follows:

(1) Mandatory (m) – the element or feature is required to be implemented, and shall be fully supported in conformance with the Specification. An implementation shall be able to generate the element, and/or receive the element and perform all associated procedures (i.e., implying the ability to handle both the syntax and semantics of the element) as relevant, as specified in the MM base standards. Where support for origination (generation) and reception is not distinguished, then both capabilities shall be assumed.

(2) Optional (o) – the capability may be implemented, and if it is implemented it is required to conform to the Specification. An implementation is not required to support the element. If support is claimed, the element shall be treated as if it were specified as mandatory support. If support for origination is not claimed, then the element is not generated. If support for reception is not claimed, then an implementation may ignore the element on delivery, but will not treat it as an error.

(3) Conditional (c) – the requirement on the capability depends on the selection of other optional or conditional items; the element shall be supported under the conditions specified in this information object ICS. If these conditions are met, the element shall be treated as if it were specified as mandatory support. If these conditions are not met, the element shall be treated as if it were specified as optional support (unless otherwise stated).

(4) Out of scope (i) – the element is outside the scope of this information object ICS - i.e., it will not be the subject of an ICS conformance test.

(5) Not applicable (–) – in the given context the base Specification makes it impossible to use this capability.

aa. Translation Gateway – A translation gateway is a component that translates between protocols used on different networks in order to support interworking between users of the different networks.

ab. UA – User Agent – The UA is a functional object that allows a user to engage in message handling.

ac. X.400 – X.400 is a generic designator used in this document to refer to the international civilian standards, both the CCITT[5] X.400 Series of Recommendations and the corresponding ISO/IEC 10021 series (MOTIS).

ad. X.500 – X.500 is generic designator used in this document to refer to the 1993 international civilian standards, both the ITU-T X.500 Series of Recommendations and the corresponding ISO/IEC 9594 series.

ABRREVIATIONS

120. This section lists abbreviations used in the rest of the document. These abbreviations are part of common usage in military messaging.

[5] Note that CCITT was recently reorganized into the ITU-T. The term CCITT is used here in the interest of maintaining clarity and continuity with references to existing CCITT documents.

ACP	Allied Communication Publication
ACSE	Association Control Service element
ADatP	Allied Data Publications
AIG	Address Indicator Group
AL	Address List
ALI	Address List Indicator
AMH	Allied Message Handling
ASE	Application Service Element
ASN.1	Abstract Syntax Notation One
AU	Access Unit
BER	Basic Encoding Rules
CAD	Collective Address Designator
CCEB	Combined Communications Electronics Board
CCITT	International Telegraph and Telephone Consultative Committee[6]
COMCEN	Communications Center
COTS	Commercial Off The Shelf
DL	Distribution List
DTG	Data Time Group
EIT	Encoded Information Type
EoS	Element of Service
IA5	International Alphabet No. 5
IO-ICS	Information Object Implementation Conformance Statement
IP	Interpersonal
IPM	Interpersonal Message
IPMS	Interpersonal Messaging System
ISM	International Subject Matter Experts
ISO	International Organization for Standardization
ISP	International Standardized Profile
ITU-T	International Telecommunications Union - Telecommunications Standardization Sector

[6] Note that CCITT was recently organized into the ITU-T. The term CCITT is used here in the interest of maintaining clarity and continuity with references to existing CCITT documents.

LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
MD	Management Domain
MH	Message Handling
MHS	Message Handling System
MM	Military Message
MMHS	Military Message Handling System
MMS	Military Messaging System
MM-AU	Military Messaging Access Unit
MM-MS	Military Messaging Message Store
MM-UA	Military Messaging User Agent
MOTIS	Message Oriented Text Interchange System
MPDU	Message Protocol Data Unit
MS	Message Store
MT	Message Transfer
MTA	Message Transfer Agent
MTS	Message Transfer System
MTSE	Message Transfer Service Element
NATO	North Atlantic Treaty Organization
NDN	Non-Delivery Notification
NRN	Non-Receipt Notification
OR	Originator/Recipient
P1	Message Transfer Protocol
P3	Submission and Delivery Protocol
P7	Message Store Access Protocol
P772	Military Messaging Protocol (defined in Annex A)
PDAU	Physical Delivery Access Unit
PDS	Physical Delivery Service
PDU	Protocol Data Unit
PER	Packed Encoding Rules
PLAD	Plain Language Address Designator
RI	Routing Indicator
ROSE	Remote Operation Service Element

RTSE	Remote Transfer Service Element
SIC	Subject Indicator Code
STANAG	(NATO) Standardization Agreement
UA	User Agent
USMTF	U.S.Message Text Format
UTC	Coordinated Universal Time

UA	User Agent
X.400	CCITT Series of Recommendations on Message Handling Systems
X.500	CCITT Series of Recommendation on Directory Services

CHAPTER 2
MESSAGE SERVICES - ELEMENTS OF SERVICE

201. This chapter describes, in X.400 terminology, the services provided by the ACP 123 MMHS. The first section lists the Basic X.400 EoS supported by the MMHS with references to their definitions in Annex B of X.400. The second section lists the definition of additional EoS needed in a military environment. These services, also defined in Annex A to STANAG 4406, contain a reference to their definition in Annex A of this document. Transitional EoS, which facilitate interoperability with existing military messaging systems (ACP 127), are grouped in a separate paragraph.

202. When an X.400 service is to be provided, it will be carried in the corresponding ASN.1 protocol element as defined in X.400. When a service is required in the MMHS context and does not fit one of the X.400 EoS or the EoS does not exist, a new service is defined. New services will be carried in new protocol elements. The description in section two of this chapter includes the purpose of the new EoS, the policies and procedures for the use of that service, as well as the field, and possible values to be used. A reference to the ASN.1 definition of the field in Annex A is included. ASN.1 definitions that describe the structure of the MM information objects (i.e., the MM content type) are found in Annex A. When appropriate, the import feature of ASN.1 is used to point to those protocol definitions that are already defined in the international base standards; therefore, the imported protocol definitions are not duplicated herein.

203. Requirements for the support of the X.400 and MM EoS in the MMHS are included in this document. In general, if a service is to be made available in the MMHS then the protocol elements supporting that service are statically mandatory. This means implementations claiming to conform to the MMHS requirements shall implement the necessary protocol to support these services. Actual use on a particular message may be a user option, making the service, and therefore its supporting protocol elements, dynamically optional (i.e., the service and corresponding protocol elements are mandatory for an implementation). If the description of an EoS says it shall be supported as a user option, then there is a requirement that the user interface allow an originator to select that EoS and specify the information to be carried as part of that service. If the description says that information in support of an EoS is to be prominently displayed to the user, then this information is to be displayed without requiring the user to issue additional commands to find that information.

SECTION I
MM ELEMENTS OF SERVICE ADOPTED FROM IPMS

204. EoS are associated with the various functions provided by the MHS and in particular by the military interpretation of the MHS. The following is a list of these

EoS. Where there are no additional requirements imposed by military messaging over what is defined in X.400, a short description is included with the name of the EoS, the type of service (i.e., Message Transfer or Military Messaging), and a reference to its definition in X.400. If an EoS is said to be supported, this means it shall be implemented by all systems supporting MMHS. Support for an EoS is as defined in X.400, unless additional requirements are stated here. An example of additional requirements might include the specification for display to the user.

BASIC X.400 ELEMENTS OF SERVICE

205. The Basic X.400 EoS make use of the MTS and enable a user to send and receive MMs. All X.400 Basic EoS shall be supported.

a. Access Management

This MT element of service enables an MM-UA and an MTA to establish access and manage information associated with access establishment. This includes the ability to identify and validate the identity of the other. Secure Access Management will be used in the MMHS context. Actual security mechanisms used to provide secure access management will be defined by national policy. Strong authentication in the bind operation is mandatory; however, the mechanism is beyond the scope of this document. (See X.400 B.1, X.400 B.79.)

b. Content Type Indication

This MT element of service enables an originating UA to indicate the content type of each submitted message. Recipient UAs may be able to accept delivery of one or more content types. Examples of content type are the Interpersonal Messaging System (IPMS) contents generated by IPM UAs or the MM contents generated by MM-UAs. MMs will have a content type designated as P772 defined herein. The MM content type will be identified with an object identifier. There is no requirement to display a specific content type indicator to the user. In most cases, the content type will be obvious from the heading information that is present. (See X.400 B.12.)

c. Converted Indication

This MT element of service enables the MTS to indicate to each recipient UA (i.e., on per-recipient basis) that the MTS performed conversion on the EIT(s) within a delivered message. Security requirements and mechanisms may not allow conversion to take place within the MTS. However, messages entering the MMHS network from a gateway (e.g., a civilian X.400 domain, an ACP 127 tactical gateway) may carry the converted indication. If this indication is present on a message, it shall be displayed to the user. (See X.400 B.15.)

d. Delivery Time Stamp Indication

This MT element of service indicates to each recipient UA (i.e., on a per-recipient basis), the date and time at which the MTS delivered a message to the MS or UA. This time, carried as Coordinated Universal Time (UTC) time, will be used for audit logging and tracing purposes. This time stamp shall be displayed to the user. (See X.400 B.22.)

e. MM Identification

This MM element of service enables cooperating UAs to convey a globally unique identifier for each MM sent or received. This identifier is used in subsequent messages to identify the original MM. The *IPMIdentifier* will contain the *ORName* of the originator plus a printable string containing a serial number and the UTC time, specified down to the seconds, indicating the filing time of the message. This field shall always be present and shall be displayed to the user. (See X.400 B.37, and Annex A B.37 on page A-12.)

f. Message Identification

A unique identifier provided, as an MT element of service, by the MTS to a UA for each message submitted or delivered by the MTS. This identifier is used by UAs and the MTS to refer to a previously submitted message in connection with EoS such as delivery and non-delivery notification. This identifier will be used internally within the MMHS system. Unlike the MM Identification EoS, there is no requirement for users to see this field. This identifier will be used for audit logging and tracing purposes. (See X.400 B.41.)

g. Non-delivery Notification

This MT element of service allows the originator to ask, on a per-recipient basis, for the MTS to notify the originator if a submitted message was not delivered to the specified recipient UA(s). 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 (see 4.I.415), a non-delivery report will be returned to the originating UA by the MTS. 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. Receipt of the non-delivery report will then cause the UA to generate a non-delivery notification to alert the originator. The information conveyed in the report must be displayed to the originator in a manner that easily allows the user to identify the associated message. (See X.400 B.47.)

h. Original Encoded Information Types

This MT element of service enables the originating UA to indicate both to the MTS and the recipient UA the EITs of a message being submitted. The EITs

identify the various formats of the body parts of a message (e.g., IA5, G3-fax, etc.). See the Typed Body EoS below for display requirements. (See X.400 B.54.)

i. Submission Time Stamp Indication

This MT element of service enables the MTS to indicate to the originating UA and each recipient UA the date and time at which a message was submitted to the MTS. This time, carried in UTC time format, will be used for audit logging and tracing purposes. The user will be able to request this time be displayed for a given message. (See X.400 B.89.)

j. Typed Body

This MM element of service permits the nature and attributes of the body of the message to be conveyed along with the body. If the type of the body is important to provide context for the message, it must be displayed to the user. For example, the distinction between ADatP-3 messages and a particular national message text format (e.g., USMTF) might be important to the recipient. Indication of an IA5 body, however, may not be necessary. (See X.400 B.90.)

k. User/UA Capabilities Registration

This MT element of service enables a UA to indicate to its MTA, through registration, the 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 EIT(s) of messages it is willing to accept.

The MTA will not deliver to a UA any messages that either exceed or do not match the capabilities registered. Military messaging requires registration of security contexts be done by external trusted management means. The mechanisms to support registration may be defined by national or local policy. This functionality is also supplied by Directory Services defined in ACP 133. (See X.400 B.93, and Annex A B.93 on page A-13.)

OPTIONAL ELEMENTS OF SERVICE

206. If a service is optional in this ACP, it is up to the implementation whether the service is available to the user. If a service is said to be a user option, it shall be implemented, however, it will only be selected for a given message according to the

originator's requirements for a given message. Support for most of the applicable X.400 services on reception is mandated by the base standard.

a. Alternate Recipient Allowed

This MT element of service enables an originating UA to specify that the message being submitted can be redirected or delivered to an alternate recipient. Unless an originator specifically requests that an alternate recipient be disallowed (see 2.I.206.ah), all MMHS messages will indicate that an alternate recipient is allowed. User interface support for requesting selection or de-selection of this service is required. (See X.400 B.3.)

b. Alternate Recipient Assignment

This MT element of service enables a UA to be given the capability to have certain messages delivered to it for which there is not an exact match between the recipient OR Address attributes specified and the OR Address of the user. Such a UA is specified in terms of one or more OR Address attributes for which an exact match is required, and one or more attributes for which any value is acceptable. This service allows a message that would otherwise be undeliverable to be delivered to a "default mailbox" within the recipient MD. This could be used to guarantee delivery to a responsible entity in cases where a minimum set of OR Address attributes is specified for the intended recipient. Alternate Recipient Allowed would have to be selected by the originating UA to enable this service for a given message. See clause 4.I.419 for security issues related to the Alternate Recipient Allowed EoS. Due to security implications, the mechanisms for providing this service will be dependent on national policy. (See X.400 B.4.)

c. Authorizing Users Indication

This MM element of service allows the originator to indicate to the recipient the names of one or more persons who authorized the sending of the message. This field is used to convey information from originator to recipient only. There is no associated security mechanism for obtaining "proof of authorization". This service will be used to convey the OR Descriptor of the release authority for the message for information only. This service shall be supported as a user option. If this service is present, it shall be displayed to the recipient. (See X.400 B.5.)

d. Auto-forwarded Indication

This MM element of service allows a recipient to determine that the body of an incoming message contains a message that has been auto-forwarded. This is to distinguish it from a message that may contain a body part that was manually forwarded by its original recipient. The requirement to support this service on origination is conditional on other areas such as security policy, use of MS, etc. and will be determined by local or national policy. If auto-forwarding is supported then, this indication shall be supported on origination.

However, if the indication is present, it shall be displayed to the recipient. (See X.400 B.6.)

e. Blind Copy Recipient Indication

This MM element of service enables the originator to provide the OR Descriptor of one or more additional intended recipients (i.e., on a per-recipient basis) of the message being sent. These names are not disclosed to the primary, copy or other blind copy recipients. This service shall be supported as a user option. This service can be used to keep some recipient names and addresses hidden from some of the other recipients. This service, when supported, will be a user option and 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 message shall be submitted to the MTS for open recipients (primary and copy recipients) and for each blind copy recipient. The *IPMIdentifier* of the blind copy message(s) shall be identical to the *IPMIdentifier* of the message submitted to the MTS for the primary and copy recipients. If the recipient is a blind copy recipient, an indication shall be prominently displayed to the user. (See X.400 B.8.)

f. Body Part Encryption Indication

This MM element of service allows the originator to indicate to the recipient that a particular body part of the message being sent has been encrypted. The methods for encrypting and decrypting that body part are outside the scope of X.400 and this ACP. Bilateral agreements concerning the algorithm used for encryption and decryption must be agreed upon by the originator and recipient(s) before this service is used. Support for originating the encrypted indication shall be optional. However, if the indication is present, it shall be displayed to the recipient. (See X.400 B.9.)

g. Conversion Prohibition

This MT element of service enables an originating UA to instruct the MTS that implicit conversion of EIT(s) should not be performed on this message. Support of this service is mandatory in cases where conversion could impact security for a given message. If security services are used such that a particular message is encrypted, the MTS is not likely to have the information necessary to perform implicit conversion. Enabling the Conversion Prohibition EoS is an added precaution, and shall be supported as a user option. If both the Conversion Prohibition EoS and the Conversion Prohibition in Case of Loss of Information EoS (see 2.I.206.h) are requested then Conversion Prohibition takes precedence and no conversion will be permitted unless the Explicit Conversion EoS (see 2.I.206.r) was also requested. Request of Explicit Conversion along with either form of

conversion prohibition is inconsistent, and should generally be disallowed by user interface. (See X.400 B.13.)

h. Conversion Prohibition in Case of Loss of Information

This MT element of service enables an originating UA to instruct the MTS that implicit conversion of encoded information type(s) should not be performed on this message, if such conversion(s) would result in loss of information. The specifics of what constitutes loss of information are discussed in detail in X.408. If both the Conversion Prohibition EoS (see 2.I.206.g) and the Conversion Prohibition in Case of Loss of Information EoS are requested then Conversion Prohibition takes precedence and no conversion will be permitted unless the Explicit Conversion EoS (see 2.I.206.r) was also requested. Request of Explicit Conversion along with either form of conversion prohibition is inconsistent, and should generally be disallowed by user interface. This service shall be supported as a user option when the ability to request Explicit Conversion is also supported. Selection of conversion prohibition may stop delivery of a message to a recipient who is located beyond an interface point (e.g., a recipient in a tactical environment). See 4.I.417 for additional security implications. (See X.400 B.14.)

i. Cross-referencing Indication

This MM 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 UA, for example, to retrieve from storage a copy of the referenced messages. This service will also be used to indicate partial corrections to earlier messages. This service shall be supported as a user option. If present, this indication shall be displayed to the user. If the originator requires a label for easy reference to multiple cross references in the text of this message, or if other types of referenced material (e.g., a document, ACP 127 message, etc.) are used, then a reference list will be included in the body of the message. In this case the originator will include the word "Reference" and a list of the references labeling each with a shorthand label (e.g., A, B, C, etc) at the top of the body requiring the references. (See 4.I.418, and X.400 B.18.)

j. Deferred Delivery

This MT element of service enables an originating UA to instruct the MTS that a message being submitted shall be delivered no sooner than a specified date and time. This would conflict with the speed of service requirements if the clock starts from the time a message is submitted to the MTS. Therefore, if Deferred Delivery is requested, time for speed of service requirements starts when the message leaves the originating MTA, rather than starting at submission time. Support for this service is optional. When this service is requested, it must be logged for audit and tracing purposes. (See X.400 B.19.)

k. Deferred Delivery Cancellation

This MT element of service enables an originating UA to instruct the MTS to cancel a previously submitted message that employed the Deferred Delivery EoS. The cancellation attempt may not always succeed. If the cancellation fails, other methods such as the Obsoleting Indication EoS (see 2.I.206.ab) may be used to nullify the message. National supplements may choose to require that messages be held at the originating MTA in order to better support this service. Support for Deferred Delivery Cancellation is conditional. If Deferred Delivery is supported, Deferred Delivery Cancellation shall be supported. (See X.400 B.20.)

l. Delivery Notification

This MT element of service enables an originating UA to request that the originating UA be explicitly notified when a submitted message has been successfully delivered to a recipient UA or Access Unit (AU). This notification is conveyed by the delivery report. The delivery report is related to the submitted message by means of the message identifier and includes the date and time of delivery. Receipt of a delivery report at the originating UA results in the generation of a delivery notification to the originator. In the case of multi-destination messages, this service shall be selectable on a per-recipient basis. In the case of recipients specified by an Address List (AL), the policies of the AL will determine whether the notifications are returned to the originator, the owner of the AL, or both. This notice is for information only. It does not imply the message has been seen by the recipient, only that it has left the MTS. If other means of message acknowledgment have been requested (e.g., Receipt Notification Requested or Reply Requested) the delivery notification should not be requested (see 4.I.405 and 4.I.406). The ability to request return of delivery notifications shall be supported as a user option. The ability to return a delivery report when delivery notification is requested shall be supported. (See X.400 B.21.)

m. Designation of Recipient by Directory Name

This MT element of service enables an originating UA to use, on a per-recipient basis, a directory name in place of an individual recipient's OR Address. This implies support of a Directory. The directory name must be translated to an OR Address for delivery to take place within the MTS. However, the directory lookup may take place at the MTA rather than at the UA level. This service is optional. If support of this service is claimed the point at which the name is translated to an OR Address may be defined by national policy or international agreement. Support for this service means if a directory name is present in a message it can be displayed to the recipient. It does not imply all originators will be able to specify a directory name for all recipients. Not all users will necessarily be assigned directory names. Unless an establishment of a global directory system is agreed to by all participating

management domains, originators may only be able to specify directory names for those recipients that are registered in the directory maintained by the originating MD. Exceptions may be possible by bilateral agreement. (See X.400 B.24.)

n. Disclosure of Other Recipients

This MT element of service enables the originating UA to instruct the MTS to disclose the OR Names of all other recipients of a multi-recipient message to each recipient UA, upon delivery of the message. The OR Names disclosed are as supplied by the originating UA or the results from AL expansion, and are derived from the P1 delivery envelope of the message. This information is provided to the UA. Not all user interfaces will display recipient information that was not contained in the content recipient information. Recipient information that the originator wants to be displayed to the recipient should be carried in the content heading of the message. This service is optional. (See X.400B.25.)

o. DL Expansion History Indication

This MT element of service provides to a recipient, upon delivery, information about the DL(s) that brought the message to this recipient. This service shall be supported in the MTS in order to protect against potential nested DL looping. On reception, the information must be correctly handled by the UA if it is present, and shall be able to be displayed to the user. (See X.400 B.26.)

p. DL Expansion Prohibited

This MT element of service allows an originating user to specify that if any of the recipient names can directly, or by reassignment, refer to a DL, then no expansion shall occur. Instead, a non-delivery notification will be returned to the originating UA. Reassignment refers to any means of redirection (e.g., alternate recipient or redirection of incoming messages). In a security conscious environment, originators should know if the addresses they use are DLs, although this might not always be the case if recipient reassignment can take place. This service shall be supported as a user option. (See X.400 B.27.)

q. Expiry Date Indication

This MM 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. Use of this service is a user option. If this indication is present, it shall be displayed to the recipient(s) to indicate the time after which this message should no longer be acted upon. It is left to the discretion of the recipient whether or not the message is discarded. Messages

containing an Expiry date indication will not be automatically deleted from a recipient's message storage when the expiration time has passed. This EoS procedurally excludes auto-discard and deletion actions (see 3.II.314.a and 3.III.318.a). Instead, the user interface will display the expiration date and time indicated to the recipient when the message is accessed. It is the responsibility of the recipient to discard the message after the expiration time. (See X.400 B.29.)

r. Explicit Conversion

This MT element of service enables an originating UA to request, on a per-recipient basis, that the MTS perform a specified EIT conversion, such as required when interworking between different Telematic Services. In a secure environment, the information necessary to perform conversion is unlikely to be available to the MTS. Therefore, support for this service is optional in the MMHS environment. Request of Explicit Conversion EoS is inconsistent with use of either the Conversion Prohibition EoS (see 2.I.206.g) or the Conversion Prohibition in Case of Loss of Information EoS (see 2.I.206.h), and should generally be disallowed by user interface. (See X.400 B.30.)

s. Forwarded MM Indication

This MM 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 several body parts of various types. An externally defined body part type called *mm-message-body-part* is defined in Annex A. Support for this body part is mandatory. An MM may contain both Forwarded-MM and Forwarded-IP messages. (See X.400 B.31.)

t. Grade of Delivery Selection

This MT element of service enables an originating UA to request that transfer through the MTS take place at a selected priority. The time periods defined for each grade of delivery must be specified by policy. The delivery time requirements are goals. National or other policy must define the level of assurance to meet the goals. (See 4.I.415.) An indication of the grade selected is sent to the recipient UA with the delivered message. The supporting protocol element, *priority*, is dynamically mandatory. Support for this service is mandatory. Grade of Delivery will always be used in the MMHS because the value of the *priority* field will be derived from the Primary Precedence selection. If a Message Protocol Data Unit (MPDU) has no primary recipients, and therefore no Primary Precedence, the *priority* value will be derived from the Copy Precedence. In the case of an MPDU with neither primary nor copy recipients (i.e., a Blind Copy recipient's copy of a message), the *priority* value will be NON-URGENT. The Grade of Delivery shall not be displayed to the recipient, because they will get more information by seeing the Primary and Copy Precedence. (See X.400 B.32.)

u. Hold for Delivery

This MT element of service enables a recipient UA to request that the MTS hold its messages and returning notifications of delivery until a later time. The UA indicates to the MTS when it is unavailable to take delivery of messages and notifications, and also, when it is again ready to accept delivery from the MTS. The MTS can indicate to the UA that messages are waiting due to the criteria the UA established for holding messages. Responsibility for the management of this element of service lies with the recipient MTA. Criteria for requesting that messages be held are:

- EIT,
- Content type,
- Maximum content length, and
- Priority.

This service differs from the function of the MS, providing temporary storage only. Delivery reports are not returned until after a message is transferred to the recipient UA. If the maximum delivery time expires while a message is being held it will be Non-delivered. Support for this service is optional. The requirement to utilize this service will depend on specific configuration employed, which may be dictated by national policy. When Hold for Delivery is supported, there must be a method for ensuring delivery to a backup recipient all messages with a *priority* value of URGENT (i.e., FLASH and OVERRIDE precedence) in order to ensure timely delivery. Possible mechanisms for achieving this backup delivery include certain uses of Auto-forwarding, Redirection of Incoming Messages, or Originator Requested Alternate Recipient. (See X.400 B.33.)

v. Incomplete Copy Indication

This MM element of service allows an originator to indicate that this message is an incomplete copy of a message with the same *IPMIdentifier* in that one or more body parts or heading fields of the original message are absent. This service might be useful in limited bandwidth environments. For example if a tactical message is defined with limited heading fields at the gateway between the restricted and standard environments, the message could be stripped to the tactical fields only and incomplete copy indicated. Another use of this indication might be with a multi-body part message where only some of the body part types are acceptable to a given UA. Use of this service, and determination of which fields can be left out, needs to be clarified by national or local policy. This service shall be supported as a user option. If this indication is present, it shall be displayed to the user. (See X.400 B.36.)

w. Language Indication

This MM element of service enables an originating UA to indicate the language type(s) of a submitted message. This service shall be supported as a user option. If this indication is present, it shall be displayed to the user. (See X.400 B.38.)

x. Latest Delivery Designation

This MT element of service enables an originating UA to specify the latest time by which the message is to be delivered. If the MTS cannot deliver by the time specified, the message is canceled and a non-delivery report returned. In a multi-recipient message, this will not negate deliveries that may already have occurred. In an instance of the user invoking the latest delivery designation EoS, the UA shall display a warning to remind the user that use of the service may result in non-delivery of a message. This service shall be supported as a user option (See X.400 B.39.)

y. Multi-destination Delivery

This MT element of service allows an originating UA to specify that a message being submitted is to be delivered to more than one recipient UA. This does not imply simultaneous delivery to all specified recipient UAs. This service shall be supported as a user option. (See X.400 B.45.)

z. Multi-part Body

This MM 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. This service shall be supported as a user option. (See X.400 B.46.)

(1) Transmission of ADatP3 formatted messages shall use the *adatp3-body-part* type. This body part type allows the user to convey formatted message data in either a linear (line-oriented) or columnar (set-oriented) format in accordance with Allied Data Publication 3 (ADatP3). It will also carry an optional message sequence reference number in the body part's parameters. Support of the *adatp3-body-part* is mandatory.

(2) The *forwarded-CSP-Message-Body-Part* body part conveys the entire received content as a structured data element. Additionally, it allows the forwarder to include the majority of the message delivery envelope (minus the *message-delivery-identifier field).* This body part is intended to support cases where a CSP message must be forwarded

intact to a new ACP 123 recipient (e.g., auto-forwarding by a MS). Use of this body part type is deprecated.

(3) Any document exchange between users shall use the *file-transfer-body-part* type. The parameters of this body part shall use the external document's object identifiers. The parameters of the body part shall be carried in the *document-type-name* subfield of the *contents-type Parameter* to describe the data that is being transferred. These object identifiers may be found in the Electronic Mail Association (EMA) Message Attachment Work Group (MAWG) Feasibility Project Guide. Support for the *file-transfer-body-part* is mandatory.

a. Transmission of Data Pattern traffic using ACP 123 shall use the *file-transfer-body-part* type. The Data Pattern messages shall be carried as an external data type described by the *id-acp123us-filetransfer-datapattern* object identifier. The object identifier shall be present in the *document-type-name* subfield within the *contents-type* parameter. The data shall be carried in the body part as an octet string and each body part shall contain only one octet string. The *Parameter* field, if present in the *document-type-name,* shall be used to convey the record count as an integer with a default of zero. Support of this *file-transfer-body-part* external data type is optional.

b. Transmission of Electronic Data Interchange (EDI) transaction sets using ACP 123 shall use the *file-transfer-body-part* type. The EDI transactions shall be carried as an external data type described by X.435-defined object identifiers listed below. The cited object identifiers shall be present in the *document-type-name* subfield within the *contents-type* parameter. The data shall be carried in the body part as an octet string and each body part shall contain only one octet string. The *Parameter* field, if present in the *document-type-name,* shall be ignored. Support of these *file-transfer-body-part* external data type is optional.

- id-bp-edifact-ISO646
- id-bp-edifact-T61
- id-bp-edifact-octet
- id-bp-ansiX12-T61
- id-bp-ansiX12-octet
- id-bp-ansiX12-ebcdic
- id-bp-untdi-ISO646
- id-bp-untdi-T61

- id-bp-private-octet
- id-bp-undefined-octet

aa. Non-receipt Notification Request Indication

This MM element of service allows the originator to ask, on a per-recipient basis, for notification if the message is deemed unreceivable. Non-receipt notification (NRN) message would be issued on any of the following events:

- The recipient's UA auto-forwards the message to another user,
- The recipient's UA discards the message prior to receipt,
- The recipient's subscription is terminated before receipt of the message.

The recipient's failure to access the message for a long period of time does not constitute non-receipt. Support for requesting NRN shall be a user option. Support for the ability to generate an NRN shall be available if any of the conditions for non-receipt can occur. Which of these events caused non-receipt is conveyed to the originator in the NRN. If the implemented system supports Auto-forwarding, it shall also be able to generate NRNs. Likewise if an implementation automatically deletes messages that have expired or been obsoleted or can terminate a user's UA (mail service) with delivered but not received messages, then it shall also support generation of NRNs. (See X.400 B.48.)

ab. Obsoleting Indication

This MM element of service allows the originator to indicate to the recipient that one or more previously sent messages are obsolete. This service will be used to provide a way for originators to cancel previously transmitted messages. Messages containing an obsoleted indication will not automatically cause the deletion of the obsoleted message from a recipient's message storage. This EoS procedurally excludes the auto-discard and the auto-deletion actions (see 3.II.314.a and 3.III.318.a). Instead, when the original message is accessed, the user interface will display information advising the recipient that the message is obsolete. It is the recipient's responsibility to discard the obsoleted message if it is still in the current message storage of the MM-UA. This service shall be supported as a user option, but if this service is supported automatic correlation of the obsoleted message and the obsoleting message shall be performed. Any local processing used to facilitate automated correlation of these messages is beyond the scope of this ACP. If this indication is present it shall be displayed to the user. (See X.400 B.52.)

ac. Originator Indication

The intent of this MM element of service is to convey to the recipient the identity of the originator in a user-friendly way. In contrast, the MTS provides the recipient UA the actual OR Address and directory name, if present, of the originator. Within the MMHS, when the *originator* field is present, it should include the directory name (if one is available) in the *formal-name* sub-field. This additional requirement is to encourage the use of a user-friendly method of identifying the originator. The *free-form-name* or *telephone-number* sub-fields may also be present. This service shall be supported. When this indication is present it shall be displayed to the user. (See X.400 B.55.)

ad. Originator Requested Alternate Recipient

This MT element of service enables the originating UA to specify, for each intended recipient, one alternate recipient to whom the MTS can deliver the message, if delivery to the intended recipient is not possible. If the intended recipient has requested the Redirection of Incoming Messages EoS, and the originating UA has requested that redirection be allowed, the system first tries to redirect the message to the recipient's designated alternate. If this fails, the system then attempts to deliver the message to the originator's designated alternate recipient. This service, like Alternate Recipient Assignment or Redirection of Incoming Messages, may impact security mechanisms. Security information to enable delivery to the specified alternate must be included in the message being transmitted. The presence of this service is required in any implementation, but the way in which alternate recipients are used shall be determined by security or local policy. If the message is delivered to an alternate recipient, the intended recipient shall be displayed to the user. (See X.400 B.56.)

ae. Prevention of Non-delivery Notification

This MT element of service enables an originating UA to instruct the MTS not to return a non-delivery report to the originating UA in the event that the message being submitted is judged undeliverable. This can be requested on a per-recipient basis. This service does not prevent a non-delivery report from being returned to the originating MTA. The service thereby prevents a Non-delivery Notification (NDN) from being presented to the originating user. This service shall be a user option for some precedence levels. Precedence levels of IMMEDIATE and above require that any associated NDNs be returned to the originator. When this service is requested it will be logged for audit and tracing purposes. (See X.400 B.61.)

af. Primary and Copy Recipients Indication

This MM element of service allows the originator to provide the names of users or ALs who are the intended primary recipients and the intended copy

recipients of the message. It is intended to enable the recipient to determine the category in which each of the specified recipients was placed. An indication of the primary versus copy designation of the recipient shall be displayed to the user. This service supports the identification of Action versus Information recipients and shall be supported. Primary recipients have responsibility to act upon the delivered message, while Copy recipients have no explicit action responsibility and are sent the message merely for information purposes. When a recipient views a message, the indication of whether that user is categorized as Primary or Copy shall be prominently displayed. It may be necessary for the user to take some action to see the entire list of all Primary and Copy recipients. (See X.400 B.62, and Annex A B.62 on page A-12.)

ag. Receipt Notification Request Indication

This MM element of service allows the originator to ask, on a per-recipient basis, for notification when a particular message is received. X.400 allows a recipient UA to respond to the Receipt Notification (RN) request either automatically or by manual instruction of the user. In addition, it is permissible for a recipient UA to allow the user to ignore the request for RN. In the MMS the RN will not be generated until the recipient has viewed the entire message, indicating acceptance of responsibility. In cases where multiple body parts are present the first text body part, which should contain an overview of the entire body, must be viewed to constitute receipt. (See 4.I.414.b.) This service shall be supported as a user option. If an RN has been requested, this shall be prominently displayed to the user and the recipient will be required to honor the request to return a RN unless a more explicit response such as a reply is sent in its place (see 4.I.405 and 4.I.406). This EoS procedurally excludes the use of MMS auto-acknowledgments (see 3.I.314.c). Originators who generate messages for which a receipt is critical shall use the S/MIME Non-repudiation of Receipt service (see Annex B section 7.7 on page B-9). (See X.400 B.67.)

ah. Redirection Disallowed by Originator

When the recipient has requested the Redirection of Incoming Messages EoS, this MT element of service enables an originating UA to instruct the MTS that redirection should not be applied to this particular submitted message. Support for this service is mandatory because it could impact the security of a given message. This service shall be supported as a user option. (See X.400 B.68.)

ai. Redirection of Incoming Messages

This MT element of service enables a UA to instruct the MTS to redirect incoming messages addressed to it, to another UA or to an AL, for a specified period of time, or until revoked. Redirection takes place before delivery to the

intended recipient. It is therefore distinct from the Auto-forwarded Indication element of service, where auto-forwarding takes place after delivery. When security provisions are in force, the MTS may examine security labels in order to determine whether redirection will take place, and to determine different alternate recipients for different incoming messages. Redirection based on other criteria in the message envelope, such as the *priority field*, may also be required by national or local policy. Use of this service may be impacted by security policy. The Directory service may be used to provide support for this service by allowing originators to include necessary keying information in case the message is redirected. The presence of this service is required in any implementation, but the way in which redirection is used shall be determined by security or local policy. (See X.400 B.69.)

aj. Reply Request Indication

This MM element of service allows the originator to request, on a per-recipient basis, that a recipient send a message in reply to the 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. MMHS uses this service for the purpose of military acknowledgment. Where acknowledgment is defined as "a communication indicating that the message to which it refers has been received and the purpose understood by the addressee." Acknowledgment should not be confused with reply, but a prompt reply may save a subsequent request for acknowledgment. In addition, Reply Request service should not be confused with Delivery Notification and Receipt Notification EoS. The Delivery Notification and Receipt Notification EoS are used for reporting message transmittal steps and not to convey proof that the recipient has understood the message. When a Reply Request Indication is received, the corresponding Reply message indicates whether the original message has been both received and understood. This service shall be supported as a user option. When this indication is present, it shall be prominently displayed to the user. Additionally, if the supporting protocol elements *reply-time* and *reply-recipients* are present, they shall also be displayed. Note that Blind Copy Recipients should consider careful to whom a reply is sent to, so that the meaning of the Blind Copy Recipient Indication EoS is preserved. (See X.400 B.72, and Annex A B.72 on page A-13.)

ak. Replying MM Indication

This MM element of service allows the originator of a message to indicate to the recipients that the message is being sent in reply to another message. The recipients of the reply receive it as a regular message, together with an indication of the message to which it is a reply. This service shall be supported as a user option. The use of this indication is encouraged when a reply was requested. When this indication is present, it shall be displayed to the user. (See X.400 B.73.)

al. Requested Preferred Delivery Method

This MT element of service allows a user to request, on a per-recipient basis, the preference of method or methods of delivery. Non-delivery results when preference(s) cannot be satisfied. No requirement has been identified for this service. Its support is optional. (See X.400 B.76.)

am. Subject Indication

This MM element of service allows the originator to indicate to the recipient(s) a user specified short description of the message. This is different from the standardized codes to be carried in the Subject Indicator Code extension service. This service shall be supported and shall be displayed to the user. The *subject* field will always be used, but it should be kept short, concise and readable. (See X.400 B.88.)

an. Use of Distribution List

This MT element of service enables an originating UA to specify, on a per-recipient basis, a Distribution List (DL) in place of all the individual recipients (users or nested DLs) mentioned therein. The MTS will add the members of the list to the recipients of the message 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 on security requirements. National policy may also dictate support of the military extension Use of Address List EoS instead of DLs, and the relationship with the Exempted Addresses EoS. (See X.400 B.92.)

OPTIONAL ELEMENTS OF SERVICE NOT USED IN MMHS

207. The following EoS are provided as part of the underlying definition of MMHS in Annex A; however, they are not required for ACP 123 use. These EoS and protocol elements may, however, be used to support nationally specific messaging characteristics within a host nation. These EoS shall not be conveyed internationally except by bilateral agreement. If the protocol elements to support these services are present in international messages they can be ignored. These EoS should not be prompted for or displayed at the user interface, except where it is necessary to support specifically required national or local messaging features. They are included in the P772 content definition in order to retain harmonization with STANAG 4406.

a. Implicit Conversion

This MT element of service enables a recipient UA to have the MTS perform necessary conversion(s) on a message prior to delivery. Conversion refers to converting the EIT of one or more body parts of the message to another EIT. Conversion in X.400 is performed by the MTS. This service is not explicitly

requested on a message by either the originator or the recipient. If security services are used such that the message is carried encrypted, the MTS is not likely to have the information necessary to perform implicit conversion. (See X.400 B.34.)

b. Importance Indication

This MM element of service allows the originator to indicate to the recipient an assessment of the relative importance of the message being sent. Three levels of importance are defined: LOW, NORMAL, and HIGH. This field is used to carry originator to recipient information only. The military extensions of Primary Precedence and Copy Precedence will be used to convey at least six different levels of importance for Action versus Information recipients, thus providing more information than this service. Therefore this service is redundant and its use might cause confusion to recipients. The importance field shall not be originated by or displayed to the user. (See X.400 B.35.)

c. Probe

This MT element of service enables a UA to establish, before submission, whether a particular message could be delivered. This service includes the capability of checking whether the content size, content type, or EITs would render the message undeliverable. For ALs, the probe merely indicates whether the originator has the right to submit messages to the AL. The invocation of this service from an MM-UA is prohibited due to security considerations. Interface points to the MMHS shall refuse the *Probe Transfer* operation. If one is detected it shall be logged and ignored. A Non-Delivery Notification shall not be returned to the originator. (See X.400 B.63.)

d. Restricted Delivery

This MT element of service enables a recipient UA to indicate to the MTS that it is not prepared to accept delivery of messages from certain originating UAs or DLs. No requirement has been identified for this service. Additionally, no protocol to support this service has been defined in X.400. (See X.400 B.77.)

e. Return of Content

This MT element of service enables an originating UA to request that the content of a submitted message be returned with any non-delivery notification. This service shall not be used as it could impact performance on the network. It is the originator's responsibility to retain a copy of a message for a required period of time or until assurance of delivery. Non-delivery Notifications can be correlated with the original message, by the Message Identification. Therefore there is no requirement to support the Return of Content element of service. (See X.400 B.78.)

f. Sensitivity Indication

This MM element of service allows the originator of a message to specify guidelines for the relative sensitivity of the message upon its receipt. This service is used to carry information from originator to recipient only. The standards do not address the actions or events to be taken based on the different values that can be carried by this service. The use of this service may conflict with the Message Security Label, which conveys more information. The sensitivity indication shall be disregarded by the MM-UA. The sensitivity field shall not be originated by or displayed to the user. (See X.400 B.80.)

g. Security Information Labels

This element of service allows the originator of a military message to convey an indication of the sensitivity of the message, and individual parts of the message to all recipients of the message. The indication takes the form of security labels, which are assigned to the whole military message content, and potentially to the MM header and individual MM body parts. Implementation of this EoS is strictly optional, and its use has been deprecated. (See Annex A B.120 on page A-19.)

PHYSICAL DELIVERY ELEMENTS OF SERVICE

208. The Physical Delivery EoS are used when interfacing to a Physical Delivery Service (PDS) such as a national postal service. All ACP 123 users will be served by MM-UAs. If a message is printed for local distribution, this will occur after message delivery has occurred. There may be a requirement for some nations to support a commercial refile capability and therefore the support of a Physical Delivery Access Unit (PDAU). Therefore, the EoS to support interworking with a PDS are optional in ACP 123. Support for origination of the addressing attributes to indicate Physical Delivery recipients of messages is also optional.

SECURITY ELEMENTS OF SERVICE

209. Support of the security EoS defined by the X.400 Civil standards is optional. The security services required within the ACP 123 environment are identified in section 4.II.

MESSAGE STORE ELEMENTS OF SERVICE

210. The MS EoS are associated with the optional use of an X.400 MS. Support for the MS EoS is dependent on use of an MS and does not impact interoperability with configurations without an MS. Support of the MS access protocol (i.e., P7) across international boundaries is not required by ACP 123. This is due to the technical difficulty associated with de-coupling the MS design from that of the user interface of the UA. Further discussion of the use of MSs will be found in section 3.III and paragraph 4.I.419.d.

a. MS Register

This element of service allows a user of an MS to register various information with it in order to modify aspects of its behavior. Information that can be registered includes the performance of automatic actions, the default set of information retrieved by the Stored Message Fetching and Stored Message Listing EoS, and the credentials used by the MS to authenticate the MS-user (i.e., the UA). If an MS is available this service is mandatory. (See X.400 B.95.)

b. Stored Message Alert

This element of service allows a user of an MS to register relevant sets of criteria that can cause an alert to be generated to the user when a message arrives at the MS satisfying the selected criteria. Criteria can be any attributes available to the MS. These could include the *priority* field, *originator* field, etc. The alert will take place if the user is connected and on-line with the MS when the message triggering an alert arrives, or the MS can use alternative means to inform the user. If a recipient who may receive time critical messages has a MS, then the associated MS shall support this service. (See X.400 B.82.)

c. Stored Message Auto-forward

This element of service allows a user of the MS to register requests that the MS auto-forward selected messages that are delivered to it. Criteria for selection can be chosen from the attributes available in the MS. One text per selection criteria can also be specified to be included with each auto-forwarded message. Support for this service may be impacted by security policy. However if a recipient who may be unavailable for periods of time has a MS, then support for this service shall be available. (See X.400 B.83.)

d. Stored Message Deletion

This element of service enables a recipient UA to delete certain of its messages from the MS. Messages that have not been listed cannot be deleted. If an MS is provided, then this service is mandatory. (See X.400 B.84.)

e. Stored Message Fetching

This element of service enables a recipient UA to fetch a message or portion of a message from the MS. Messages, or message portions, can be fetched based on the same criteria that can be used for listing stored messages. If an MS is provided, then this service is mandatory. (See X.400 B.85.)

f. Stored Message Listing

This element of service provides a recipient UA with a list of information about certain of its messages stored in the MS. The information comprises selected attributes from a message's envelope and content and others added by the MS. If an MS is provided, then this service is mandatory. (See X.400 B.86.)

g. Stored Message Summary

This element of service provides a recipient UA with a count of the number of messages satisfying specified criteria based on one or more attributes of the

message stored in the MS. If an MS is provided, then this service is mandatory. (See X.400 B.87.)

SECTION II
ADDITIONAL MILITARY ELEMENTS OF SERVICE

211. The additional Military EoS provide services required within the MMHS context that are not found in the civilian X.400. ASN.1 for the new protocol elements that will support these services is defined in Annex A.

MILITARY ELEMENTS OF SERVICE

212. Support for the following Military EoS is mandatory. If these services are present in a message, the information contained shall be displayed to the user.

a. Primary Precedence

This element of service enables an originating MM-UA to convey the military precedence level of a message in the MM content type's heading for a primary recipient. This service is provided not only as information from originator to recipient, but also is used to automatically select the MTS Grade of Delivery. This service is supported by the military heading extension *primary precedence.* (See Annex A B.101 on page A-13.) The six defined levels of precedence (see 4.I.404.a for semantic definitions) are mapped to only three levels of Grade of Delivery. Military precedence is mapped to the MTS priority protocol element as follows:

Military Precedence	**MT Priority**
DEFERRED (0)	NON-URGENT
ROUTINE (1)	NON-URGENT
PRIORITY (2)	NORMAL
IMMEDIATE (3)	NORMAL
FLASH (4)	URGENT
OVERRIDE (5)	URGENT

The delivery time requirements will be assigned in such a way as to meet or exceed current requirements for the transfer of messages at each military precedence level. The actual precedence assigned for Primary and Copy recipients will be conveyed from originator to recipient and shall be displayed to the recipient. (See Annex A B.101 on page A-13.) The Primary Precedence level shall be prominently displayed for each primary recipient user. Values 16 through 31 are reserved for national use. National policy will mandate these values and the mapping to the Grade of Delivery.

b. Copy Precedence

This element of service enables an originating MM-UA to convey the additional precedence of a message in the MM content type's heading for a Copy recipient. The Copy Precedence has the same range of values as the Primary Precedence. The value of the Copy Precedence assigned shall be the same or a lower value than the Primary Precedence of the same message. This service is provided for conveying information from originator to recipient only. This service is a user option, however if there are Copy Recipients in a message, Copy Precedence will be selected if it is different from the Primary Precedence. If present, the Copy Precedence shall be displayed to the user. (See Annex A B.102 on page A-14.) This service is supported by the military heading extension *copy precedence.* The Copy Precedence level shall be prominently displayed for each Copy recipient user.

c. Message Type

This element of service enables originating MM-UAs to distinguish messages that relate to a specific exercise, operation, drill, or project. (See Annex A B.103 on page A-14.) The information carried in support of this EoS is an integer identifying the type of the message and an optional printable string specifying the name of exercise, operation, project or drill. This service is carried by the military heading extension *message-type*. This service is a user option. If present, the Message Type shall be prominently displayed to the user.

(1) The value *exercise* (0) shall be assigned to all formally released military messages sent for training exercises, command post exercises, tactical exercises and maneuvers conducted in the interest of training and readiness. A printable string, assigned by a proper authority, shall be included in the identifier field to distinguish a specific exercise scenario, or to convey any additional information that is specific to the exercise. The organization conducting the exercise shall include the appropriate instructions for identifying exercise messages in the directive for the conduct of the exercise in order to preclude alarming non-participants.

(2) The value *operation* (1) may be assigned to formally released military messages pertaining to a specific military operation. An "operation" is a coordinated action by one or more of the Services that generally involves mobilization of armed forces. If the Message Type value is used, a printable string identifier shall in the identifier field to distinguish the specific operation in question, and convey any additional information that is specific to the operation.

(3) The value *project* (2) may be assigned to formally released military messages pertaining to a specific support activity project. A

"project" is a logistic, programmatic, or acquisition activity that generally does not involve mobilization of armed forces. If this Message Type value is used, a printable string identifier shall be included in the *identifier* field to distinguish the specific project in question, and convey any additional information that is specific to the project.

(4) The value *drill* (3) shall be assigned to all formally released military messages pertaining to a specific military drill. A printable string identifier may be included in the *identifier* field to distinguish the specific drill in question, and convey any additional information that is specific to the drill.

(5) Values in the range of 128 to 255 are not defined and may be used as defined by national policy or as agreed bilaterally.

d. Exempted Addresses

This element of service is used to convey the names of members of an AL that the originator has specified are to be excluded from receiving the message. An AL could be carried either by the *address-list-indicator* heading field, as an X.400 DL, or as a list name on the *primary-recipients* or *copy-recipients* field. Exclusion is provided at the point of AL expansion (see clause 4.III.433.a.) The names or addresses of exempted list members is also conveyed to the remaining recipients and shall be displayed to the user. There is no guarantee that the exempted addresses will not receive the message as the result of redirection, DL expansion, etc. (See Annex A B.105 on page A-15.) This service is carried by the military heading extension *exempted-address.*

e. Extended Authorization Info

This element of service enables the originating MM-UA to indicate to a recipient MM-UA the date and time when the message was released as a Date-Time Group (DTG). Depending upon national requirements, the DTG may indicate either the date and time when the message was officially released by the releasing officer or the date and time when the message was submitted to the communications facility for transmission. (See Annex A B.106 on page A-15.) The information for this service is carried in the military heading extension *extended-authorisation-info*. This information shall be automatically added to all officially released messages as a default; however, the originator shall have ability to override the information in this extension. If this information is present upon reception, it shall be displayed to the user.

f. Distribution Code

This element of service enables the originating MM-UA to give distribution information to a recipient MM-UA. The recipient MM-UA can use this information to perform distribution of the message to one or more persons or staff cells. This service contains two components, the Subject Indicator Code (SIC) and a Distribution Code, each of which is optional. The Distribution Code allows for future definitions of distribution criteria for either national or Allied use. Any number of codes may be specified. The assignment of the Distribution Code can be privately defined or may be subject to future standardization. SICs are published, nested codes that provide information for message distribution after delivery to the recipient organization. For example the NATO Subject Indicator System (NASIS), defined in APP-3, is one source for SICs. (See Annex A B.107 on page A-15.) The information for this service is carried in the military heading extension *distribution-codes*. This information is a user option on origination, but shall be displayed to the user if present on reception.

g. Message Instructions

This element of service enables the originating MM-UA to indicate to the recipient MM-UAs that message instructions accompany the message. (Message instructions are also called remarks). It may be used to carry Operating Signals specified in ACP 131 and related national publications. Message Instructions are not visible within the MTS and therefore cannot be acted upon by the MMHS. They are used for informational purposes at the end points. This information, if present, shall be displayed to the user. (See Annex A B.109 on page A-16.) This service is a user option. The information for this service is carried in the military heading extension *message-instructions.*

(1) For each message sent, the originator shall determine if any of the message recipients have been placed under Minimize conditions. The originating user shall be prompted to consider omitting any recipient for whom Minimize is indicated. If the user chooses to include such a recipient despite the Minimize condition, then "MINIMZE CONSIDERED" shall be included in the Message Instructions EoS. If this instruction is present, then the message should be delivered to recipient MM-UAs that are under Minimize restrictions. If this instruction is absent, then system components that have access to MM heading fields may block the message depending upon local policy. Note that specific requirements for specific component handling of Minimize is beyond the scope of this document. (See 4.I.411.)

(2) For each message, the originator shall have the option to request the extent of distribution be limited after the messages are received by the intended recipients (primary and copy recipients and other recipients indicated). If the originator decides the message

should be limited to those who need to know, then "LIMITED DISTRIBUTION" shall be included in the Message Instruction EoS. If this instruction is present, the recipients shall respect the originator's request and distribute the message only to those whom the recipient determines require access to the message. The meaning implied by the message instruction, "LIMITED DISTRIBUTION," shall be defined by local policy. If this instruction is present, it shall be prominently displayed to the user.

(3) After the originator has determined the recipients of the message, the originator shall then have the option to instruct the recipients not to further distribute the message without the originator's approval. If the originator determines the message should not be distributed beyond the specified recipients (primary and copy recipients and other recipients indicated), then "NO DISTRIBUTION" shall be included in the Message Instruction EoS. If this instruction is present, the recipients shall not distribute the message further without first gaining approval from the message originator. The definition of further distribution shall be determined by local policy. If this instruction is present, it shall be prominently displayed to the user.

(4) For each message to be received by the intended recipients, all recipients must have access to the MMHS. If the originator knows that the intended recipient is temporarily without MMHS access, then the recipient's name, responsible for getting the message to the intended recipient, shall be placed before "SEND TO" followed by the intended recipient's name. The recipient's name, "SEND TO", and the intended recipient's name shall be included in the Message Instruction EoS. The originator shall ensure that the intended recipient's name is unambiguously specified. If this instruction is present, the recipient of the message shall deliver the message to the recipient specified after the "SEND TO" in the Message Instruction. The method of delivery and extent to which this Message Instruction will be used shall be determined by national policy. If this instruction is present, it shall be prominently displayed to the user.

(5) Any message for which a signal (see 4.I.404.b) is required at the recipient MM-UA, but which does not qualify for a high precedence value (i.e., OVERRIDE, FLASH, and nationally defined values) shall have the instruction "ALARM REQUIRED" included in the Message Instructions EoS. Any received message containing this instruction shall be handled as a high-precedence message by the MM-UA in accordance with clause 4.I.403. Procedures for determining what messages may use this Message Instruction will be determined by national policy.

(6) The originator shall have the option to request the message not be sent via fleet broadcast. If the originator determines that the message should not be sent via fleet broadcast, then "NO FLT BRDCAST" shall be included in the Message Instruction EoS. If this instruction is present, Fleet Broadcast stations shall not transmit the message via fleet broadcast. If this instruction is present, it shall be prominently displayed to the user.

(7) The originator shall have the option to request the message not be sent via fleet operational intelligence broadcast. It is the originator's responsibility for determining if this instruction applies to the message. If the originator determines that the message should not be sent via fleet operational intelligence broadcast, then "NO FLT OPINTEL BRDCAST" shall be included in the Message Instruction EoS. If this instruction is present, fleet broadcast stations shall not send the message via fleet operational intelligence broadcast. If this instruction is present, it shall be prominently displayed to the user.

(8) The originator shall have the option to request a Night Action, which indicates that the alternate recipients shall recall intended recipients to receive a message. Any originator that uses this message instruction shall assure that an originator requested alternate recipient (see clause 2.I.206.ad) is specified for each intended recipient of the message. If the originator determines that the message requires a Night Action, then "NIGHT ACTION" shall be included in the Message Instruction EoS. If this instruction is present, an alternate recipient shall notify (via telephone, pager, etc) the intended recipient that a Night Action message was received, and the alternate recipient shall then forward the message to the originally intended recipient. It is not required that the copy recipients be notified. If this instruction is present, it shall be prominently displayed to the user.

h. Clear Service

This element of service indicates to the recipient MM-UA that the message containing classified information has been transmitted over an non-secure channel. The message, when received, shall be marked with the phrase "RECEIVED IN CLEAR, TREAT AS CONFIDENTIAL" by the MM-UA prior to presentation to the end user. This phrase will be prominently displayed to the user. This may be used to indicate that the message originated outside the MMHS (e.g., in a tactical environment). (See Annex A B.112 on page A-17.) This service is provided by interpretation of the values of the message security label. The value "CLEAR" in the *privacy-mark* field, in conjunction with an appropriate military value in the *security-policy-identifier* field, is used to represent the clear service. The clear service is defined to be messages of any classification except TOP SECRET that in tactical operations, simulated or actual, the speed of delivery is so essential

that time cannot be spared for encryption and the transmitted information cannot be acted upon by the enemy in time to influence current operations. In such cases, transmission in the clear must be authorized separately for each message. These messages shall be handled as CONFIDENTIAL material. Should the addressee desire the information to be forwarded to another addressee, a new message shall be originated, appropriately classified, and handled as the situation dictates. These rules do not apply to messages that are not normally encrypted such as enemy contact reports, position reports, etc. The security policy identifier to be used in conjunction with the "CLEAR" *privacy-mark* may be specified by national policy or international agreement. The ability to originate message security label indicating the clear service may not be available to all MM-UAs.

i. Other Recipient Indicator

This element of service enables the originator to indicate to the recipient the names of one or more recipients, as well as the category (Primary or Copy), in which they are placed, that are intended to receive, or have received, the message via other means. The intent of this service is to enable a recipient to determine which recipients are intended to receive the message without the use of MMHS, as well as the category in which they are placed. While the Primary and Copy Recipient Indication EoS and *address-list-indicator* field provide the names of recipients that can be reached through MMHS, other recipients can be determined with this service element. This service is a user option. The information for this service is carried in the military heading extension *other-recipient-indicator* and if present, shall be displayed to the user. (See Annex A B.113 on page A-17.)

This element of service does not carry the reason why the other recipient(s) will not receive the message through MMHS. Some reasons might include:

(1) The recipient is not a user of the MMHS and has been sent the message by other means;

(2) The originator knows (or presumes) that a secure path to the recipient will not be found through the MMHS and has therefore sent the message by other means; and

(3) The recipient has already received the message by other means before it was entered in the MMHS.

j. Originator Reference

This element of service enables the originating MM-UA to indicate to a recipient MM-UA a reference called the "originator's number". The originator's number is used by the originating organizational unit. The use of this field will be further clarified by national policy. This service is different

from the *IPMIdentifier* in that this reference is assigned by the originator, while the *IPMIdentifier* is supplied by the MM-UA. (See Annex A B.111 on page A-16.) This service is a user option. This service is carried in the military heading extension originator-reference.

k. Use of Address List

This element of service conveys the name of a pre-defined list of recipients to which the originator has sent the message. The AL can be qualified as either a Primary or Copy recipient, and indicates if notifications or replies are requested from the members. The Exempted Addresses element of service can be used in conjunction with an AL to exclude certain members of the list. Originating domains are responsible for expanding ALs for which they have configuration responsibility. This service is carried either as an ORName of an AL in the *primary-recipients* or *copy-recipients* protocol elements or in the military heading extension *address-list-indicator*. (See Annex A B.104 on page A-14.) Use of the *address-list-indicator* field to support this is for transition only. If the AL is addressed as a copy recipient, all members of the list shall be considered copy recipients. If the AL is addressed as a primary recipient, individual members may be either primary or copy recipients and should know their role by basis of membership in the list. When the *address-list-indicator* is used to convey the AL, the status of the AL as a primary or copy recipient is indicated by the state of the *primaryAddressList* and *copyAddressList* elements. If an AL is present, it shall be displayed to the user.

TRANSITION ELEMENTS OF SERVICE

213. The following Military EoS are required for interworking with older military messaging domains (ACP 127). They are included in ACP 123 in order to allow ACP 123 users to correctly receive and understand these elements from ACP 127 gateways. This will enable the ACP 123 environment to interoperate with ACP 127 in the short term, and to do so in a harmonized way. Origination of these EoS is not a requirement for UAs in the ACP 123 environment because any gateways should operate transparently, without the need for originating users to be aware of the environment of the recipients. Once all nations have fully deployed the ACP 123 MMHS, support of these services will no longer be required.

a. Handling Instructions

This element of service enables the originator to indicate to the recipient that local handling instructions accompany the message, and that the message requires manual handling by a traffic operator. (Handling instructions are also called transmission instructions.) (See Annex A B.108 on page A-15.) This service carries information that is only used by the traffic operators in ACP 127. It is not necessary in the ACP 123 network. This service is for transition only. If this service is deemed necessary for a message originated by a user in the older (ACP 127) messaging domain, the information for it will be carried in the military heading extension *handling-instructions.*

b. Pilot Forwarded

This element of service is intended for use with gateways from older military messaging domains (ACP 127) and allows a gateway to translate a pilot message. The original received "body/text" of the message is sent as the "text body" of a new message. The Pilot Forwarded service conveys information that equals or supersedes the received heading information for precedence, classification, local handling instructions and addressing. (See Annex A B.115 on page A-18.) This service is for transition only. If the information for this service is received coming into the MMHS, it is carried in the military heading extension *pilot-forwarding-info*. This information, if present, shall be displayed to the user.

c. Corrections

This element of service enables a message originating in an older military messaging domain (ACP 127) to indicate to the recipient that there are corrections required to the text body. (See Annex A B.114 on page A-17.) This service is for transition only. During the transition if corrections are present in an ACP 127 message that must be translated into an ACP 123 message, the corrections will be carried in the externally defined body part type *corrections-body-part*. If this information is present in a received message, the user shall have the capability to display it.

d. ACP 127 Message Identifier

This element of service conveys the message identifier of an ACP 127 formatted message in MMHS. This identifier consists of the RI of the originating COMCEN, the Station Serial Number, and the Filing Time. (See Annex A B.116 on page A-18.) This service is for transition only and will be used to support the tandeming of full ACP 127 messages through MMHS domains. It may, however, be used by MMHS domains who wish to ensure a unique message identifier that is common to both MMHS and ACP 127 for messages originated by ACP 127 users. It will be carried in the *acp127-message-identifier* heading field. If this information is present, the user shall be able to display it.

e. Originator PLAD

This element of service enables the originator to indicate to a recipient the plain language address of the originator of the message. (See Annex A B.117 on page A-18.) This service is for transition only. It is only necessary if there is no easy way of translating between the originator's PLAD and an ORName. The information for this service, together with the Extended Authorization Info service, provides a cross reference for message identification in both ACP 127 and MMHS domains. It is carried in the military heading extension *originator-plad*.

f. Codress Message Indicator

This element of service enables the originator to indicate to the recipient that the message is in codress format. This applies only to codress encrypted messages, which are restricted to a single body part. Codress is defined as a procedure in which the entire address of a message is encrypted within the text, while the heading of any transmission of that message contains only information necessary to enable communications personnel to handle it properly. Codress may be implemented by a nation, service or appropriate Allied authority for use with high-grade off-line cryptographic systems. This service is for transition only, and is carried in the *codress-message* heading extension. This service is supported on reception to enable codress messages from older military messaging domains (ACP 127) to be carried inside an ACP 123 message. (See Annex A B.110 on page A-16.) The information for this service is carried in the military heading extension *codress-message.* A value of zero (0) indicates "NC" or No Count.

g. ACP 127 Notification Request

This service element enables the originator to request notifications specifically from ACP 127 gateways. (See Annex A B.118 on page A-18.) In cases where interoperability with ACP 127 domains is provided transparently, this service may not be practical. This is because users will not necessarily know in advance whether a recipient address is located within an ACP 127 domain. ACP 127 Notifications can be requested for the following scenarios:

(1) Positive notification – the ACP 127 gateway successfully transfers the message and accepts responsibility for its submission into the ACP 127 domain;

(2) Negative notification – the ACP 127 gateway has received the message, but fails to transfer it; and

(3) Transfer notification – the ACP 127 gateway successfully transfers the message but has not kept a record of the message and does not accept responsibility for it.

Depending upon national policy, the gateway scenario described by the Transfer Notification may be prohibited. This service is for transition only, and is carried in the *acp127-notification-request* extension of the *RecipientSpecifier*.

h. ACP 127 Notification Response

This element of service conveys the results of an attempt to transfer a message into an ACP 127 domain. (See Annex A B.119 on page A-19.) It indicates

whether the transfer was positive, negative, or positive but without responsibility. It also conveys the receipt time, the ALs of the message, the ACP 127 recipient address, and any pertinent supplementary information. This service is for transition only, and is carried in the *acp127-notification-response* extension of the MN element *other-notification-type-fields*. If this information is present, the user shall be able to display it.

CHAPTER 3
MESSAGE HANDLING SYSTEM COMPONENTS

SECTION I
MESSAGE TRANSFER SYSTEM

301. In the X.400 Message Handling Environment (MHE), messages are relayed in a store-and-forward fashion between MTAs until the message reaches the specified destination(s). The collection of MTAs (and the underlying communication service) is referred to as the MTS. Since it has been agreed that there may be a requirement to use a commercially provided MTS service, modifications to the existing MTS Transfer Protocol (i.e., P1) used by the MTAs to exchange messages have been avoided. Modifications to the submission and delivery protocols (i.e., P3 and possibly P7) used in communicating to the MTAs have also been avoided in order to enable the use of commercial MTAs.

302. To ensure interoperability and further maximize the possible use of commercial MTAs, ACP 123 defines specific profiles for use of MHS protocols. These profiles are addressed in Chapter 5.

303. Additionally, the following services provided within the MTS may be exploited to meet specific military messaging requirements:

PROHIBITION OF PROBES

304. Submission control will be used to prohibit a probe from being originated within the MMHS environment. However, it shall be the responsibility of MMHS interface points to prohibit probes that originate outside the MMHS environment from entering an MMHS domain. MTAs shall refuse the *Probe Transfer* operation. Reports concerning a probe shall not be returned to the originator of the probe. If a probe is received at an MTA, this shall be logged as a potential security problem. The log shall include the probe's originator, the originating domain, the time of receipt, and the intended recipient. (See 2.II.207.c, and 4.I.412.)

DELIVERY AND NON-DELIVERY REPORTS

305. Since the originator is responsible for messages until they have been delivered, Delivery and Non Delivery Reports can be utilized to indicate when a shift of responsibility has occurred. Policy or local implementation can dictate whether Delivery Reports are provided to the user or used to automate retention of messages at the originating system for the required time as a default. Delivery Reports can always be requested by the originating user. An MTA in the MTS shall generate a Non-Delivery Report if it has held messages with a *priority* field of URGENT, NORMAL, and NON-URGENT for 12 minutes, 60 minutes, and 96 hours, respectively (see 4.I.404). These limits are imposed in cases where an MTA encounters transient problems for which a retry may succeed, and for which the Latest Delivery

Designation EoS was not specified by the originator. The time limit for NON-URGENT was determined by considering the likely duration of periods of unmanned operation including 3-day weekends and time zone differences. (See 2.II.205.g, 2.II.206.l and 4.I.406.)

RETENTION OF OTHER RECIPIENTS

306. The MTA shall not discard the transfer envelope per-recipient fields associated with recipients for which the responsibility flag has been set (i.e., for which delivery has already occurred). This Retention of Other Recipients is necessary to ensure that the Disclosure of Other Recipients EoS functions correctly.

CONFIGURATION MANAGEMENT

307. Each time a new MTA is introduced in to the network there are ramifications for other MTAs. Routing decision tables need to be updated to reflect the new MTA and the UAs for which it will be responsible for delivering messages. MTA peer-to-peer authentication information must be distributed to every MTA to which an MTA can make a direct association. Network information such as address and available communications stack must be registered and made available. Registration of appropriate names and addresses will be performed according to established national registration procedures. Configuration management information for the messaging and its supporting security services must be securely controlled to prevent unauthorized modification.

AUDIT TRAIL AND LOGGING REQUIREMENTS

308. Storage of audit data by the MTA 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 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. National policy may require longer retention periods and additional information be stored. The integrity of audit logs must be protected.

Table 3-1 MTA Logging Requirements

Inbound Messages	Outbound Messages
Message Submission Envelope:	Message Delivery Envelope:
MTS Message Identifier	MTS Message Identifier
Message Submission Time	Message Delivery Time
Priority	Priority
Message Transfer Envelope:	Message Transfer Envelope:

Table 3-1 MTA Logging Requirements

Inbound Messages	Outbound Messages
MTS Message Identifier*	MTS Message Identifier*
Priority*	Priority*
Bind Arguments & Results*	Bind Arguments & Results*
Probe Submission Envelope†	Report Delivery Envelope
Probe Transfer Envelope*†	Report Delivery Time
Report Delivery Envelope:	Report Transfer Envelope*
Report Delivery Time	Time of Transfer Out*
Report Transfer Envelope*	
Time of Transfer In*	

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

† If a probe is received at an MTA, this should be logged as a potential security problem, including the originator, the originating domain, as well as the time of receipt and the intended recipient.

SECTION II
MILITARY MESSAGING USER AGENTS (MM-UA)

309. Enhancements to commercial X.400 services to support Military Messaging occur mainly in the definition of a new message content type. This content type will be supported by enhanced UAs for military messaging. The services supported by this content type are described in the previous chapter. The protocol that supports the services is described using ASN.1 in Annex A. These UAs are referred to as MM-UAs. Issues to be addressed in national supplements to complete the definition of MM-UAs include:

- Release authorization procedures and techniques,
- Verification of message authenticity,
- Message accountability,
- Distribution policies,
- Requirements (prohibitions) for the use of MSs or intermediate storage between the MTA and a remote UA.

STORAGE AND RETRIEVAL POLICIES

310. How long messages shall be stored and how they can be accessed after receipt will be defined by national policy. All MM-UAs will store both outbound and incoming messages for a minimum of 10 days. This is to support the possible request for retransmission of a message and in support of message accountability and tracer action. Outgoing messages shall be stored with the original security services invoked since any retransmission requires the precise form forwarding of the original message. If the message was originally encrypted, it must be decrypted by the originator prior to retransmission.

PROHIBITION OF PROBES

311. The Probe EoS presents a serious security risk in the MMHS environment. MM-UAs are therefore prohibited from originating probes in accordance with clause 2.I. 207.c.

PRECEDENCE BASED DISPLAY

312. The user interface of the MM-UA shall prominently indicate the presence of unread high precedence (i.e., precedence that map to the URGENT Grade of Delivery) messages. The MM-UA should automatically adjust the user's display to reveal and highlight unread high-precedence messages in preference to either low precedence messages or previously read high-precedence messages.

PRECEDENCE SIGNALLING

313. Messages that map to the URGENT Grade of Delivery shall cause the MM-UA to prominently (e.g., audibly) signal the recipient upon delivery.

MMS AUTO-ACTIONS

314. The MMS can perform auto-actions on behalf of the user if configured to do so. The following constraints are imposed on the use of MMS Auto-Actions.

a. Auto-discard

The MM-UA shall not automatically discard messages that have either the *expiry-time* or *obsoleted-IPMs* heading fields present. Messages shall only be deleted by the intended recipient and in accordance with national audit trail requirements.

b. Auto-forward

The MM-UA may be configurable to auto-forward messages. If configurable to forward messages then the MM-UA may auto-forward received messages to one or more recipients.

c. Auto-acknowledgment

The MM-UA shall not be configurable to automatically originate receipt notifications for messages with a *notification-request* field on behalf of the user.

AUDIT TRAIL AND LOGGING REQUIREMENTS

315. Storage of audit data by the MM-UA 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 MM-UA 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 MM-UA for submitted and received messages. National policy may require longer retention periods and additional information be stored. The integrity of audit logs must be protected.

Table 3-2 MM-UA Logging Requirements

Submitted Messages	Delivered/Receive Messages
Message Content:	Message Content:
Authorizing Users (Release Authority)	Extended Authorization Information
Extended Authorization Information	MM Identifier
MM Identifier	Originator Indication
Notifications Requested	Precedence Values Assigned
Precedence Values Assigned	ESS Security Label
Requested Recipients	Message Delivery Envelope:
S/MIME Signed Receipt Requests	MTS Message Identifier
ESS Security Label	Message Delivery Time
Message Type	Bind Arguments & Results
Message Submission Envelope:	Report Delivery Envelope:
Deferred Delivery Time (if applicable)	Report Delivery Time
MTS Message Identifier	Time of Retrieval from MS (if MS is implemented)
Time of Submission	
Bind Arguments & Results	

SECTION III
MESSAGE STORES

316. An MS is designed to support delivery of messages when the intended recipient's UA is unavailable to accept messages from the MTS. The MS is an optional component and its use with any given MM-UA will be determined by national or local policy. Support of the MS access protocol (i.e., P7) across international boundaries is not required by ACP 123. This is due to the technical difficulty associated with de-coupling the MS design from that of the user interface of the UA. However, when an MS is used, it must not degrade the service provided. This section is devoted to describing the issues surrounding the use of an MS in a military environment.

317. To support retrieval of MMs from a MS based on MM heading fields, MS attributes were defined (see Annex A page A-53). MSs that support retrieval of messages based on MM-specific MS attributes are referred to as MM-MSs.

MS FUNCTIONAL RESTRICTIONS

318. The MS can perform auto-actions on behalf of the user if configured to do so. The following constraints are imposed on the use of MS Auto-Actions.

a. Auto-deletion

Automatic deletion of messages by the MS is strictly prohibited. Messages shall only be deleted from the MS by the intended recipient and in accordance with the national audit trail requirements policy.

b. Auto-forward

If an MM-UA and its associated MS may be unmanned, then in order to handle receipt of high precedence messages, the MS shall support automatic forwarding. Automatic forwarding based on the mt-message-submission-time and mt-priority attributes shall be provided. Any URGENT message shall be auto-forwarded if the time elapsed from submission exceeds ten (10) minutes. Any NORMAL message shall be forwarded if the time elapsed from submission exceeds forty five (45) minutes. National or other policy may specify shorter times for automatic forwarding. When automatic forwarding is performed by the MS, then a content type of P772 shall be originated with the delivered message included as either a content-body-part (for messages received with S/MIME protection) or an mm-message-body-part (for messages previously forwarded without S/MIME protection).

c. Auto-alert

Automatic alerts shall be sent to recipient's MM-UA immediately on delivery of URGENT and NORMAL priority messages. In cases where the MM-UA is

not available to service the alert (i.e., no P7 association established), mechanisms must be supported that allow the user to be alerted. These mechanisms may include support of messaging protocols (e.g., special message sent to an alternate position indicating that alerts are not being serviced) or other non-messaging solutions (e.g., proprietary interface to a paging service).

AUDIT TRAIL AND LOGGING REQUIREMENTS

319. Storage of audit data by the MS 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 MS 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 MM-UA for delivered and submitted messages. National policy may require longer retention periods and additional information be stored. The integrity of audit logs must be protected.

Table 3-3 MS Logging Requirements

Delivered Messages	Submitted Messages
Message Content	Message Content
Message Delivery Envelope:	Message Submission Envelope:
MTS Message Identifier	MTS Message Identifier
Message Delivery Time	Message Submission Time
Bind Arguments & Results	Bind Arguments & Results
Report Delivery Envelope:	Time of Indirect Submission
MTS Message Identifier	
Report Delivery Time	
Time of Retrieval from MS	

CHAPTER 4
POLICIES AND PROCEDURES

SECTION I
GENERAL PROCEDURES

401. There are a number of procedures to be implemented in a military messaging environment that may or may not correspond directly to a specific format field within the messages being transmitted and received. This section describes those procedures and documents the methodology and circumstances necessary for full implementation.

CLEAR SERVICE

402. All MMs originating in the MMHS will incorporate the security services, included in the security section of ACP 123 (see 4.II). However, there may be some instances where classified messages will have originated outside the MMHS in the clear. In this case, on entry to the MMHS, the point of entry will add the Clear Service. The message should be treated as CONFIDENTIAL even though the message was originally received without a security classification. The Clear Service will be carried as part of the Message Security Label, using the *privacy-mark* field. (See 2.II.212.h, and 4.I.404.b.) Messages with this indication require the MM-UA to display to the recipient the words "RECEIVED IN CLEAR, TREAT AS CONFIDENTIAL".

RECIPIENTS

403. It is the originator's responsibility to select the appropriate recipients for each message. It is essential that the originator of a message limit the number of recipients to those who need to take action thereon and, in the case of copy recipients, to those for whom the information contained in the message is essential. Once the appropriate recipients have been determined, a Directory service may be used to obtain the necessary recipient information required for proper addressing and security information. Upon origination all recipients present in the envelope fields shall be indicated in either the primary, copy, or blind copy heading fields.

PRECEDENCE HANDLING (LOCAL)

404. The extension fields *primary-precedence* and *copy-precedence* will be used to carry originator to recipient information about the military importance of the message. Possible values for these fields are: DEFERRED, ROUTINE, PRIORITY, IMMEDIATE, FLASH, and OVERRIDE.

a. Definitions of Precedence Levels

Six (6) levels of precedence are defined in ACP 123. However, the DEFERRED and OVERRIDE levels of precedence are defined by ACP 123

but are not expected to be widely supported. These values should be used only within the context of bilateral agreements. Additional precedence values are also reserved for national use. The following levels of precedence are defined by ACP 123:

(1) FLASH – The FLASH precedence is reserved for initial enemy contact message or operational combat messages of extreme urgency. Brevity is mandatory.

(2) IMMEDIATE – The IMMEDIATE precedence is reserved for very urgent messages relating to situations that gravely affect the security of national/Allied forces or populace.

(3) PRIORITY – The PRIORITY precedence is reserved for messages concerning the conduct of operations in progress and for other important and urgent matters when ROUTINE precedence will not suffice.

(4) ROUTINE – The ROUTINE precedence is to be used for all types of messages that justify transmission by rapid means but are not of sufficient urgency and importance to require a higher precedence.

(5) DEFERRED – The DEFERRED precedence is lower than ROUTINE and left for national policy or international agreement for further definition.

(6) OVERRIDE – The OVERRIDE precedence is higher than FLASH and is left for national policy or international agreement for further definition.

b. Grade of Delivery

The *primary-precedence* field will automatically be used to select the associated Grade of Delivery service. If both Primary Precedence and Copy Precedence indicators are present, and they map to two different MTS Grades of Delivery, then multiple copies of the MPDU will be submitted (or the MPDU may be divided by the originating MTA): one for the Primary Precedence recipients and the other for the Copy Precedence recipients. If, however, the originating MTA can determine that all the Copy recipients are served by delivering MTAs for Primary recipients, only one copy of the MPDU need be transmitted with the MTS Grade of Delivery derived from the Primary Precedence. In the case of an MM-UA not collocated with its originating MTA, the responsibility for two MPDUs would rest with the MM-UA. The MM-UA would have to invoke two message submissions in order to ensure the proper Grade of Delivery selection for appropriate recipients, as the message submission envelope does not carry an indication of which recipients are Primary and which are Copy recipients. If there are no Primary recipients,

the Grade of Delivery is taken from the Copy Precedence. MPDUs for Blind Copy Recipients will always be sent at a NON-URGENT Grade of Delivery. In messages that contain Blind Copy Recipients, the MPDU may need to be submitted using up to three different Grades of Delivery.

c. Determining Precedence

The assignment of precedence to a message is the responsibility of the originator. The importance of judicious assignment (avoidance of use of a higher precedence than necessary) cannot be overemphasized. The precedence assigned to a message by the originator does not necessarily indicate the action to be taken by the addressee or the precedence designation that should be assigned to the reply. Such instructions, if necessary, will be included in the text. The factors to be considered for each message are:

(1) Consideration should be given to the urgency of the subject matter. Importance does not necessarily imply urgency. The originator should consider the urgency of the message as it applies to the addressee(s).

(2) Consideration should be given to the time difference between widely separate geographical areas (e.g., Eastern United States is six hours behind Central Europe). Recipients with MM-UAs not manned 24 hours/day, 7 days/week, may have requested auto-forwarding based on the value of the *priority* field or invoked the Redirection of incoming messages EoS.

(3) If a message is auto-forwarded then, the auto-forwarded message shall have the precedence level that applies to the recipient of the message.

d. Processing

All components shall process messages according to the Priority values in the envelope. Messages with an URGENT Priority shall be processed before NORMAL, which shall be processed before NON-URGENT messages. For each Priority level and destination, messages should be processed in a First-In-First-Out (FIFO) order. No message of a lower Priority shall delay a message of higher priority. Some examples of priority processing are:

(1) Multiple associations may be used to transfer messages simultaneously. Associations established using network layer precedence mechanisms shall not be reused to transfer messages of differing MTS Priority levels.

(2) Pre-emption may be useful in bandwidth-constrained environments to meet the speed of service requirements. Pre-emption

is the suspension of the transmission of a message to allow the transmission of a higher priority message with the resumption of the transmission of the suspended message at the completion of the transmission of the higher priority message.

MESSAGE ACKNOWLEDGMENT

405. There are two levels of message acknowledgment that can be requested from originator to recipient. The Request for Receipt Notification service will result in a service message, called a Receipt Notification (RN), being returned from the recipient MM-UA after the message has been displayed to the recipient. However, this is the equivalent of a recipient signing for a letter in the Physical Delivery postal service. No authentication of the recipient is associated with this receipt notification. A receipt notification does not imply an understanding of the contents, but simply that the recipient has accepted responsibility for having received the message. If explicit Military Acknowledgment, which indicates that the message has been "read and understood", is required, the originator shall ask for Reply Requested. The originator may possibly include Reply By and Reply To (in the *reply-time* and *reply-recipients* heading fields, respectively) indications. In this case, the recipient will generate a new message indicating not only receipt, but also whether the received message has been understood. This new message invokes security requirements and is the preferred acknowledgment method when authentication of recipients is required. The following guidelines are recommended:

- Request for Reply shall be displayed to the recipient, so the recipient knows "Explicit Military Acknowledgment" has been requested. If *reply-time* and *reply-recipients* fields are present, these shall also be displayed to the recipient.
- Replies can be requested for both Primary and Copy recipients. However, the reply request is only mandatory for Primary recipients.
- If the message recipient is a Primary recipient, then a reply shall be generated back to the message originator or requested reply recipients before the time specified, if present, or once the message has been read and understood, whichever comes first.
- If the Primary recipient does not respond by the time specified, the originator will consider the message not received. It will be the responsibility of the originator to take action to determine the cause of the failure according to national policy. This could be contacting the recipient to ensure the original message was received or issuing a second request for response. Audit logs can be used to initiate a tracer action if the message was not received.
- If the message recipient is a Copy recipient, then generation of the reply is at the sole discretion of the recipient (dependent on local policy).

- National policy shall specify the procedures for recipients that receive receipt notifications, S/MIME signed receipt notifications, and reply requests.

CONFIRMATION OF DELIVERY

406. An optional service will allow an originator to ask the MTS to return a Delivery Notification indicating the message was successfully delivered to the recipient MM-UA. This is strictly confirmation of delivery at the MTA level, may not be authenticated, and does not indicate any sort of acceptance of responsibility at the User level. Explicit message acknowledgment, or request for Receipt Notification, shall be used if User acknowledgment of receipt of the message is required. In order to limit excessive use of Delivery Notifications the following guidelines are recommended:

- For messages that map to the URGENT MTS Grade of Delivery (i.e., FLASH and OVERRIDE), requesting Delivery Notification is encouraged, unless actual recipient acknowledgment has been requested (e.g., Receipt Notification Requested or Reply Requested).
- For messages that map to the NORMAL MTS Grade of Delivery (i.e., IMMEDIATE and PRIORITY), requesting Delivery Notification is neither encouraged nor discouraged and is solely at the discretion of the message originator.
- For messages that map into the NON-URGENT MTS Grade of Delivery (i.e., ROUTINE and DEFERRED), requesting Delivery Notification is discouraged.

407. In all cases, it should be noted that non-delivery report will be returned to the originating MTA and the non-delivery information will be given to the originating MM-UA unless the Prevention of Non-delivery Notification EoS was requested with the message.

CANCELLATIONS

408. If a previously sent message is no longer considered valid, a second message indicating the first has been obsoleted can be sent to all recipients. This will be implemented using the X.400 service Obsoleting Indication. The body of the new message can either contain a replacement message or a short message indicating the original message is no longer valid. Cancellation of a message may only be done following the authentication policies of the originating nation. If a cancellation applies only to some recipients of a message, then the body of the canceling message should indicate the nature and limitations of the cancellation.

CORRECTIONS

409. If a previously sent message needs to be corrected, one of two methods may be used. If the corrections are small compared to the size of the original message a new message, which describes the changes and identifies the original message in the Cross-Referencing Indication, may be sent. The second method is to transmit an entire replacement message indicating the original message to be replaced in the Obsoleting Indication. Only the original message originator or the original release authority is permitted to correct the previously transmitted message following the proper release and authentication policies of the originating nation. In the case of partial corrections, appropriate references shall be made to the specific location of the correction(s) within the body of the message (e.g., the following sentence replaces the third sentence in the second paragraph of Section 10).

REPETITIONS, CHECKS, AND VERIFICATIONS

410. In the event that message integrity is lost resulting in corruption of a message, the recipient is responsible for contacting the originator and requesting retransmission of the message. If it is necessary to verify that all or part of a message is valid, a separate message may be sent.

MINIMIZE

411. The purpose of the minimize procedure is to significantly reduce normal or routine message traffic in specific regions or areas during times of crisis in favor of more essential, higher priority message traffic. There is no explicit X.400 service defined to implement the Minimize capability; however, Message Instruction (see 2.I.212.g) is defined to indicate that the originator has considered Minimize. If the Message Instruction is present the message should, barring any delivery problems, be delivered to the recipient. It is the responsibility of originators to enforce Minimize criteria. In the MMHS, the Directory, or similar hard copy notification, will be used to ensure users are aware that Minimize is in effect for potential recipients. It is still the originator's responsibility to ensure that only mission essential messages are sent to a recipient in the Minimize affected area.

MESSAGE CACHE

412. All users are procedurally required for locally storing complete copies of both outgoing and incoming messages on-line for minimum of ten (10) days after submission and receipt. This is to support the possible request for retransmission of a message and to support recipient inquires. After ten (10) days have passed, stored messages will be archived in accordance with national records management policy. Messages shall be stored with the original security services invoked since retransmission requires the forwarding of the original message. If the message was originally encrypted, it must be decrypted by the originator prior to retransmission.

TRACER ACTION

413. If acknowledgment of a message is requested and not received by an originator, then the user can request a Tracer Action. A Tracer Action may consist of a request for operator assistance in examining whatever trace information records are available. The method by which trace information can be traced is a management issue that should be addressed by national policy. However, if an MMHS domain can show from its trace information that a message was successfully passed to another MMHS domain, they should expect the receiving domain to provide assistance in tracing the message to the intended recipient.

MILITARY MESSAGE BODIES

414. The actual information of an MM will be carried in the body of the MM. This can be formatted as either a single body part or as multiple body parts. X.400 messages can carry many different types of encoded body parts. To avoid misinterpretation and further explanatory messages, the message shall state exactly what is meant and shall not be vague or ambiguous. The message should be as concise as possible. If a military text format has been defined which is appropriate for use, that body part type will be used. If no explicit military text format is appropriate a "free-formatted" text body part will be used following the guidelines below.

a. Sequence of Textual Matter

When a body part is free-formatted text the following guidelines will be used in preparing the text:

- The security classification of the body part will be the first word(s) of the text, except that the security classification may be preceded, when necessary, by appropriate international alliance prefix/designator (e.g., COSMIC, NATO, etc);
- If appropriate, the next text would be a list of references; (See 4.I.418.)
- The remainder of the text of the message would follow.

b. Multiple Body Parts

When a message contains multiple body parts, possibly some of them in formats other than plain text (e.g., graphics), the first body part will be "free-formatted" text and follow the format described in 4.I.414.a. This part will provide an overview of the other body parts and action to be taken for each. This descriptive text body part shall also be present in all messages conveying non-text body parts. Every body part included shall contain within it, the appropriate security classification, prominently displayed.

c. Military Body Part Types

A military ADatP-3 body part will be supported. Additional body parts may be required. For example, each nation may want to define a national Military Text Format (e.g., USMTF) that can then carry an identifier for the format as well as the actual text of the message. An MM can also be forwarded.

SPEED OF SERVICE

415. There are two different aspects to speed of service considerations. The first aspect is the need for varying transfer speed requirements for the underlying infrastructure (i.e., the X.400 MTS). The second aspect is the speed of handling of messages (i.e., originator to recipient). Both of these aspects are tied to the precedence levels associated with the message. The transfer time is the difference between the MTS submission time and the MTS delivery time. The originator to recipient time, which includes the transfer time, is the time interval after the originator types the message and takes an action to send the message recipient and when the intended recipient can view the message. Included in this interval is the time needed for the application of security services, resolution of OR Addresses, interconnection of components, submission to the MTS, transfer by the MTS, delivery by the MTS, decryption of the message, validation of signature and signature path, and local handling. Speed of service requirements for the originator to recipient time for the system must be guaranteed. The speed of service times are further qualified with a maximum message size. The maximum message size is not the largest size message that the system will be able to carry at each level, but rather the largest size for which the required speed of service shall be guaranteed. A message character is equivalent to the binary representation for the system in question (e.g., 1 character in ASCII = 1 byte [8 bits]). Total message length, expressed in characters, does not include all required system and protocol overhead. In addition to the message size, service is affected by the number of recipients selected. As such, the speed of service shall be guaranteed only for predefined number of recipients. Definitive quantities numbers will be provided when available. The following table indicates the supported precedence levels, the corresponding originator to recipient speed of service requirements, the assumed message length, the MTS Grade of Delivery, the derived MTS speed of service requirements, and message retransmission times.

Table 4-1 Speed of Service Requirements

Precedence	Overall Requirements		System Requirements		
	Originator to Recipient Time Requirement	Assumed Message Length*	MTS Grade of Delivery	Target MTS Deliver Time	Message Retransmit Time
OVERRIDE (5)	3 minutes	5,400	URGENT(2)	As fast as possible, no	4 minutes

Table 4-1 Speed of Service Requirements

Precedence	Overall Requirements		System Requirements		
	Originator to Recipient Time Requirement	Assumed Message Length*	MTS Grade of Delivery	Target MTS Deliver Time	Message Retransmit Time
FLASH (4)	10 minutes	7,000		more than 3 minutes	11 minutes
IMMEDIATE (3)	20 minutes	1,000,000	NORMAL(0)	No more than 20 minutes	25 minutes
PRIORITY (2)	45 minutes	2,000,000			50 minutes
ROUTINE (1) DEFERRED (0)	No more than 8 hours, or start of next business day	2,000,000	NON-URGENT(1)	No more than 8 hours, or start of next business day	N/A

* = This message length (in characters) represents the maximum size for which the MTS Time of Delivery must be guaranteed. The maximum size of messages supported is not constrained by this document.

a. Speed of Transmission

In order for the precedence level to affect the speed of message transit through the MTS, the selected precedence levels are grouped together and mapped to the Grade of Delivery Selection upon submission. The target MTS delivery time for each Grade of Delivery is the time interval between message submission and delivery (direct or indirect) that is required in order to meet the speed of service requirements (i.e., the maximum time for delivery to meet the ACP 123 requirements if there were no other components needed to perform messaging). If the transmission speed required of the MTS cannot be met, the MTS shall continue trying to deliver the message as quickly as possible. Action shall be taken to ensure delivery, possibly including: retransmission, tracer action, or transmission by other means (applicable only for precedence levels of PRIORITY, IMMEDIATE, FLASH, and OVERRIDE). If the Latest Delivery Time EoS was specified by the originator, then passing this time will cause a Non-Delivery Notification to be returned to the originator. The MTS will also no longer attempt delivery of the message. An MTA shall be configurable to allow a Non-Delivery Notification (NDN) after a Maximum Non-Delivery Time has elapsed for any message. The time at which an NDN shall be returned from the MTA may be measured either from the time of submission to the current time or the time the message has been resident in a single MTA. When a message has been deemed undeliverable, a Non-delivery Notification is returned to the recipient in the case of transmission system problems where retries may succeed and Latest Delivery was not specified. How this default is established, and

whether operators are notified in case of transmission system problems are both management issues that need to be addressed in national supplements.

b. Speed of Handling

Speed of handling includes everything from dictating physical delivery requirements to the final action officer, to the order of messages displayed on an end-user workstation. Although these criteria are viewed as local, non-communication oriented procedures, they cannot be implemented without indicating the level of precedence in the message heading to the user. The Primary and Copy Precedence EoS will be used to convey precedence information from originator to recipient.

DUPLICATE DETECTION

416. If the text of a message is an exact duplicate of an earlier message, but the *IPMIdentifier* or other heading field in the second message is different (due to forwarding, auto-forwarding, etc.), then the message can not be detected as a duplicate by the system. The burden for recognizing a message of this type as a duplicate will be on the recipient. However, if a UA receives two messages with the same *IPMIdentifier*, the system can automatically determine the second message is a duplicate and discard the second message. The user will be given an indication that a duplicate was detected and information about the duplicate including its *IPMIdentifier* and Submission and Delivery Times, will be logged for audit purposes. Automatic detection of this type of duplicate message is dependent on the local implementation and availability of the earlier message within the UA's knowledge base. (e.g., if the earlier message had been printed and deleted from the system, the UA may not have the knowledge to determine that the second message contained a duplicate *IPMIdentifier*.) This duplicate detection scenario will not work in the case of auto-forwarded messages since auto-forwarding from components places a new *IPMIdentifier* on each auto-forwarded message.

CONVERSION

417. Conversion is not compatible with originator-to-recipient integrity, authentication, and content confidentiality. Implicit conversion will be used in the military environment where interface points are utilized (e.g., tactical gateways).

REFERENCES

418. The text of MMs often employ references to other messages. The following paragraphs describe procedures for use of such in-text references.

a. When references are made to other messages that have been conveyed as MM, the *IPMIdentifier* will be used as the reference. When referring to letters, orders, ACP 127 messages, and other forms of military communications other than ACP 123 MMs, references will consist of the authorized abbreviated title of the originator of the communication, followed

by the identification of the reference and its date (day, month, and year). When referring to an ACP 127 message, the SIC shall be added.

b. When more than one reference is quoted, the originator may, if considered necessary, identify each reference separately by a letter label. In this case the list of references should appear near the top of the text body part of the message that makes use of those reference labels. (See 4.I.414.a.)

c. When all the references are in the form of *IPMIdentifiers*, and the references are appropriate to the entire message (i.e., all included body parts), the Cross-referencing Indication EoS should be used. If the reference is only appropriate to one body part of a multi-body part message, the references should appear near the top of that appropriate text body part. (See 2.II.206.i.)

d. When references are placed in messages destined for several addressees, care must be taken that such references are available to all addressees. In cases where a reference is not held by all addressees and the originator determines that those addressees do not need it, then the indication "(NOTAL)" (meaning "Not to, nor needed, by all addressees") should be included after the reference. In this case the references need to appear in the body of the message. (See 4.I.414.a.)

e. If the communications referenced are included as additional body parts to a message, this will be indicated by appending the indication "(INCLUDED)" after the reference in the text.

USE OF ALTERNATE DELIVERY MECHANISMS

419. Support for message redirection is impacted by the security services of S/MIME (see 4.II.426). The following sections clarify the effects of using all the forms of alternate delivery supported by X.400.

a. Originator Requested Alternate Recipient

(1) Within the MMHS, two requirements have been identified for this EoS. The first requirement allows the originator to choose an alternate recipient for each intended recipient of the message in cases where the message does not reach the intended recipient as a result of message transfer or delivery problems. The second requirement is for any message recipient within the MMHS to be able to publish in the X.500 directory who the alternate recipient should be in cases where the message does not reach the intended recipient. See 4.II.426 for a description of the interactions with security services.

(2) Organizational users who may receive messages with precedence values of IMMEDIATE, OVERRIDE, or FLASH may publicize an alternate recipient address; however, the procedural

requirements for publication of the alternate recipient shall be specified by national policy. All message originators, originating messages with a precedence values of IMMEDIATE, OVERRIDE, or FLASH, are procedurally required to honor and utilize the published alternate recipient selection of the recipient, unless the Redirection Disallowed by Originator EoS (see clause 206.ah) has been selected by the originator. Use of this particular mechanism is discouraged for short-term redirection of messages (e.g., between the beginning and end of users shift, stoppage of work [i.e., lunch, meetings, etc.], certain tactical situations) by recipients because of a dependency on timely updates of the directory. Short-term redirection by recipients is better handled through the auto-forwarding EoS. Subsequent redirection operations (e.g., when alternate recipient is also unavailable) will not be supported by this mechanism. In cases when more than a single tier of redirection coverage is required, other options must be used.

b. Redirection of Incoming Messages

The Redirection of Incoming Messages service may be used by prospective recipients to designate an alternate for their particular MM-UA for an agreed period of time. This type of redirection applies to all incoming traffic that has been correctly addressed to the recipient MM-UA in question. See 4.II.426 for a description of the interactions with security services.

c. Alternate Recipient Assignment

The Alternate Recipient Assignment service may be used to designate a "default mailbox" (e.g., Postmaster) for a particular part of the OR Addressing tree. This type of redirection applies to messages for which a delivery decision cannot be made. It can only be assumed that the default mailbox administrator will be able to make decisions based on the envelope fields (see 4.II.426). Establishment of this EoS must occur as an agreement between the messaging user and the delivering MTA service provider through non-standard means (e.g., service type agreements). International use of this mechanism is discouraged because a Non-delivery report to the originator is preferable to a default mailbox receiving it. Use of this service will be defined by national policy.

d. MS Auto-forwarding

The MS Auto-forwarding service may be used to designate an alternate for a particular recipient MM-UA. This service is encouraged for users who are required to retain a copy of all messages delivered to their MM-MS. This type of redirection applies to all incoming traffic that has been correctly addressed to the recipient MM-UA in question including any one of the redirection mechanism described above. The new recipient will be alerted that the message was auto-forwarded by the Auto-forwarded Indication (see clause

2.II.206.d). If the originator has requested a non-receipt notification, one will be returned that may contain the reason why the intended recipient enabled auto-forwarding. Further auto-forwarding rules can be made based on the *mt-message-submission-time* and *mt-priority* attributes carried in the message delivery envelope. Note that this redirection mechanism is the most flexible; however, it is slower compared with the other mechanisms because the message must first be delivered to the MS before it can be forwarded. See 4.II.426 for a description of the interactions with security services.

e. UA Auto-forwarding

The availability of the MM-UA auto-forwarding service shall be defined by national policy. If MM-UA auto-forwarding is supported, then the MM-UA shall support the Auto-forwarded Indication EoS.

SECTION II
SECURITY

420. Although this particular section may be documented separately from ACP 123, it is anticipated that both protocol and procedural issues related to security will require some degree of Allied agreement. This section describes generic security requirements independent of the mechanisms used to provide the security. It is recognized that gateways may be required to facilitate interoperability between national systems that adopt different security solutions. Incompatibilities may arise due to the selection of different security mechanisms, cryptographic algorithms, or key management strategies. In this event, it may not be possible to provide these security services directly between the originator and the intended recipients in the strict X.400 sense. Therefore, the definition of both the message originator and the intended recipients may be refined subject to bilateral or multi-national agreements. The following security services will be supported.

421. Annex B defines a security solution based on the Secure Multipurpose Internet Mail Extensions (S/MIME) protocols. Nations will need to reach supplemental agreements on the interoperability of labeling, cryptographic algorithms and Public Key Infrastructure (PKI) in order for secure interoperability to be achieved.

SECURITY SERVICES

422. Annex B specifies a set of security services based on the protocols and other features of the S/MIME Cryptographic Message Syntax (CMS) and Enhanced Security Services (ESS) specifications. Specific implementation requirements for these services are as described in Annex B. ACP 123 security services consist of the following.

a. Access Control

This service provides a means of enforcing the authorization of users to originate and receive messages. Access control implementation details are a local matter. Messages both sent and received shall not violate the security policies of the originators and recipients. (See Annex B, section 7.1 on page B-7.)

b. Authentication of Origin

This service provides assurance that the message was originated by the user indicated as the sender. (See Annex B, section 7.2 on page B-8.)

c. Non-repudiation of Origin

Non-repudiation 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. This evidence is a digital signature and the certificates necessary to verify it. However, to preclude a subsequent denial by the originator of having sent the message, the digital signature for this particular message must not be affected by subsequent revocations of the originator's certificates. To preserve this evidence, additional records management procedures must be applied. These include trusted timestamps with another signatures, and audit logs. (See Annex B, section 7.3 on page B-8.)

d. Message Integrity

This 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. (See Annex B, section 7.4 on page B-8.)

e. Message Data Separation

This service protects against unauthorized disclosure of the message, and separates data contained in one message from that contained in another message. (See Annex B, section 7.5 on page B-8.)

f. Security Labels

This service provides a method for associating Security Labels with objects in the MHS. This then allows a Security Policy to define what entities can handle messages containing associated Security Labels. The Security Label associated with a message shall also indicate the Security Policy to be followed. (See Annex B, section 7.6 on page B-9.)

g. Non-repudiation of Receipt

Non-repudiation 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 receipt includes a cryptographic binding to the original message received. However, to preclude a subsequent denial by the recipient of having sent the message, the digital signature for this particular message must not be effected by subsequent revocations of the recipient's certificates. To preserve this evidence, additional records

management procedures must be applied. These include trusted timestamps with another signatures, and audit logs. (See Annex B, section 7.7 on page B-9.)

h. Secure Mailing Lists

This 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). (See Annex B, section 7.8 on page B-10.)

i. Message Counter-signature

Message counter-signature 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. (See Annex B, section 7.9 on page B-10.)

j. Certificate Binding

This service allows for a certificate, which is sent with the message to be cryptographically bound to the message. (See Annex B, section 7.10 on page B-10.)

k. Compressed Data

The Compressed Data service reduces message size, which has several security benefits. (See Annex B, section 7.11 on page B-10.)

ACCOUNTABILITY

423. The MMHS shall ensure that all actions taken on a message from release by the originator to viewing by the recipient are recorded. Accountability in MMHS is provided procedurally as described in 413 and 438.

PROHIBITION OF PROBES

424. The MMHS shall prohibit the use of probes to prevent users from finding out information about potential recipients on the network without the knowledge of the recipient. This service shall be implemented by MMHS interface points into ACP 123 MHS domains to block probes from entering the ACP 123 MHS.

SECURITY CLASSIFICATION

425. The Security Labels service (see 4.II.422.f) provides the means to associate a security label with a message. The following procedures apply to use of MMHS security labels.

a. Responsibility

It is the responsibility of the originator to ensure that the proper classification is indicated on the message. A reply or reference to a classified message may be assigned a lower classification when the contents of the text of the message containing the reply or reference permits.

b. Classifications

Messages are to be classified TOP SECRET, SECRET, CONFIDENTIAL, or RESTRICTED whenever their content falls within the definition set forth in appropriate national regulations. Messages bearing no security classification should be marked UNCLASSIFIED or the abbreviation UNCLAS. The abbreviation of UNCLAS is valid only in conjunction with the procedural requirement to place the classification in the first line of text. If a X.411 security label is utilized, UNCLAS will be represented as UNCLASSIFIED with an integer value of 1. The security classification of a message shall be displayed to the user at all times during processing of the message. National regulations shall also dictate the policies for marking security classifications on individual paragraphs or body parts within a message.

c. Security Label

The security label assigned to the entire message will be that of the highest classification of any part of the message or the appropriate label for the aggregate of the information contained in the entire message including all body parts. The security label will be defined by a security policy. The determination as to whether it is national policy or a multi-national agreed policy is considered outside the scope of the ACP 123.

MM AND MT EOS INTERACTION WITH S/MIME SERVICES

426. Interaction of security services with certain MT, MM, and MS EoS require special considerations be taken in order to provide the EoS to the MTS users. Messages must be decrypted before any of the MM EoS may be provided to MTS users. The following clauses identify the considerations that shall be taken in order for MT and MM EoS to be provided in an S/MIME environment.

a. Alternate Recipient Allowed

This MT EoS enables an originating UA to specify that the message being submitted can be redirected or delivered to an alternate recipient. This MT EoS shall not be used as a means of access control as it cannot be assured that the recipient will not receive the message as the result of redirection, DL expansion, etc.

b. Blind Copy Recipients

This MM EoS enables the originator to provide the OR Descriptor of one or more additional recipients of the message being sent. These names are not disclosed to the primary, copy, or other blind copy recipients. This MM EoS shall not be used as a means of access control as it cannot be assured that the blind copy recipients will not be disclosed to other primary, copy, or blind copy recipients as the result of redirection, DL expansion, etc.

c. Clear Service

Security services provided according to the S/MIME profile cited in Annex B provide a security label, which includes the privacy mark, only when the message is signed. Clear service can only be provided if the message is signed.

d. Conversion

When a message is either encrypted or signed, conversion (whether implicit or explicit) will negate any security services that might have been provided. Message originators that encrypted or signed messages shall ensure that the Conversion Prohibition EoS is invoked thereby ensuring conversion does not take in the MTS. If the Explicit Conversion EoS is available to the user, the conversion prohibition in case of loss of information EoS shall not be invoked.

e. Deferred Delivery

The deferred delivery EoS may impose significant message delivery delays. If security services are applied, the originator shall ensure that their certificate is valid for the anticipated message delay period or the recipient may be unable to perform security processing upon message reception.

f. Exempted Addresses

This MM EoS is used to convey the names of members of an AL that the originator has specified are to be excluded from receiving the message. This EoS shall not be used as a means of access control as it cannot be assured that the exempted addresses will not receive the message as the result of redirection, DL expansion, etc.

g. Hold for Delivery

This MT EoS enables a recipient UA to request that the MTS hold its messages and returning notifications of delivery until later time. If security services are applied, the recipient shall ensure that the hold for delivery time is less than the anticipated validity period of the originator’s certificate or the recipient may be unable to perform security processing upon the message.

h. Redirection Disallowed by Originator

This MT EoS enables an originating UA to instruct the MTS that redirection should not be applied to this particular message. If the originator requests redirection be disallowed, the recipient may still specify an alternate recipient receive the message via an auto-forwarding service (i.e., this EoS does not guarantee delivery to only the intended recipient). See 4.I.419 for additional information.

i. Use of Distribution Lists

Originators should be aware of whom they are addressing messages and the recipients of the DL because a DL cannot be distinguished from another OR address. Where the DL is expanded is up to security policy.

j. Use of Alternate Redirection Mechanisms

In order to allow alternate recipients access to messages that have been encrypted with S/MIME security services and redirected through any of the alternate delivery mechanisms, the alternate recipients must possess the same key material as the original recipient or the alternate recipients key material must be transmitted with the message. The intended recipients key material is contained within a certificate and must be made available to the message originator. The following clauses specify additional procedural requirements dealing with the alternate delivery mechanisms that will ensure alternate recipients can access the messages.

(1) Originator Alternate Recipient – Use of this EoS in the S/MIME encryption environment requires the originator of the message to include the intended recipients and alternate recipients, if alternate key distribution methods have not been used for the alternate recipients, in the original message for the message to be decrypted by the specified recipient.

(2) Redirection of Incoming Messages – If the incoming message has been encrypted by S/MIME security services and is redirected to an alternate recipient, the alternate recipient is required to posses the same key material as the original recipient or the alternate recipient key material must be transmitted with the original incoming message if the alternate recipient requires access to the message. In addition, redirection of messages with confidentiality applied in the MTS can only be based on information in the message envelope.

(3) Alternate Recipient Assignment – When Alternate Recipient Assignment is used, the default mailbox administrator may be capable

of accessing the content of secure messages provided that adequate provisions have been made by the security infrastructure.

(4) MS Auto-forwarding – Because the security label of the message is unavailable to the MS, messages may be forwarded to a secondary recipient who is unable to process the message due to inconsistencies between the user authorizations and the message's security label. Recipients of the forwarded message may be capable of accessing the content of secure messages provided that adequate provisions have been made by the security infrastructure.

SECTION III
NAMING AND ADDRESSING

427. Users of MMHS are identified by OR Names, which consist of either an OR Address, a Directory Name, or both. The OR Address is used for routing messages to recipients within the Message Transfer Service, by locating MTAs required to take the message closer to its destination. In this way, the OR Address is related to the MTA Routing Architecture. Directory Names reflect the hierarchical structure of the users of MMHS. Although some of the attributes used in OR Addresses and Directory names may be the same (e.g., Organization name) there is not necessarily a one-to-one mapping between the values used for those attributes in the two contexts. In the absence of a Directory Name, the OR Address serves to name originators or recipients. Therefore, the distinction between Naming and Addressing is not always entirely clear.

O/R ADDRESSES

428. The Mnemonic and Numeric forms of OR Address (as defined by X.402) shall be supported by all MM-UA and MM-MS elements. OR Addresses shall be present in the P1, P3, and P7 envelopes and in the P772 content. The address support requirements for MTAs are addressed by AMH1n(D).

429. Guidelines for determining what goes in the Organization and Organizational Unit attributes and how these might be derived from the PLAs will be defined by policy of appropriate registration authorities. Registration authorities will be determined by national policy or multi-national agreement.

430. Two Military Domain Defined Attributes (DDAs) are used in interworking with the ACP 127 domain. Support for generating and displaying these DDAs when part of an OR Address is mandatory. The use of these DDAs is optional when defining the OR Address of any given user. If ACP 127 users are not registered in the MMHS, then those users will be identified by the OR Address of the ACP 127 gateway together with the PLAD or RI (or both) of the user. In such cases, the PLAD and RI of the user will be carried as DDAs. The use of these DDAs is transitional,

and may only be used while interworking with ACP 127 messaging is required. These Military DDAs are:

Domain Defined Attribute	Type	Value
PLAD	ACP-PLAD	ACP-address including but not limited to: PLADs, SMAs, AIGs, and CADs
RI	ACP-RI	Any ACP 127 RI, including collective RIs

431. The Domain Defined Attributes will not be used for inter-domain routing purposes.

DIRECTORY NAMES

432. A Directory Name can be used to identify originators and recipients in the content of messages within the MMHS in a more user-friendly manner than using OR Addresses. In order for messages to be delivered via the MTS, the correct OR Addresses must be present in the envelope (directory names alone are not sufficient). It is the responsibility of the originating domain to ensure that the correct OR Addresses are present. The directory name shall be present in both the envelope (i.e., P1, P3, and P7) and in the P772 content.

ADDRESS LISTS

433. This section addresses the unique requirements involved with shorthand methods of addressing lists of recipients. An AL is a form of military recipient designator representing a predetermined list of specific and frequently recurring combinations of primary and copy recipients. The purpose of ALs is to reduce the length of the address component. ALs can be used whenever suitable, irrespective of the classification of the message concerned or the security mechanism used. ALs may be carried as OR Names in the *primary-recipients* or *copy-recipients* fields, or in the *address-list-indicator* field. (See 2.II.212.k.)

a. List Expansion

The AL expansion is the responsibility of the originating domain except by agreement. For example, some ALs may be expanded in the recipient domain. List expansion shall consider associated exempted addresses. There are two types of mechanisms that can be used to perform list expansion. These are source expansion and remote expansion.

(1) Source Expansion – the originating UA performs expansion of ALs prior to submission. The expanded list of recipients shall be indicated within the content in the appropriate heading fields. Any exempted addresses (see clause 2.II.212.d) included in the heading shall be considered in the source expansion. Allowable variations of this mechanism allow the originator's MS or MTA to perform the expansion (i.e., in a client-server or other collocated environment)

provided that the expansion is performed prior to application of security mechanisms. When source expansion is used, the *address-list-indicator* field may be used to indicate the name(s) of the ALs used in the source expansion. Use of the *address-list-indicator* field to support this is for transition only.

(2) Remote Expansion – the originating UA addresses the message to a well defined OR address associated with the AL. Security mechanisms shall then be applied to protect the message en route to the AL expansion point. The message is then submitted and the MTS conveys the message to the AL expansion point. The AL expansion point shall examine the message and expand the AL. Any exempted addresses (see clause 2.II.212.d) included in the heading shall be considered in the expansion. Disruptions in the security mechanisms shall be minimized, and shall be limited to the extent necessary to allow the expanded list recipients to access the message. The MM content heading shall indicate the AL names themselves rather than the AL member names. The expanded list of recipients shall be indicated in the envelope.

b. Owner

Responsible commanders and authorities may request assignment of an AL to a fixed combination of recipients to which messages are frequently addressed. The command or authority requesting assignment of an AL will assign a cognizant authority to be the owner of that AL. The owner is responsible for maintaining the AL and reviewing it at least quarterly for continued requirement and necessary modification. Requests for permanent modifications by anyone other than the owner shall be forwarded to the owner to insure that the requested modifications do not detract from the intended use of the AL.

c. Notifications

If a Receipt or Non-receipt Notification is requested for a recipient specified as an AL, the notification returned indicates whether or not the list was successfully expanded and the originator had the appropriate submission privileges to use the AL as a recipient. The AL owner controls the policy of the AL, which indicates whether reports received about delivery to members of the list are forwarded to the originator of a message. The owner is discouraged from propagating reports from the members of the AL to the originator of the message.

d. Titles

A concise AL descriptive title may be included in the directory entry supporting the AL. Descriptive titles assigned to ALs do not preclude use of a

particular AL for other type messages, provided the text sufficiently identifies the message as other than that shown in the descriptive title.

e. Use

If all addressees of a particular message are not contained in any AL, the most appropriate AL may be selected and Primary or Copy recipient(s) may be added to or exempted from the address using the appropriate recipient designators. There is no limit upon the number of recipients that may be added to or exempted from the address of an AL. However, care must be taken not to create a longer recipient list using ALs and exemptions than would be required if individual recipient designators were used for all recipients. If the same list of recipients is to be added to or exempted from the composition of an AL regularly, the AL should be modified, or a second AL defined.

DIRECTORY SERVICES

434. The Directory service (also known as "the Directory") is expected to play a significant role in the successful implementation of the X.400-based MMHS. The ACP 133 will specify the Directory for use by MMHS. The Directory will support a number of critical functions that will be used to support everything from OR Name lookup to distribution of the user certificates necessary to support various encryption algorithms.

435. Registration Authorities shall be established following appropriate national procedures. Addressing information for registered MMHS users shall be published and made available to other MMHS users authorized to originate messages to them.

SECTION IV
MANAGEMENT

436. Military Messaging in MMHS will be possible by the interconnection of MMHS MDs within the different nations. The actual management of each of these MMHS MDs will follow national or local policy. However, some cooperation will be required in order to meet the quality of service requirements specified in this ACP.

ACCOUNTING POLICIES AND PROCEDURES

437. Bilateral agreements may need to be arranged to support requirements for accounting policies and procedures across national boundaries.

TRACE AND ACCOUNTABILITY

438. The MMHS is required to provide assurance that messages sent are received by the intended recipient(s), or that the originator is notified of any problems with delivery. During normal operation of the MMHS, messaging services are employed to satisfy this requirement. In the event of certain system failures, however, messaging services may not provide adequate assurance. Therefore, additional capabilities are required nationally to maintain an audit trail sufficient to provide inter-domain trace and accountability functions. To satisfy this requirement in the event of failures, it is recommended that several MMHS components log audit trail information. A management system shall provide the capability of accessing this audit trail and exchanging necessary trace information across international domain boundaries. Combining the allocation of responsibility for ensuring messages have been received, and the maintenance and management of audit trail information act in concert to provide accountability in the MMHS.

a. Accountability Requirements

Accountability will be provided to MMHS users by audit utilities and tracer actions. MMHS users should be assured that the MMHS will deliver messages in a timely manner to the intended recipients with the proper security mechanisms intact. If the MMHS does not perform these functions in a satisfactory manner, the user may request that system managers identify the portion of the system that that caused the degraded performance. The request will invoke audit utilities and tracer actions to provide system accountability. Note that across international domain boundaries, the resolution of the accountability is not required to extend below the domain level. Within nations boundaries, identification of the specific component, process, or user that caused the degradation may also be possible.

b. Audit Trail Information Management

Audit utilities will provide a detailed record of system activity to facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of messages, possible compromise of sensitive information, or denial of service. Local policy shall be developed that explains which actions are to be taken when discrepancies are found. The management function should be able to identify the following events:

- Messages delivered after the required Speed of Service time has elapsed
- Messages not retrieved from the MM-MS for a specified time
- Messages retrieved but not read for a specified time
- Messages submitted but not delivered
- Message signature verification failures

- Probe submissions or transfers attempted
- Peer-entity authentication failures
- User authentication failures
- Violations of the security policy.

Information shall be maintained by management system for ten (10) days.

c. Tracer Action

This paragraph describes how a tracer action can be initiated and under which circumstances it will be used. If acknowledgment of a message is requested and not received by an originator, then the user can request a tracer action. A tracer action may consist of a request for system operator assistance in examining whatever audit trail records are available. Alternatively, a system management function may be used by a system manager to access remote audit trail logs to determine the exact disposition of the message in question. Tracer actions should be initiated within ten (10) days of the perceived problem to facilitate usage of audit data stored on-line at local components; however, procedures and guidelines for initiating tracer actions may vary depending on the specific environment in question (e.g., multiple tactical environments, strategic environments).

d. Interdomain Trace Operations

If a domain can show from its audit logs that a message was successfully passed to another domain, the domain that passed the message forward should expect the receiving domain to provide assistance in tracing the message to the intended recipient. Bilateral agreements may be necessary to coordinate tracer actions across national boundaries. The interface points with other national systems shall maintain the information necessary to support interdomain message tracing and accountability.

PERFORMANCE MANAGEMENT

439. In order to meet the speed of service requirements each MD will be responsible for monitoring the performance of the MTS within its domain. This could be accomplished by either performance or fault monitoring. If faults occur that the transfer speeds can no longer be met within that MD, it may affect messages originating or destined for users in other MDs. Although these factors are strongly dependent on the overall system architecture, the management system will need to include procedures to ensure that these requirements are being met. The procedures should describe the actions that will be taken if problems are detected.

a. Transfer Delay

Transfer delay is the delay incurred during transmission of a message either through an individual MTA or through the MTS. MTA transfer delay is the difference between the time a message enters an MTA and the time the message leaves the MTA. MTS transfer delay is the difference between the message's submission and delivery time. The management system should strive to keep both MTS and MTA delays minimal to ensure that the speed of service goals are met.

b. Connection Establishment Delay

Connection delay is the time needed to establish the initial dialog between two platforms (e.g., MTA to MTA, MTA to MS, MTA to UA). This delay should be minimized to achieve the Grade of Delivery associated with the precedence level of the message.

c. Storage Availability

Various components, including primarily the MTA and MS, will require sufficient storage space for receiving and transferring messages. The management functions shall provide for the monitoring of available storage space. The management system shall initiate corrective action when storage availability falls below a nationally defined threshold.

CONFIGURATION MANAGEMENT

440. Configuration management will be performed according to national or local policy. However, bilateral agreements will be necessary to ensure that changes to the configuration of one nation's MTS which may impact the operation of another nation's MTS will be mutually agreed upon before implementation.

CHAPTER 5
PROFILES

501. Chapters 2 and 4 define the services provided in the MMHS and the policies and procedures to be used with these services. This chapter provides additional information about which of the services and procedures apply in specific military environments. In chapter 2 if an element of service is specified as optional, an implementation can still claim conformance to military messaging if it does not implement that service. In the following sections, if a profile states that some of those optional EoS shall be supported, an implementation cannot claim conformance to the specified profile without implementing those optional EoS.

502. If additional policies or procedures are required in order to conform to the specified profile, these additional requirements are also defined in this chapter.

SECTION I
TAXONOMY

503. The profiles specified by this ACP are organized according to a taxonomy similar to the International Standardized Profile (ISP) taxonomy defined by ISO/IEC TR 10000. The taxonomy defines the relationship between each of the profiles required to implement the MMHS. Two relevant types of profiles are included in the taxonomy: A-profiles which specify the requirements for connection-oriented applications, and F-profiles which specify the requirements for abstract information objects conveyed by A-profiles. If a requirement for connectionless application profile is identified it may be included as a B-profile. The relevant portions of the ACP taxonomy are depicted in Figure 5-1.

A-PROFILES

504. A-profiles define requirement for connection-oriented applications. The "MH" branch of the taxonomy identifies requirements for connection-oriented MHS applications. Each MHS application is assigned a number. Under each MH branch, there are three profiles to list the MMHS requirement on the three PDUs defined in X.400, MTA Transfer Protocol (P1), MTS Access Protocol (P3), and MS Access Protocol (P7). Two additional parts, which contain no profiles on their own, are also part of the multi-part profile to list common MMHS service support and MMHS requirements for Reliable Transfer Service Element (RTSE), Remote Operation Service Element (ROSE), Application Control Service Element (ACSE), and presentation and session protocols.

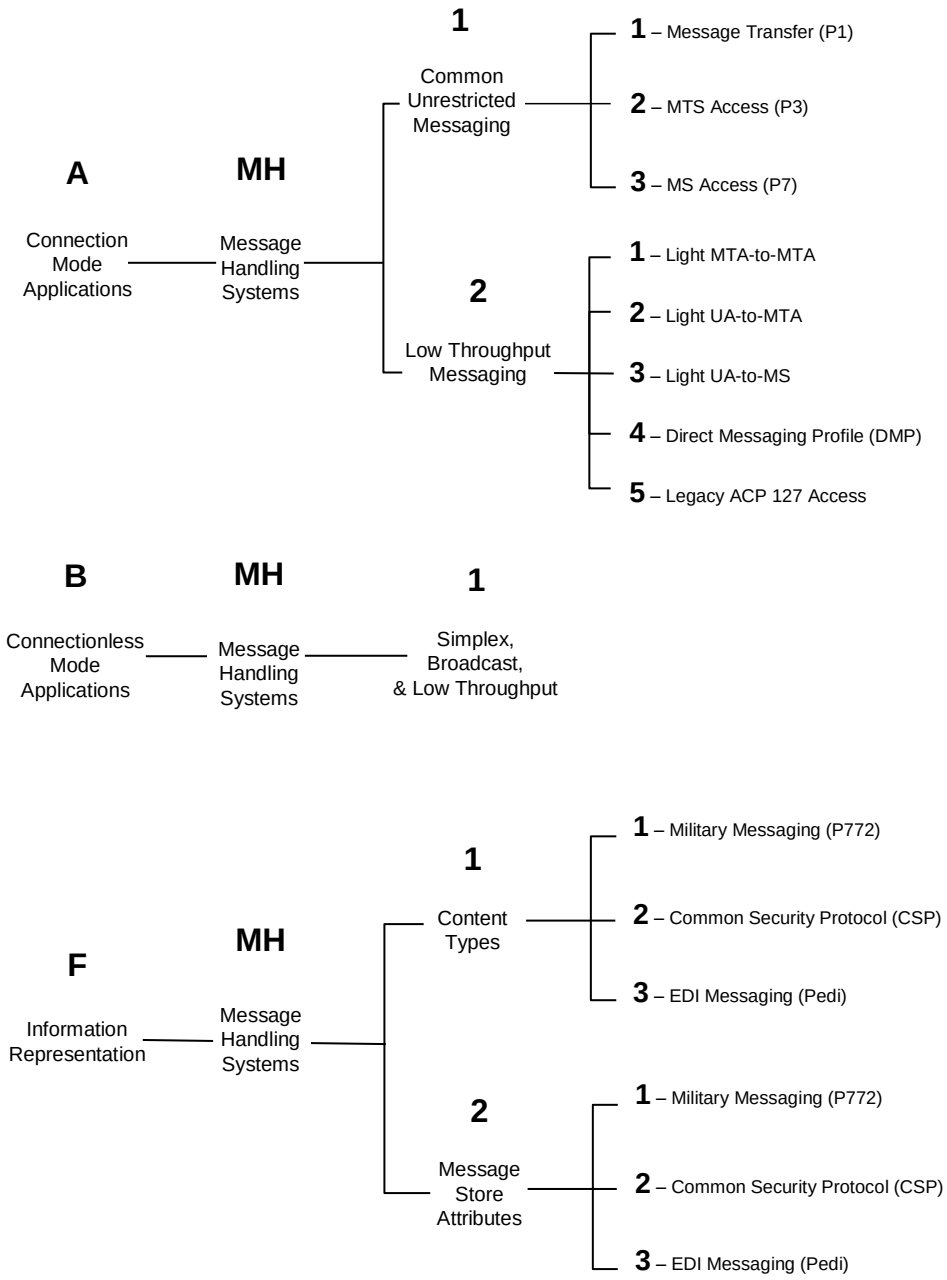


Figure 5-1 Profile Taxonomy

505. The ISO/IEC ISP 10611 defines a broadly recognized set of requirements for MHS support. The ISO/IEC ISP 10611, which is titled "Common Messaging", is a multi-part profile that specifies the requirements for the entire taxonomy branch AMH1n. The ISO/IEC ISP 10611 consists of the following 5 parts:

- Part 1 – MHS Service Support
- Part 2 – Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS
- Part 3 – AMH11 – MHS Requirements for Message Transfer (P1)
- Part 4 – AMH12 – MHS Requirements for MTS Access (P3)
- Part 5 – AMH13 – MHS Requirements for MS Access (P7).

506. For the Standard Profile described in 5.II, the number "1" has been assigned to the MMHS Common Unrestricted Messaging. The multi-part profile included in Annex C of this ACP is referred to as AMH1n(D)[7]. The A-profiles defined by this ACP are presented as "deltas" to the ISO/IEC ISP 10611. The multi-part profile has the following five parts:

- Part 1 – MHS Service Support
- Part 2 – Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MMHS
- Part 3 – AMH11(D) – MMHS Requirements for Message Transfer (P1)
- Part 4 – AMH12(D) – MMHS Requirements for MTS Access (P3)
- Part 5 – AMH13(D) – MMHS Requirements for MS Access (P7).

507. Other A-profiles may be included in later revisions to document MMHS Low-throughput Messaging[8].

B-PROFILES

508. If a requirement for a connectionless applications profile is identified the profile may be included as a B-profile.

---

7 The "D" stands for Defense.

8 This environment has yet to be defined; however, it is envisioned that it will embody connection-oriented applications constrained by low-thoughputs.

509. B-profiles list requirements on connectionless applications. The "MH" branch of the taxonomy identifies requirements for connectionless MHS applications. Each MHS application is assigned a number.

510. There are currently no civilian ISPs for connectionless MHS.

511. Future versions of this ACP may include a profile to document the requirements for the restricted profile described in 5.II.

F-PROFILES

512. F-profiles specify requirements for abstract information objects conveyed by A- and B-profiles. Abstract information objects conveyed by A- and B-profiles include: MM content type, and MS attributes.

513. This ACP specifies five F-profiles in Annexes D, F, and G as follows:

- ANNEX D: FMH11(D) – MM content (P772)
- ANNEX F: FMH20(D) – General MS Attributes
- ANNEX G: FMH21(D) – MM-specific MS Attributes

SECTION II
STANDARD PROFILE

PROFILE DEFINITION

514. This MMHS Standard Profile specifies any additional required behavior of Message Handling Systems providing the ability to perform Military Messaging in an environment essentially unrestricted by bandwidth considerations. The required characteristics of MMHS as specified in Chapters 2 and 4 of this document apply as the base requirements for Military Messaging. AMH1n(D) in Annex C specifies the standard profile. This is expected to be the normal environment for Military Messaging where services to satisfy standard military requirements for messaging are expected to be available to users of the system.

IMPLEMENTATION REQUIREMENTS

515. International messaging between nations is expected to be achieved via the following three types of interfaces:

- P1 interface
- P3 interface
- P7 interface

516. In order to promote basic interoperability, all nations are required to support the P1 interface requirements. Support for the P3 and P7 interface requirements are optional.

517. The following are conformance requirements for the three types of interfaces. Note profiles identified by the prefix "FMH" are information representation profiles for which conformance is strictly independent of the identified interface.

a. P1 Interface: Nations are required to demonstrate conformance to the following profiles:

- AMH11(D)
- FMH11(D)
- S/MIME Profile (Annex B)

b. P3 Interface: Nations are required to demonstrate conformance to the following profiles:

- AMH12(D)
- FMH11(D)
- S/MIME Profile (Annex B)

c. P7 Interface: Nations are required to demonstrate conformance to the following profiles:

- AMH13(D)
- FMH11(D)
- FMH20(D)
- FMH21(D)
- S/MIME Profile (Annex B)

d. P1 Interface: If Nations claim to support security services provide by ACP 120

- FMH12(D)

e. P3 Interface: If Nations claim to support security services provide by ACP 120

- FMH12(D)

f. P7 Interface: If Nations claim to support security services provide by ACP 120

- FMH12(D)
- FMH22(D)

SECTION III
RESTRICTED THROUGHPUT PROFILES

PROFILE DEFINITION

518. Based on the requirements for MMHS to function in tactical operational scenarios, this section defines a set of interoperability profiles that cover use of alternative protocol interfaces as defined in Annex E. These interfaces include alternative application layer messaging protocols and related lower layer protocols that have been adapted to suit the target environment. They also include use of data compression, encoding techniques, and alternative addressing. The target environment includes the assumption of communication channels that exhibit low thoughput and simplex operation.

IMPLEMENTATION REQUIREMENTS

519. Tactical messaging between nations is expected to be achieved via the following five types of interfaces:

- TMI-1: Light MTA-to-MTA
- TMI-2: Light UA-to-MTA
- TMI-3: Light UA-to-MS
- TMI-4: Light UA-to-UA
- TMI-5: ACP 127 AU to ACP 127 System

520. Support for the Restricted Profile of ACP 123 is optional. Nations claiming support for the Restricted Profile shall support the TMI-1 messaging interfaces as specified in Annex E.

521. The following are conformance requirements for the five types of interfaces. Note profiles identified by the prefix “FMH” are information representation profiles for which conformance is strictly independent of the identified interface.

a. TMI-1 Interface: Nations are required to demonstrate conformance to the following profiles:

- AMH11(D)

– FMH11(D)

– AMH21(D) (Annex E section 2.2.1)

b. TMI-2 Interface: Nations are required to demonstrate conformance to the following profiles:

– AMH12(D)

– FMH11(D)

– AMH22(D) (Annex E section 2.2.2)

c. TMI-3 Interface: Nations are required to demonstrate conformance to the following profiles:

– AMH13(D)

– FMH11(D)

– AMH23(D) (Annex E section 2.2.3)

d. TMI-4 Interface: Nations are required to demonstrate conformance to the following profiles:

– FMH11(D)

– AMH24(D) (Annex E section 2.2.4)

e. TMI-5 Interface: Nations are required to demonstrate conformance to the following profiles:

– AMH25(D) (Annex E section 2.2.5)

ANNEX A

MILITARY MESSAGING CONTENT TYPE

This annex is written as a delta document to the CCITT X.400 Series Recommendations, defining the enhancements and modifications to X.400 required for Military Messaging. This annex is aligned with the common text portions of Annex A of STANAG 4406 (excluding NATO-only text). Keeping the definition of the actual protocol for MM the same in both ACP 123 and STANAG 4406 ensures there is only one definition of the MM content type for use in the Allied community.

ANNEX A: MILITARY MESSAGE HANDLING SYSTEM EXTENSIONS

[Conforming systems SHALL comply with this annex.]

INTRODUCTION

The Military Base Standard (MBS) is defined by a set of extensions to the civilian Message Handling System standard [ITU-T X.400 | ISO/IEC 10021] which are required for Military Messaging (MM). This standard fully supports the Interpersonal Messaging defined in the civil X.400 standards (i.e. both P2 and P22 Content types) as well as the Military Messaging defined by these extensions.

The military extensions are achieved using the standard extension mechanisms defined in [ITU-T X.400 | ISO/IEC 10021]. This approach defines military-specific semantics in the extensions. The semantics of the civil standard are not changed. This STANAG does not redefine the civil semantics. It is therefore a superset approach of the civil standard. If nations have requirements for additional national or bilateral extensions they should adopt the same approach in developing a superset of the MBS.

In order to highlight the military extensions and avoid duplication of text in the civilian standards, a delta document approach has been taken. The sections of this annex follow the same structure as the civil MHS standard [ITU-T X.400 |ISO/IEC 10021-1] to which they correspond. Each of the sections of this Annex identifies any necessary extensions and restrictions to the corresponding section of the civil standard. This technique provides traceability and puts the delta text in context.

Unless exceptions are noted, all statements which apply to Interpersonal Messaging Services (IPMS) also apply to Military Messaging Services (MMS). The reader should therefore make this mental substitution when reading the

civilian standards which form the base upon which the military delta requirements are overlaid.

The military extensions to [ITU-T X.400 |ISO/IEC 10021] series of documents are summarized as follows:

MMHS Extensions of [ITU-T X.400 | ISO/IEC 10021-1]

This section identifies the extensions required to the System and Service Overview of MHS to accommodate MMHS. It includes an overview of the additional services and the specialized use of existing features;

MMHS Extensions of [ITU-T X.402 | ISO/IEC 10021-2]

This section identifies the extensions required to the Overall Architecture of MHS to accommodate MMHS. In particular the extensions required for naming and addressing are described here;

MMHS Extensions of [ITU-T X.407 | ISO/IEC 10021-3]

No extensions are necessary

MMHS Extensions of [ITU-T X.411 | ISO/IEC 10021-4]

This section identifies the extensions required to the Message Transfer System Definition and Procedures of MHS in order to support MMHS;

MMHS Extensions of [ITU-T X.413 | ISO/IEC 10021-5]

This section identifies the extensions required to the Message Store Abstract Service definition of MHS in order to support MMHS;

MMHS Extensions of [ITU-T X.419 | ISO/IEC 10021-6]

No extensions are necessary

MMHS Extensions of [ITU-T X.420 | ISO/IEC 10021-7]

This section identifies the extensions required to the Interpersonal Messaging System of MHS in order to support MMHS.

MMHS EXTENSIONS TO [ITU-T X.400 | ISO/IEC 10021-1]

SECTION 1 – INTRODUCTION

1 SCOPE AND FIELD OF APPLICATION

This standard pertains to the communications aspects of Military Message Handling. The local interfaces, such as the human computer interface, are not part of this standard.

2 REFERENCES

MMHS Intercept Interoperability Functional Profile

CCITT X.400(1984)

CCITT X.400(1988)

ITU-T X.400(1992)

MHS Implementors' Guide, Version 11

ACP 121

ACP 127

ACP 128

ACP 131

APP-3

3 DEFINITIONS

MMHS – Military Message Handling System - The purpose of MMHS is to convey military messages between [NATO/military] organizations or individuals.

MMS – Military Messaging Service - The purpose of MMS is to provide an electronic mail like service to staff units and individual users in military organizations which fulfills established military requirements for messaging systems.

MM – Military Message - The military information object supported by the MMS.

MMTA – Military Message Transfer Agent - The functional object that provides the store and forward transport of a MM.

MMTS – Military Messaging Message Transfer System -The functional object, composed of MMTA's, that conveys information objects to organizations, to subscribers, or to distribution list members.

MM-UA – Military Messaging User Agent - The functional object by means of which an organization or subscriber engages in military message handling.

MM-AU – Military Messaging Access Unit - The functional object that links another communication system to the MMTS.

MM-MS – Military Messaging Message Store - The functional object that provides an organization or subscriber with capabilities for message storage and retrieval.

SECTION 2 – GENERAL DESCRIPTION OF MHS

7 FUNCTIONAL MODEL OF MHS

8 THE MESSAGE TRANSFER SERVICE

One of the principal reasons for developing MMHS as an extension of MHS is to minimize cost by taking advantage of well-known standards and their related products. It is, therefore, desirable to minimize, and if possible eliminate, any extensions to the P1 protocol as specified in the civilian standards. Also, in order to promote interoperability with other MHS-based systems, it is desirable to incorporate MMHS extensions not as reinterpretations of existing services and protocol elements but as new fields and elements. These are sometimes competing mandates. The MMHS extensions are identified as deltas to [ITU-T X.411 | ISO/IEC 10021-4].

9 THE MM SERVICE

The Military Messaging Service (MM Service) is similar to the IPM Service defined in the civilian standards. It includes extensions for services required in the military environment. These extensions are defined in the MM Extensions to [ITU-T X.420 | ISO/IEC 10021-7].

9.1 MM Service Functional Model

The MM service functional model is slightly different from the one defined in [ITU-T X.400 | ISO/IEC 10021-1]. The MM service functional model is shown in Figure A-1. Interoperability with ACP 127 and civilian MHS systems is included. The access units for Teletex and Telex are not included. The MM service provides messaging between organizations, between persons and between persons and organizations.

9.2 Structure of Military Messages

The structure of military messages is fundamentally the same as that of IP-messages. Additional elements in the Heading are required to support MM. In order to support this extended message structure, military messages will form their own content type, called P772, as shown in figure A-2. This is distinct from the IPMS content type, called P22.

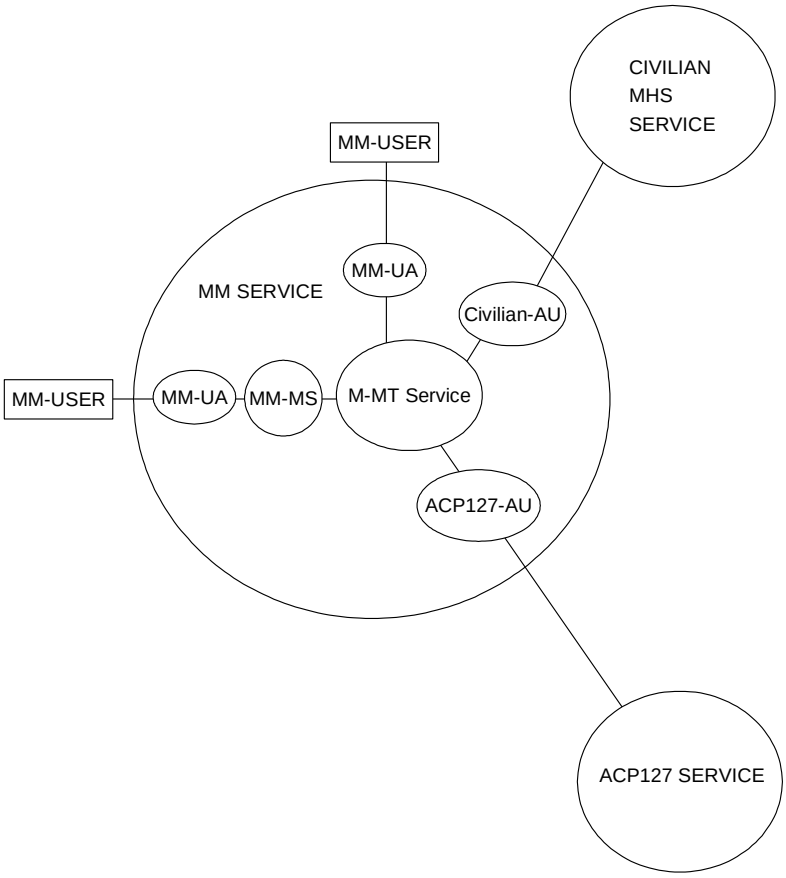


Figure A-1 – [ITU-T X.400 | ISO/IEC 10021-1] MM Extensions

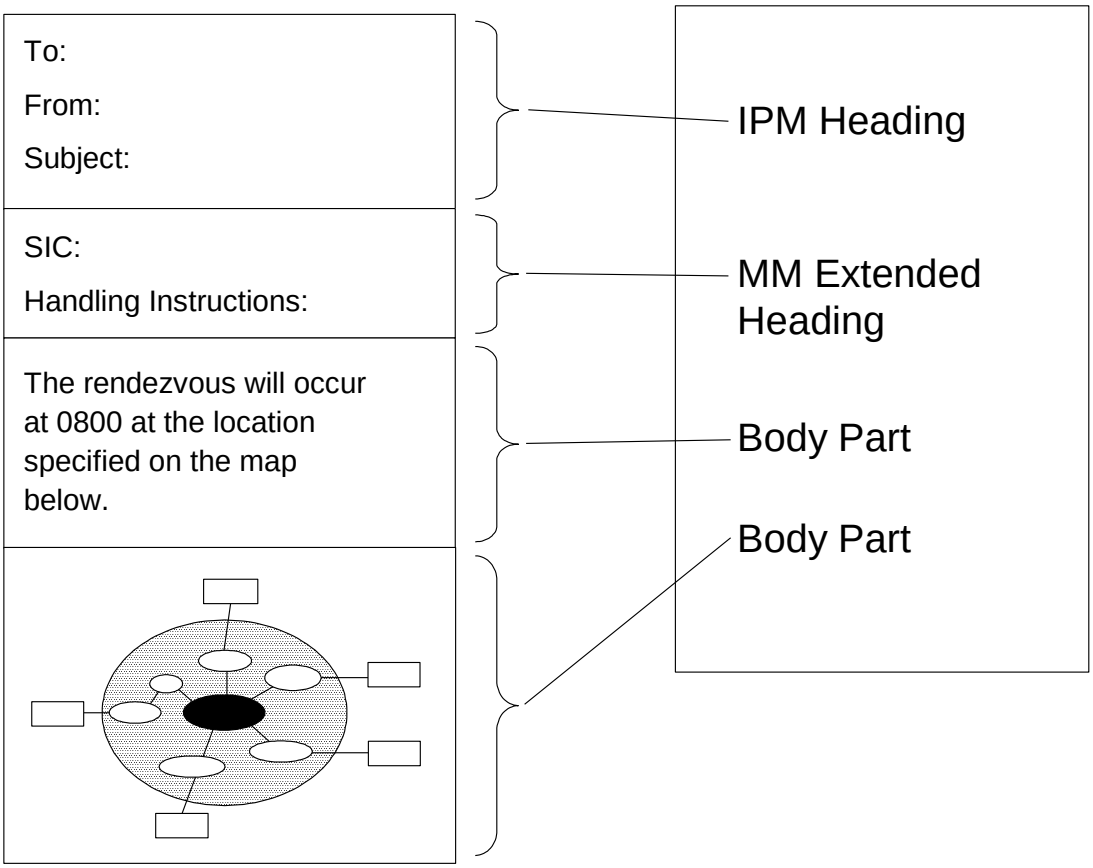


Figure A- 2 : MM Message Structure

11 SPECIALIZED ACCESS

11.1 Introduction

The MM Service includes access to ACP 127 and Civilian MHS systems. Access to such systems is via a specialized AU, which acts as a gateway.

11.2 Teletex Access

Direct access to teletex is not within the scope of MMHS.

11.3 Telex Access

Direct access to telex is not within the scope of MMHS.

SECTION 3 – CAPABILITIES OF MHS

12 NAMING AND ADDRESSING

12.4 O/R Addresses

Military O/R Address: Provides a means of identifying originators and recipients by organizational identity. In ACP 127 networks this is done using Plain Language Address Designators (PLAD). Nations may choose their own addressing scheme within their PRMD. For full interworking between MMHS and ACP 127 networks organizations must be registered in both networks.

14 DISTRIBUTION LISTS IN MHS

16 CONVERSION IN MHS

17 USE OF MHS IN PROVISION OF PUBLIC SERVICES

The requirements of clause 17 of X.400 do not apply to MMHS. (MMHS does not provide a public mail service.)

SECTION 4 – ELEMENTS OF SERVICE

18 PURPOSE

This part specifies the military specific elements of service. Different military messaging services will be built by selecting elements of service from the military specific UA elements of service, normal ISO/IEC 10021 IPMS UA elements of service and the MT elements of service. The selection of supported elements of service is defined in related MMHS Profiles.

The Military Messaging Service (MMS) is one of the services. The military specific elements of service for the MMS are described in the amendments to Annex B of [ITU-T X.400 | ISO/IEC 10021-1]. They are summarized in Table 1. In this table the "ACP" column indicates a service which is required solely to support interoperability with ACP 127 based networks.

Specific MM Element	ACP	STANAG CLAUSE
ACP 127 Message Identifier	x	B.116
ACP 127 Notification Request	x	B.118
ACP 127 Notification Response	x	B.119
Use of Address List		B.104
Clear service		B.112
Codress message indicator	x	B.110
Copy precedence		B.102
Corrections	x	B.114

Specific MM Element	ACP	STANAG CLAUSE
Distribution code		B.107
Exempted addresses		B.105
Extended authorization info (DTG)		B.106
Extended grades of delivery		B.100
Security information labels		B.120
Message instructions		B.109
Message type		B.103
Handling instructions	x	B.108
Originator reference		B.111
Originator PLAD	x	B.117
Other recipient indicator		B.113
Pilot forwarded	x	B.115
Primary precedence		B.101

Table 1 – Military Specific Elements of Service for MMS

19 CLASSIFICATION

ANNEXES TO [ITU-T X.400 | ISO/IEC 10021-1]

EXTENSIONS TO ANNEX A – Glossary of Terms

Military Messaging Service

The Military Messaging Service (MMS) provides an electronic mail facility between military personal and military organizational users. This service is a superset of the commercial IPMS in which the O/R name and UA can be dedicated to either an individual, or to an organizational post, irrespective of the identity of personnel involved. This service is sometimes known as "Formal Messaging" or "Record Traffic".

Military Messaging User Agent

The Military Messaging User Agent (MM-UA) is the entity that represents a military individual or organization within the MMS.

MMS Protocol

The MMS protocol supports the exchange of messages between military individuals or organizations. The nomenclature adopted for this protocol is P772.

Military Message Transfer Service

The MMTS provides a store and forward service which supports the exchange of military messages. It clarifies the behaviour of an MTA for military purposes.

Miscellaneous Terms

In addition to the abbreviations in the references, MMHS documentation also uses the following abbreviations:

ACCIS	Automatic Command and Control Information System
ACP	Allied Communications Publications
ACCSA	Allied Communications and Computer Security Agency
ADatP	Allied Data Processing Publications
AIG	Address Indicator Group
AL	Address List
CAD	Collective Address Designator
CCIS	Command and Control Information System
CEN/CENELEC	Joint European Standards Institution
CL	Classification Word(s)
CMS	Conferencing Messaging System
CMW	Compartmented Mode Workstation
COMPUSEC	Computer Security
COMSEC	Communications Security
DES	Data Encryption Standard
DTG	Date Time Group
ENV	European Pre-standard
MBS	Military Base Standard
MLA	Mail List Agent
MLS	Multi Level Secure
MMHS	Military Message Handling System
MM	Military Message
MM-	Military Messaging
MM-AU	Military Messaging Access Unit
MMI	Man Machine Interface
MM-MS	Military Messaging Message Store
MM-MTS	Military Messaging Message Transfer Service
MMS	Military Messaging Service
MM-UA	Military Messaging User Agent

MMTA	Military Message Transfer Agent
MPDU	Military Protocol Data Unit
P772	MMS protocol
PLAD	Plain Language Address Designator
PTT	Public Telephone and Telegraph
RI	Routing Indicator
SOTF	Start of Transmission Function
SW	Security Warning Operating Signal
UTC	Coordinated Universal Time

Double Enveloping

Double enveloping is a technique consisting of encapsulating the content and envelope of a message in a new outer envelope. This is done in order to protect the information borne on the envelope whenever a message is forwarded through a less trusted domain. The content of the new outer envelope, which is the inner envelope and in turn the original content, may be either encrypted or not depending on the degree of trust accorded the less trusted domain.

Plain Language Address Designator

The Plain Language Address Designator (PLAD) is defined in ACP 127 and is used for naming organizations in ACP 127 networks.

Routing Indicator

The Routing Indicator (RI) is defined in ACP 127 and is used to define the network address of a ComCen serving an organization or organizations. It is used for addressing and routing purposes within ACP 127 networks.

Priority and Precedence

The term "precedence" is used in reference to any military enhanced specification of message urgency. The terms "Primary Precedence", "Copy Precedence" are used to denote military precedence service definitions.

Address List

An address list in MMHS is a predefined list of recipients which is expanded by either the originating or receiving MMHS management domains depending on AL expansion policy.

Mail List Agent

A mail list agent is a specific entity of the MM-MTS in charge of the expansion of address lists. The MLA has to open the P772 message if it wants to access

to AL address information in the P772 extensions. So the MLA can be considered as a special Access Unit with its associated MTA.

EXTENSIONS TO ANNEX B – DEFINITION OF ELEMENTS OF SERVICE

Extended IPM services

MMS supports all of the IPMS services. MMS also supports the elements of service that are part of the basic MT (Message Transfer) Service. These are used to transfer military message and are available as part of the basic MM service. As part of MMS some interpersonal services require more precise definition which are included in this Annex.

B.37 MM-message Identification

This element of service permits co-operating MM-UAs to convey an identifier for each message sent or received. The MMS identification provides a unique identification of the MM-UA-message as follows:

- the O/R name of the originating MM-UA (mandatory), including the O/R address and all components of the global domain identifier.

- a serial number generated by the organization MM-UA (mandatory).

- the filing time (the time the message generation is finished) generated by the organization MM-UA (mandatory). This time is specified in UTC format including seconds.

Note: the serial number and the filing time are concatenated in sequence within the printable string of the MM-message identification, separated by a space.

B.43 Message Security Labelling

Security labeling in MMHS shall comply with the provisions of Annex B. Use of envelope fields for security labeling is now deprecated.

B.62 Primary and Copy Recipients Indication

Primary and copy recipients correspond respectively to what is normally referred to in ACP 127 as action and information addressee. In MMS, therefore, a primary recipient has responsibility to act upon the delivered

message, while a copy recipient has no action responsibility and is sent the message merely for information purposes.

B.72 Reply Request Indication

This element of service allows the originator to request a reply to a message. This can be used to support the procedures of a military acknowledgment, which is requested within the body of the message. Military acknowledgment is procedurally defined, examples of which are given in ACP 121, and means that the message to which it refers has been received and the purpose is understood by the recipient.

B.90 Typed Body

This element of service has been extended in MMHS, to support additional body part types. The additional body part types are defined in section 7.3.12 of MMHS extensions to [ITU-T X.420|ISO/IEC 10021-7].

B.93 User/MM-UA Capabilities Registration

A user shall not be able to change registered security labels. This is a management function.

The remaining text in Annex B summarizes the military extensions to ISO/IEC 10021:

B.101 Primary Precedence

This element of service enables an originating MM-UA to convey the military precedence level of a message in the content header for a primary recipient. This service is provided not only as information from originator-to-recipient, but is also used to automatically select the MTS Grade of Delivery element of service. This service is supported by the Miltiary Header Extension primaryPrecedence. The six levels of precedence are mapped to the three levels of Grade of Delivery. Military precedence is mapped to the MTS Priority protocol element as follows.

MANDATORY MTS	
Primary Precedence	**Priority**
Override	Urgent(2)
Flash	Urgent(2)
Immediate	Normal(0)
Priority	Normal(0)

Routine	Non-Urgent(1)
Deferred	Non-Urgent(1)

Note: Additional levels of precedence may be defined for national use. Upon receipt, the handling of unknown precedence levels will be dictated by the local handling policy.

B.102 Copy Precedence

This element of service enables an originating MM-UA to convey the additional precedences of a message in the heading for a copy recipient. The copy precedence has the same range of values as the primary precedence but must assume for each message a value equal to or lower than the primary precedence. The copy precedence does not affect the handling of the message by the MM-MTS.

B.103 Message type

This element of service enables originating MM-UAs to distinguish messages that relate to a specific exercise, operation , project or drill.

B.104 Use of Address List

This element of service:

- conveys the name of a pre-defined list of recipients to which the originator has sent a message.
- specifies if the address list (AL) was sent as action or information.
- defines if notifications or replies are required from action and/or info recipients of the address list.

Two alternative protocol realizations may support this service: use of MMS addressing fields for conveyance of the AL, and conveyance of the AL in the addressListIndicator heading extension. Of these two realizations, the addressListIndicator form is deprecated. National systems are expected to continue existing use of the address list indicator (ALI) in the short term.

The expansion of the AL will be performed by either the originating or receiving MMHS management domains depending on AL expansion policy, which will create an X.400 MMTS recipient for each member of the AL not excluded, but will not create separate OR descriptors for each member of the AL in the heading fields.

B.105 Exempted addresses

This element of service is used to convey the names of members of an AL that the originator has specified he wants to be excluded from receiving the message. Exclusion is provided in its AL expansion by either the originating or receiving MMHS management domains depending on AL expansion policy. No further processing is performed in MMHS and the element of service is information conveying only. There is therefore no guarantee that the exempted addresses will not receive the message as the result of redirection, DL expansion, etc.

B.106 Extended authorization info

This element of service consists of a Date-Time Group (DTG). Depending upon national requirements, the DTG may indicate either the date and time when the message was officially released by the releasing officer or the date and time when the message was handed into a communications facility for transmission.

B.107 Distribution Code

This element of service enables the originating MM-UA to give distribution information to a recipient MM-UA. The recipient MM-UA can use this information to perform local distribution of a message. This service contains two components, the Subject Indicator code (SIC) and a Distribution Code, each of which is optional. The Distribution Code allows for future definitions of distribution criteria by either national or allied use. Any number of codes may be specified. The assignment of the Distribution Code can be privately defined or may be subject to future standardization. The SIC's are published codes that provide information for message distribution after delivery to the recipient organization.

Each SIC can consist of between 3 and 8 characters. It is possible to attach upto 8 SICs to a message.

B.108 Handling instructions

This element of service enables the originating MM-UA to indicate to the recipient MM-UAs that local handling instructions accompany the message, and that the message requires manual handling by a traffic operator.

Handling instructions (also called transmission instructions) are a part of format line 4 as defined in ACP 127, and concern the sending of the message, e.g. that a particular system shall be used for transfer of the message.

B.109 Message instructions

This element of service enables the originating MM-UA to indicate to the recipient MM-UA that message instructions accompany the message. (Message instructions are also called remarks.) It may be used to carry operating signals specified in ACP 131 and related national publications.

The difference between Handling instructions and Message instructions is that the former is only for manual handling by traffic operators, while the latter also contains information of interest to the persons reading the message.

B.110 Codress message indicator

This element of service enables the originating MM-UA to indicate to the recipient MM-UA that the message is in codress format. The element of service applies only for codress encrypted messages, which are restricted to a single body part.

As defined in ACP 121 , "Codress is a procedure in which the entire address of a message is encrypted within the text while the heading of any transmission of that message contains only information necessary to enable communication personnel to handle it properly. Codress may be implemented by a nation, service or appropriate allied authority for use with high grade off-line cryptosystems".

B.111 Originator Reference

This service enables the originating MM-UA to indicate to a recipient MM-UA a reference called the "originator's number". The originator's number is used by the originating organizational unit. The originator's number differs from the MM-message identification in that this reference is wholly supplied by the originator while the MM-message Identification is supplied by the MM-UA.

B.112 Clear Service

This element of service indicates to the recipient MM-UA that a message containing classified information has been transmitted over an unsecure channel, prior to entering the security domain and may have been compromised. The service shall be supported by using the printable string "CLEAR" in the privacy mark, together with an appropriate security policy identifier. The fact that the message may have been compromised shall be made available to the recipient.

The service may be used locally within the MMHS domains, when permitted by the security policy of the security domain. In this case the message originator may submit a message with a lower security level or without its full security protection mecahnisms being involved. In these circumstances the clear service may be supported by using a specific security label, together with an appropriate security policy identifier.

B.113 Other recipient indicator

This element of service enables the originator to indicate to the recipient the names of one or more recipients, as well as the category (primary or copy) in which they are placed, that are intended to receive or have received the message via other means. The intent of this element of service is to enable a recipient to determine which recipients are intended to receive the message without the use of MMHS, as well as the category in which they are placed. While the Primary and Copy Recipients Indication and/or Address List Indicator gives the names of recipients that can be reached through MMHS, other recipients can be determined with this element of service.

Note: This element of service gives no reason why the other recipient(s) will not receive the message through MMHS.

Some reasons might be:

a. the recipient is not a user of the MMHS and has been sent the message by other means;

b. the originator knows (or presumes) that a secure path to the recipient will not be found through the MMHS and has therefore sent the message by other means; and

c. the recipient has already received the message by other means before it was entered in the MMHS.

B.114 Corrections

This ACP 127 element of service enables the originating MM-UA to indicate to the recipient that there are corrections required to the text body. This service is implemented by defining an Extended Body part of type Corrections.

B.115 Pilot forwarded

This element of service is intended for use with ACP 127 gateways and allows a gateway to translate a pilot message. The original received "body/text" of the message is sent as the "text body" of a new message. Pilot Information contains information which equals or supersedes the received header information for precedence, classification, local handling instructions and addressing.

B.116 ACP 127 Message Identifier

This element of service conveys the message identifier of an ACP 127 message in MMHS. This consists of the RI of the originating commcen, the Station Serial Number and the Filing Time which is conveyed in Format Line 3.

This element of service is only required to support the tandeming of ACP 127 messages through the MMHS domains.

B.117 Originator PLAD

This element of service enables the originator MM-UA to indicate to a recipient MM-UA or ACP 127 Access Unit the plain language address, as defined in ACP 127, of the originator of the message. Its purpose is to provide a consistent non-translated reference across the domain types.

This element of service, together with the Extended Authorization Info element of service, provides a cross reference for message identification in both ACP 127 and MMHS domains.

B.118 ACP 127 Notification Request

This element of service enables the originator to request notifications from ACP 127 gateways. They can be requested for the following scenarios:

a) positive notification - the ACP 127 gateway successfully transfers the message and accepts responsibility for its submission into the ACP 127 domain;

b) negative notification - the ACP 127 gateway has received the message, but fails to transfer it; and

c) transfer notification - the ACP 127 gateway successfully transfers the message but has not kept a record of the message and does not accept responsibility for it.

B.119 ACP 127 Notification Response

This element of service conveys the results of an attempt to transfer a message into an ACP 127 domain. It indicates whether the transfer was positive, negative, or positive but without responsibility. It also conveys the receipt time, the ALs of the message, the ACP 127 recipient address, and any pertinent supplementary information.

B.120 Security Information Labels

This element of service allows the originator of a military message to convey an indication of the sensitivity of the message, and individual parts of the message to all recipients of the message. The indication takes the form of security labels, which are assigned to the whole military message content, and potentially to the MM-message header and individual MM-message body parts.

Note: Unless both end systems have mutual trust in each end system’s ability to process and separate information based on security labels, this label should not be used to implement mandatory access control. How mutual trust is established is outside the scope of this document.

Note: The clear service of ACP 127 may be provided by interpretation of the values of the Information label. The clear service is defined in B.112.

Note: The Security Information Labels element of service is now deprecated. Its use is, therefore, discouraged. See STANAG 4406 Annex B for instruction on the use of its replacement, the ESSSecurityLabel.

MMHS EXTENSIONS TO [ITU-T X.402 | ISO/IEC 10021-2]

SECTION 2 – ABSTRACT MODELS

7 FUNCTIONAL MODEL

7.4 Selected AU Types

An AU is used as the interface between an MMHS and an ACP 127 system.

SECTION 4 – NAMING, ADDRESSING AND ROUTING

18 ADDRESSING

18.5 O/R Address Forms

18.5.5 MMHS O/R Address

An MMHS O/R address may contain an RI, a PLAD, or both.

An important objective of the MMHS is to provide functionality consistent with ACP 127. This has implications for MMHS addressing in that the existing ACP 127 addressing scheme based on RI's, PLAD's and address lists (address groups) must be accommodated.

A second objective is to provide an addressing mechanism which goes beyond the organizational level, the level supported by ACP 127, and supports direct organizational unit or personal addressing.

A third objective is to allow inter-operability between MMHS and civilian messaging networks. This implies that the MMHS addressing scheme must be a compatible superset of the civilian one.

These objectives have been met with a single O/R addressing scheme.

18.5.5.1 MMHS OR-Addressing

The main idea behind the MMHS addressing scheme is to use only the standard attribute list as defined in the base standard as routing attributes within the MTS.

The appropriate Military Registration Authorities will register MMHS O/R Names, which may be based on existing PLADs and RIs, or any other address information, such as staff cell name, role name or staff title.

Existing military names and addresses for message handling defined in the ACP publication (i.e. PLAD's and RI's) can be conveyed intact within the military domain defined attributes of the O/R Address.

Standard Attribute List

Military Domain Defined Attribute List

Domain Defined Attribute	Type Value
RI	"acp-ri"
PLAD	"acp-plad"

MMHS EXTENSIONS TO [ITU-T X.411 | ISO/IEC 10021-4]

SECTION 1 – INTRODUCTION

2 References

ACP 121 Transmission Instructions
ACP 127 Message Relay Procedures

SECTION 2 – MESSAGE TRANSFER SYSTEM ABSTRACT SERVICE

8 Message Transfer System Abstract Service Definition

8.2 Submission Port

8.2.1 Abstract Operations

8.2.1.1 Message Submission

8.2.1.1.1.8 Priority

Military Precedence should be mapped on to the civilian message priority in the following manner.

Military Precedence	Civilian Priority
Deferred	Non-Urgent
Routine	Non-Urgent
Priority	Normal
Immediate	Normal
Flash	Urgent
Override	Urgent

8.2.1.1.1.30 Message-security-label

NOTE: Use of the message security label in the envelope is now deprecated. Its use is, therefore, discouraged. See STANAG 4406 Annex B for instruction on the use of its replacement, the ESSSecurityLabel.

8.2.1.1.1.34 Content-type

This Annex identifies the following additional content types:

Military-messaging-1988: identifies the military-messaging-1988 content-type defined in the MMHS extensions to [ITU-T X.420 | ISO/IEC 10021-7].

8.2.1.4 Submission Control

8.2.1.4.2 Permissable Operations

The MMTS should tell the MMTS user that submission of probes is prohibited.

9. Message transfer system abstract syntax definition

```
-- OR Names
-- Domain-defined attributes

-- Domain Defined Attribute   Type Value
--    RI                  "acp-ri"
--    PLAD                "acp-plad"
-- others to be defined
```

SECTION 3 – MESSAGE TRANSFER AGENT ABSTRACT SERVICE

12 Message Transfer Agent Abstract Service Definition

12.2 Transfer Port

12.2.1 Abstract Operations

12.2.1.1 Message Transfer

When relaying, all attributes in an OR Address should be relayed. Specifically, all occurrences of Domain Defined Attributes shall be relayed. Domain Defined Attributes are not used for interdomain routing.

12.2.1.2 Probe Transfer

Submission of probes is not permitted, nor is transfer of probes via gateways to other networks. They should not occur in the MMTS.The occurrence of probes shall be audited.

13 Message Transfer Agent Abstract Syntax Definition

SECTION 4 – PROCEDURES FOR DISTRIBUTED OPERATION OF THE MTS

14 Procedures for Distributed Operation of the MTS

14.3 Main Module

14.3.10 Distribution List Expansion Procedure

DL owners should be able to optionally request delivery/non-delivery reports for all the DL's members.

14.4 Report Module

14.4.3 Report Generation Procedure

When copying an ORName of an incoming message into a DeliveryReportMPDU (e.g. the originator of the original message), all attributes (also UNSUPPORTED attributes) should be copied.

ANNEXES TO [ITU-T X.411 | ISO/IEC 10021-4]

ANNEX A – Reference Definition of MTS Object Identifiers

```
id-nato-mmhs-cont-mm84 OBJECT IDENTIFIER
      ::= {id-mcont 0}

id-nato-mmhs-cont-mm88 OBJECT IDENTIFIER
      ::= {id-mcont 1}

id-nato-mmhs-cat-atomal OBJECT IDENTIFIER
      ::= {id-cat 1}                -- This value is deprecated.

id-nato-mmhs-cat-cryptosecurity OBJECT IDENTIFIER
      ::= {id-cat 2}                -- This value is deprecated.

id-nato-mmhs-cat-specialhandlingintel OBJECT IDENTIFIER
      ::= {id-cat 3}                -- This value is deprecated.

id-nato-mmhs-cat-ussiopesi OBJECT IDENTIFIER
      ::= {id-cat 4}                -- This value is deprecated.

id-nato-mmhs-cat-eyesonly OBJECT IDENTIFIER
      ::= {id-cat 5}                -- This value is deprecated.

id-nato-mmhs-cat-exclusive OBJECT IDENTIFIER
      ::= {id-cat 6}                -- This value is deprecated.

id-nato-mmhs-cat-information-label OBJECT IDENTIFIER
      ::= {id-cat 7}                -- This value is deprecated.
```

ANNEX D – Conformance

Dynamic conformance statements

The "priority" element of the PDUs is dynamically mandatory.

MMHS EXTENSIONS TO [ITU-T X.413 | ISO/IEC 10021-5]

SECTION 2 – MESSAGE STORE ABSTRACT SERVICE DEFINITION

6 MESSAGE STORE MODEL

6.4 Stored-messages

c) Processed - means that the MM-UA has "completely fetched" the message and made the contents available to the user. Auto-actions which would result in the message being deleted are prohibited.

MMHS EXTENSIONS TO [ITU-T X.420 | ISO/IEC 10021-7]

MMHS EXTENSIONS FOR P772 PROTOCOL

SECTION 1 – INTRODUCTION

The Military Messaging Service (MMS) is a new service which is based on the Interpersonal Messaging Service (IPMS) specification, defined by the ITU-T X.420 Recommendation and International Standard ISO/IEC 10021-7.

1 SCOPE

The specification of the Military Messaging Service (MMS) is defined as a delta from the civilian Interpersonal Messaging Service (IPMS). When reading the civilian standard [ITU-T X.420 | ISO/IEC 10021/7] which forms the baseline, the reader should therefore substitute "MMS" for "IPMS".

2 REFERENCES

See MMHS Extensions to [ITU-T X.400 | ISO/IEC 10021-1]

3 DEFINITIONS

See MMHS Extensions to [ITU-T X.400 | ISO/IEC 10021-1]

4 ABBREVIATIONS

See MMHS Extensions to [ITU-T X.400 | ISO/IEC 10021-1]

SECTION 2 – ABSTRACT INFORMATION OBJECTS

7 MILITARY MESSAGES

7.1 Heading Field Component Types

7.1.1 MM Identifier

NOTE: The IPMIdentifier protocol element shall be used in respect of mandatory support in order to acheive the global Military Message identification requirement.

NOTE: The O/R Name of the originating MM-UA shall include the O/R Address and all components of the global domain identifier.

User	-	the O/R name of the originating MM-UA (mandatory), including all components of the global domain identifier
LocalIPMIdentifier	-	a serial number generated by the originating MM-UA (mandatory)
	-	the filing time (the time the message generation is finished) generated by the originating MM-UA (mandatory). This time is specified in UTC format including seconds.

NOTE: the serial number and the filing time are concatenated in sequence within the printable string of the IP-message identification, separated by a space.

NOTE: The LocalIPMIdentifier as part of the IPMIdentifier is defined as a printable string and it should be handled as such. It is recommended not to interpret the serial number as a number.

7.1.2 Recipient Specifier

A given recipient may be reachable only via a gateway between MMHS and ACP 127 domains. A per-recipient extension has been defined to permit the originator to request that if such a gateway is encountered then it should generate a notification identifying the level of success in translating the message. A description of these levels is provided in Section 8.4. The detailed specification is provided in Annex A. It makes use of the recipient-extensions component of the RecipientSpecifier.

7.2 Heading Fields

7.2.17 Extensions

Header extensions for MMHS are defined in ANNEX A. Nations may define additional header extensions for private use. Support of Nationally defined header extensions across National boundaries are subject to bilateral agreements. Unsupported header extensions may be ignored by an MM-UA on reception.

7.3 Body Part Types

7.3.8 Message

A message body represents an IPM body. If security is used then its delivery envelope is included in the body part.

An MM-UA can forward an MM-message in the MM-message body part and/or an IPM message using the message body part.

7.3.12 Externally Defined

Externally defined body part types for MMHS are listed in ANNEX B. They include body part types:

1) ADatP3;
2) Corrections;
3) Forwarded-Encrypted;
4) MM-Message; and
5) ACP127Data.

7.3.12.1 ADatP3

The ADatP3 body part will be used to convey military ADatP3 messages or sometimes refered to as proforma messages.

The text in the ADatP-3 body part can be delimited by carriage return/line feed or can be set oriented. The ADatP-3 body part also includes the message index reference number for identification of the ADatP-3 message type.

7.3.12.2 Corrections

Corrections body part will be used to convey corrections to a message, which maybe conveyed in another body part type.

7.3.12.3 Forwarded Encrypted

The forwarded encrypted body part will be used to convey a message that has been forwarded by an MM-UA. The forwarded encrypted body part will contain the original encrypted content type and envelope information.

Note, this functionality is also applicable to an MM-MS and an MM-AU.

NOTE: Forwarded encrypted body parts shall not be included in a content that is expected to be exchanged between nations except by bilateral agreement. Forwarded messages protected by S/MIME shall employ the forwarded content body part IAW Annex B.

7.3.12.4 MM-Message

The MM-Message body part will be used to convey a Military Message that has been forwarded by an MM-UA. The MM-Message body part will contain the original contents. In the case of an encrypted message, the message will be decrypted prior to forwarding the message.

Note, this functionality is also applicable to an MM-MS and an MM-AU.

7.3.12.5 ACP127Data

The ACP127Data body part will be used to convey ACP 127 data pattern traffic.

7.3.13 Body Parts defined by ITU-T X.420 | ISO/IEC 10021-7 1996 (E)

The Forwarded Content body parts as defined by clause 7.4.16 in the 1996 version of the civil MHS standard is supported. The Content Body Part Type will enable any content type (e.g. CMS-protected content) to be forwarded in Military Messages.

8 MILITARY NOTIFICATIONS

8.4 Other Notification Type Fields

Three types of notifications have been defined in order to provide information to the originator about a message which encounters an MMHS/ACP 127 gateway:

1. A positive ACP 127 notification indicates that a gateway has successfully translated a military message into ACP 127 and takes communications responsibility for its trace and recovery.

2. A negative ACP 127 notification indicates that a gateway has failed to translate a military message to ACP 127 and does not take communications responsibility for its trace and recovery.

3. A transfer ACP 127 notification indicates that a gateway has successfully translated a military message to ACP 127 but does not take communications responsibility for its trace and recovery.

Any or all of these notifications may be requested by the originator using an ACP 127 notification request. The detailed ASN.1 specification is provided in Annex A.

SECTION 3 – ABSTRACT SERVICE DEFINITION

12 ABSTRACT OPERATIONS

12.1 Origination Abstract Operations

12.1.1 Originate Probe

MM-UA's shall not be allowed to submit probes.

12.1.2 Originate MM

Both X.400 distribution lists (DLs) and Address Lists (ALs) will be supported by MMHS. DL expansion and management will be performed by the MTS as described in the civil standards. In absence of MLA in the MMHS domain, it is recommended that AL expansion, tailored by the exempted address list, be performed by the originating management domain.

12.3.3 Change Auto-forwarding

The change auto-forwarding abstract operation enables or disables auto-forwarding, the automatic forwarding of MMs by the MM-MS to pre-specified users or DLs. Such forwarding occurs upon delivery of the MMs.

```
ChangeAutoForwarding ::= ABSTRACT-OPERATION
      ARGUMENT SET {
            auto-forward-IPMs BOOLEAN,
            auto-forward-recipients SEQUENCE OF ORName OPTIONAL,
            auto-forward-heading    Heading OPTIONAL,
            auto-forward-comment    AutoForwardComment OPTIONAL }
      RESULT
      ERRORS {
            SubscriptionError,
            RecipientImproperlySpecified }
```

NOTE: The auto-forward-IPM structure is used to indicate auto-forward-MM.

The body of each MM the MM-MS originates as a result of auto-forwarding comprises a single body part of type mm-message or forwarded-encrypted. The content of the message represented by that body part is the forwarded MM.

NOTE: For implementations which support dual MM and IPM functionality, the single body part within the body can also be of type message. In this case, the content of the message represented by that body part is a forwarded IPM.

When it auto-forwards a message, the MM-UA originates an NRN on the user's behalf if, and only if, one was requested of him by means of the notification-requests component of the subject recipient specifier.

This abstract operation has the following arguments:

a) **auto-forward-IPMs** (M) : Whether or not MMs are to be auto-forwarded. A Boolean.

b) **auto-forward-recipients** (C) : The users or DLs to which MMs are to be auto-forwarded. A sequence of O/R names.
This conditional argument shall be present if, and only if,the auto-forward-IPMs argument has the value *true*.

c) **auto-forward-heading** (C) : The heading that is to be used for each forwarding IPM. Its auto-forwarded heading field shall have the value *true*.
This conditional argument shall be present if, and only if, the auto-forward-IPMs argument has the value *true*.

d) **auto-forward-comment** (C) : The value that is to be supplied as the auto-forward comment non-receipt field of each NRN conveyed to the originator of an auto-forwarded IPM.
This conditional argument shall be present if, and only if, the auto-forward-IPMs argument has the value true.

This abstract operation has no results.

NOTE: This abstract operation is intended to define the essence of auto-forwarding, sophisticated auto-forwarding capabilities, e.g., like those of an MS.

NOTE: For implementations which support dual MM and IPM functionality, the arguments above may apply to both MMs and IPMs.

SECTION 4 – ABSTRACT SERVICE PROVISION

16 SECONDARY OBJECT TYPES

16.6 Message Transfer System

The gateways to ACP 127 and Civilian MHS domains are both access units (AU).

18 USER AGENT OPERATION

The expansion of the AL will be performed *by either the originating or receiving MMHS management domains depending on AL expansion policy,* which will create an X.400 MMTS recipient for each member of the AL not excluded, but will not create separate OR descriptors for each member of the AL in the heading fields. The MLA will use the mLExpansionHistory attribute to prevent mail loops. In absence of MLA in the MMHS domain and to avoid duplicate messages it is recommended that AL expansion be performed **by the originating management domain.** In that case, it is recommended that AL expansion **occurs at the originating MM-UA.** ALs support the Exempted Addresses capability in an MMHS domain.

18.2 Performance of Origination Operations

18.2.1 Originate Probe

MM-UA's shall not be allowed to submit probes.

18.2.2 Originate MM

Both X.400 DL's and AL's will be supported by MMHS. DL expansion and management will be performed by the MTS as described in the civil standards. In absence of MLA in the MMHS domain, it is recommended that AL expansion, tailored by the exempted address list, be performed by the originating management domain.

The setting of the message submission fields for each recipient shall either:

(1) defaulted to a configurable set; or
(2) user selectable.

18.5.3.1 Prevention of Loops

The UA shall suppress auto-forwarding if, and only if, the MM to be forwarded itself contains a forwarding MM that the UA created. Autoforwarding shall be suppressed whether the forwarding MM appears (directly) in either a MM-

message or a Forwarded-encrypted body parts of the MM to be forwarded, or (nested) in the body parts of the MM that appears in such body parts.

NOTE - For implementations which support dual MM and IPM functionality, the above mentioned conditions also apply to forwarded MMs which include Message bodies containing IPMs.

The UA shall consider itself to have created the forwarding MM above (whose Auto-forwarded heading fields has the value *true*) if, and only if, the Originator-name component of the MM's Parameter component matches the O/R name of the UA.

NOTE - Auto-forwarding an MM of the kind above constitutes an Autoforwarding loop.

18.5.3.2 Construction of MM

The UA shall construct a forwarded MM whose Heading is the Auto-forwarded-heading state variable (it's Auto-forwarded field having the value *true*) and whose body comprises a single body part, which can be either of type:

a) *Forwarded-Encrypted*: This body part type will be used if, and only if, the received message (either an MM or an IPM) is encrypted and the UA is unable to decrypt the message prior to forwarding. The entire original encrypted message will be conveyed in the forwarded-encrypted body part.

b) *MM-Message:* This body part type will be used if, and only if, the received message is an MM and the condition described in a) above does not apply (i.e., the MM is not encrypted or has been decrypted) prior to forwarding the message.

The two body part types used for message forwarding shall have the following components:

a) *Parameters*: The envelope argument of message delivery.

b) *Data*: The message (either MM or IPM) to be forwarded."

NOTE: For implementations which support dual MM and IPM functionality, it is also possible to use the **message** body part type. It may be used to convey (a) messages received as IPMs and (b) messages received as MMs but downgraded to an IPM by any UA with capabilities to do it. Encrypted IPMs that cannot be decrypted by the UA prior to forwarding may be forwarded within a **Forwarded-Encrypted** body part type.

18.5.3.4 Construction of NRN

The following note shall be appended to clause 18.5.3.4 in X.420.:

NOTE: This is applicable for both forwarded MMs and forwarded IPMs.

19 MESSAGE STORE OPERATION

19.2 Maintenance of Attributes

"Processed" means that the MM-UA has completely fetched the message and made the message contents available to the user.

19.4 Auto-forwarding

The following note shall be appended to clause 19.4 in X.420.:

NOTE: the requirements are also applicable to an MS implementation which performs Autoforwarding of IPMs.

19.5 Manual Forwarding

An MM-MS shall support the manual forwarding of a message, using the forwarding-request extension of recommendation [ITU-T X.413 | ISO/IEC 10021-5]. The MM-MS user may submit an MM,including heading and body, using the message submission operation and identify by using the forwarding request extension, a message in the MS which needs to be forwarded.

The MS will construct a forwarded message using the following body part type:

a) *Forwarded-Encrypted*: This body part type will be used if, and only if, the received message to be forwarded (either an MM or an IPM) is encrypted and the UA is unable to decrypt the message prior to forwarding. The entire original encrypted message will be conveyed in the forwarded-encrypted body part.

b) *MM-Message:* This body part type will be used if, and only if, the received message to be forwarded is an MM and the condition described in a) above does not apply (i.e., the MM is not encrypted or has been decrypted) prior to forwarding the message.

The submitted message and the message to be forwarded are the combined by inserting the appropriate body part type into the submitted message."

NOTE: For implementations which support dual MM and IPM functionality, it is also possible to use the **message** body part type to forward a message. This may be used whenever (a) the message to be forwarded is an IPM or (b) the message is an MM, but the UA has the capability to downgrade it into an IPM. Encrypted IPMs that cannot be decrypted by the UA prior to forwarding may be forwarded within a **Forwarded-Encrypted** body part type.

20 MESSAGE CONTENTS

20.2 Content Type

Military messaging will use a content type denoted by the object identifier id-nato-mmhs-cont-mm88. The protocol used for military messaging is called P772.

22 CONFORMANCE

The requirements a secondary object (excluding the MST) and its implementor shall meet when the latter claims conformance to this MM Recommendation are indentified below. The requirements listed below supersede the requirements listed in Clauses 22.1 - 22.4 of Fascicle VIII.7 - Rec. X.420.

22.1 Origination versus Reception.

A MM-UA, or AU shall be said to support upon origination a particular heading field, heading extension, basic body part type, or extened body part type, if and only if, it accepts, preserves and emits, in full accord, with this STANAG, that particular heading field or extension, or body parts of that particular basic or extended type, whenever, a user calls upon it to convey an MM containing them to the MTS or the user’s MM-MS (the latter only in the case of a MM-UA).

A MM-UA, or AU shall be said to support upon reception a particular heading field, heading extension, basic body part type or extended body part type, if and only if, it accepts, preserves and emits, in full accord with this STANAG, that particular heading field or extension, or body parts of that particular basic or extended type, whenever, the MTS or a user’s MM-MS (the latter only in the case of a MM-UA) calls upon it to convey to the user an MM containing them.

22.2 Statement requirements

The implementor of an MM-UA, MM-MS, or AU shall state the following. For each item beleow, he shall make separate statements concerning conformance upon origination and conformance upon reception:

a) The heading fields and heading extensions for which he claims conformance.

b) The basic and extended body parts for which he claims conformance.

c) In the case of an MM-MS or MM-UA accessing an MM-MS, the Military-Messaging-specific MS attribute-types for which conformance is claimed.

d) In the case of an MM-MS or MM-UA accessing an MM-MS, any claim of conformance for the auto-forward, auto-action defined in [ITU-T X.413 | ISO/IEC 10021-5].

22.3 Static requirements

A MM-UA, MM-MS, or AU shall satisfy the following static requirements:

a) A MM-UA, MM-MS, or AU shall implement the heading fields and heading extensions, and the basic and extended body parts for which conformance is claimed.

b) A MM-MS or a MM-UA accessing a MM-MS shall support the Military Messaging-specific MS attribute-types for which conformance is claimed. Including as a minimum those attributes-types designated as mandatary in Annex C.

c) A MM-UA, MM-MS, or AU shall concretely realize its abstract ports as specified in Clause 21 of [ITU-T X.420 | ISO/IEC 10021-7].

d) A MM-UA or MM-MS shall be able to submit and accept delivery Military Messages of the content type specified by object identifier id-nato-mmhs-cont-mm88.

22.4 Dynamic requirements

A MM-UA, MM-MS, or AU shall satisfy the following dynamic requirements:

a) A MM-UA or MM-MS shall follow the rules of operation specified in Clause 18 of [ITU-T X.420 | ISO/IEC 10021-7] or Clause 19 of [ITU-T X.420 | ISO/IEC 10021-7] respectively.

b) A MM-UA, MM-MS, or AU shall submit and accept delivery of Military Messages of the content type specified by the object identifier id-nato-mmhs-cont-mm88.

c) A MM-UA, MM-MS, or AU shall register with the MTS its ability to accept delivery of Military Messages of the content specified by the object identifier id-nato-mmhs-cont-mm88, as well as, any message of the other two content types specified in Clause 20.2 of [ITU-T X.420 | ISO/IEC 10021-7].

d) The Primary Precedence shall be mapped onto the grade of delivery abstract service (and extended grade of delivery if that option is selected by the profile in question).

ANNEXES TO [ITU-T X.420 | ISO/IEC 10021-7]

The following annexes are additional to annex A to X.420.

All extentions defined in Annex A of X.420 are also applicable for MM messaging.

ANNEX A1 – Military Heading Extensions

This annex contains definitions of military heading extensions which are defined using the IPMS-EXTENSION macro.

Note, all lower bounds and upper bounds used in this section are defined in Annex K of this part of the MBS.

A1.1 Exempted address

The **exempted address** heading extension, by its presence indicates the names of members in an Address List that should not receive the message.

```
exempted-address IPMS-EXTENSION
      VALUE SEQUENCE OF ExemptedAddress
      ::= id-nato-mmhs-mm-exempted-address

ExemptedAddress ::= ORDescriptor
      -- O/R Descriptor, as defined in 7.1.3 of ITU-T X.420
```

If this extension is absent from the Extensions heading field, all members of an AL will be considered to be valid recipients of the message.

A1.2 Extended authorisation information

The **extended authorisation info** heading extension, by its presence indicates either the date and the time when the message was officially released by the releasing officer or the date and time when the message was handled by a communication facility for transmission.

```
extended-authorisation-info IPMS-EXTENSION
      VALUE ExtendedAuthorisationInfo
      ::= id-nato-mmhs-mm-extended-authorisation-info

ExtendedAuthorisationInfo  ::= UTCTime
      -- UTCTime as defined in 8.5.4 of ITU-T X.411
```

The originating message domain shall ensure that the extended-authorization-info extension is always present in the message.

A1.3 Distribution codes

The **distribution codes** heading extension, by its presence indicates distribution information to a recipient or a recipient's MM-UA. This information can be used to perform automatic or manual local distribution of a message.

```
distribution-codes IPMS-EXTENSION
      VALUE DistributionCodes
      ::= id-nato-mmhs-mm-distribution-codes

DistributionCodes ::= SET {
      sics                [0]  SEQUENCE SIZE (1..ub-military-
number-of-sics) OF
                                     Sic OPTIONAL,
      dist-Extensions     [1]  SEQUENCE OF
DistributionExtensionField OPTIONAL}

Sic ::= PrintableString (SIZE (lb-military-sic..ub-military-sic))

DistributionExtensionField ::= SEQUENCE {
      dist-type           OBJECT IDENTIFIER,
      dist-value          ANY DEFINED BY dist-type}
```

If this extension is absent, then the local distribution will be in accordance with the message handling policy of the recipient's domain.

A1.4 Handling instructions

This is a transitional heading extension, used when interoperating with ACP 127 domains.

The **handling instructions** heading extension, by its presence indicates local handling instructions that may require some manual handling by a traffic operator.

```
handling-instructions IPMS-EXTENSION
      VALUE HandlingInstructions
      ::= id-nato-mmhs-mm-handling-instructions

HandlingInstructions ::= SEQUENCE OF MilitaryString

MilitaryString ::= PrintableString (SIZE(1..ub-military-string))
```

If this extension is absent the message will be considered as not requiring manual handling by a traffic operator.

A1.5 Message instructions

The **message instructions** heading extension, by its presence indicates message instructions accompaning the message (e.g., similar to the operating signals specified in ACP 131).

```
message-instructions IPMS-EXTENSION
      VALUE MessageInstructions
      ::= id-nato-mmhs-mm-message-instructions

MessageInstructions ::= SEQUENCE OF MilitaryString
      -- MilitaryString as defined in A1.4
```

If this extension is absent the message will be considered received without message instructions.

A1.6 Codress message

This is a transitional heading extension, used when interoperating with ACP 127 domains.

The **codress message** heading extension, by its presence indicates that the message is in codress format.

```
codress-message IPMS-EXTENSION
      VALUE CodressMessage
      ::= id-nato-mmhs-mm-codress-message

CodressMessage ::= INTEGER
```

If this extension is absent the message will be considered received without the codress format.

A1.7 Originator reference

The **originator reference** heading extension, by its presence indicates a user defined reference called the ‘originator’s number’.

```
originator-reference IPMS-EXTENSION
      VALUE OriginatorReference
      ::= id-nato-mmhs-mm-originator-reference

OriginatorReference ::= MilitaryString
      -- MilitaryString as defined in A1.4
```

If this extension is absent, then the message will be considered received without any user defined reference.

A1.8 Primary precedence

The **primary precedence** heading extension, by its presence indicates the precedence level of the primary recipients.

```
primary-precedence IPMS-EXTENSION
      VALUE MMHSPrecedence
      ::= id-nato-mmhs-mm-primary-precedence

MMHSPrecedence ::= INTEGER {deferred (0), routine (1), priority
(2),
      immediate (3), flash (4), override (5)}

-- Note: Values 0 to 15 are reserved for NATO defined precedence
levels.
-- Values 16 to 31 are reserved for national user.
```

The message originating domain shall ensure that this extension is always present for action addressees.

A1.9 Copy precedence

The **copy precedence** heading extension, by its presence indicates the precedence level of the copy recipients.

```
copy-precedence IPMS-EXTENSION
      VALUE MMHSPrecedence -- MMHSPrecedence as defined in A1.8
      ::= id-nato-mmhs-mm-copy-precedence

-- Note: Values 0 to 15 are reserved for NATO defined precedence
levels.
-- Values 16 to 31 are reserved for national user.
```

The message originating domain shall ensure that this extension is present for all information addressees.

A1.10 Message type

The **message type** heading extension, by its presence indicates whether the message is to be considered as an exercise, an operation, a projet or a drill.

```
message-type IPMS-EXTENSION
      VALUE MessageType
      ::=id-nato-mmhs-mm-message-type

MessageType ::= SET{
      type               [0]  TypeMessage,
      identifier         [1]  MessageIdentifier OPTIONAL}

TypeMessage ::= INTEGER {exercise(0), operation(1), project(2),
drill(3)}

-- Note: Values 0 to 127 are reserved for NATO defined Message
```

```
Type
-- identifiers. Values above 128 to 255 are not defined by NATO
and may
-- be used nationally or bilaterally.

MessageIdentifier ::= MilitaryString      -- MilitaryString as
defined by A1.4
```

If this extension is absent the message will be considered to be an undefined typed.

A1.11 Address list indicator

The **address list indicator** heading extension, by its presence indicates the names of predefined list of recipients. In addition, it specifies the precedence level of each list and whether a notification or a reply has been requested.

```
address-list-indicator IPMS-EXTENSION
      VALUE SEQUENCE OF AddressListDesignator
      ::=id-nato-mmhs-mm-address-list-indicator

AddressListDesignator ::=SET {
      type                [0]  INTEGER {primaryAddressList (0),
                                        copyAddressList (1) },
      listName            [1]  ORDescriptor,
            -- O/R Descriptor as defined in 7.1.3 of ITU-T X.420
      notificationRequest [2]  AddressListRequest OPTIONAL,
      replyRequest        [3]  AddressListRequest OPTIONAL }

AddressListRequest ::= INTEGER {action(0), info(1), both(2)}
```

The addressListIndicator form of address list (AL) is deprecated. However national systems are expected to continue existing use of the address list indicator (ALI) in the short term.

A1.12 Other recipients indicator

The **other recipients indicator** heading extension, by its presence indicates the names of recipients, as well as the category (primary or copy) in which they are placed, that are intended to receive or have received the message via means other than MMHS.

```
other-recipients-indicator IPMS-EXTENSION
      VALUE SEQUENCE OF OtherRecipientDesignator
      ::=id-nato-mmhs-mm-other-recipients-indicator

OtherRecipientDesignator ::= SET {
      type                [0]  INTEGER {primary(0), copy(1)},
      designator          [1]  MilitaryString }
            -- MilitaryString as defined in A1.4
```

The absence of this element does not guarantee that all recipients are within the MMHS.

A1.13 Pilot forwarding information

This is a transitional heading extension, used when interoperating with ACP 127 domains.

The **pilot forwarding info** heading extension, by its presence indicates ACP 127 related useful information, which equals or supersedes the received header information for precedence, classification, local handling instruction and addressing.

```
pilot-forwarding-info IPMS-EXTENSION
      VALUE SEQUENCE OF PilotInformation
      ::= id-nato-mmhs-mm-pilot-forwarding-info

PilotInformation ::= SEQUENCE {
      pilotPrecedence     [0]  MMHSPrecedence OPTIONAL,
            -- MMHSPrecedence as defined in A1.8
            -- Note: Values 0 to 15 are reserved for NATO defined
precedence levels.
            -- Values 16 to 31 are reserved for national use.
      pilotRecipient      [1]  SEQUENCE OF ORDescriptor OPTIONAL,
            -- O/R Descriptor as defined in 7.1.3 of ITU-T X.420
      pilotSecurity       [2]  MessageSecurityLabel OPTIONAL,
            -- MessageSecurityLabel as defined in 8.5.9 of ITU-T
X.411
      pilotHandling       [3]  SEQUENCE OF MilitaryString OPTIONAL
}
            -- MilitaryString as defined by A1.4
```

If this extension is absent, the message will be considered as one that does not contain any pilot information.

A1.14 ACP 127 message identifier

This is a transitional heading extension, used when interoperating with ACP 127 domains.

The **ACP 127 message identifier** heading extension, by its presence indicates an ACP 127 message identifier which originated from an ACP 127 domain.

```
acp127-message-identifier IPMS-EXTENSION
      VALUE Acp127MessageIdentifier
      ::= id-nato-mmhs-mm-acp127-message-identifier

Acp127MessageIdentifier ::= MilitaryString            -- as
defined in A1.4
```

If this extension is absent, then the message did not encounter an ACP 127 domain.

A1.15 Originator PLAD

This is a transitional heading extension, used when interoperating with ACP 127 domains.

The **originator plad** heading extension, by its presence indicates the plain language address associated with an originator for cross reference purposes.

```
-- string to store routing indicator, station serial number and
julian file
-- time, separated by spaces

originator-plad IPMS-EXTENSION
      VALUE OriginatorPlad
      ::= id-nato-mmhs-mm-originator-plad

OriginatorPlad ::= MilitaryString         -- MilitaryString as
defined in A1.4
```

If this extension is absent, then the message will be considered to not having an originators PLAD cross reference between the MMHS and ACP 127 domains.

A1.16 Security Information Labels

The **security information labels** heading extension, by its presence indicates that a security label has been assigned to the complete message content and optionally, one or more of the following;

- The message header
- One or more of the message body parts.

When security labels are assigned to one or more body part the originator shall indicate which body part the information label relates to, based on the order in which the body parts are encoded by the originating UA. The information security labels for the body parts shall be in the same order as the body parts which are encoded by the originating UA. If all body parts have a security label assigned, then the order in which they appear in the heading extension shall relate to the order in which they were encoded by the originating UA and the numeric indication of the order of the body part may be absent.

```
security-information-labels IPMS-EXTENSION
      VALUE SecurityInformationLabels
      ::= id-nato-mmhs-mm-information-labels

SecurityInformationLabels ::= SEQUENCE{
      content-security-label  [0]   SecurityLabel,
                               -- SecurityLabel as defined
                               -- in 8.5.9 of ITU-T X.411
      heading-security-label  [1]   SecurityLabel OPTIONAL,
      body-part-security-labels [2]  SEQUENCE OF
                               BodyPartSecurityLabel OPTIONAL }

BodyPartSecurityLabel ::= SET {
      body-part-security-label  [0]  SecurityLabel,
      body-part-sequence-number [1]  BodyPartSequenceNumber
OPTIONAL }

BodyPartSequenceNumber ::= INTEGER

--  Note: If all body parts of the message are labelled, each
--  element in the body sequence above shall correspond to the
--  same numbered element of the Body sequence, and the body
--  part sequence number may be absent. (i.e. the first element
--  of this field shall correspond to the first body part, etc.).
--  Otherwise the body part sequence number shall be present
--  and shall correspond to the sequence of the body part
--  to which the security label relates. (i.e. the value of the
--  body part sequence number shall correspond to sequence in
which
--  the originator encoded the body parts of the message).
```

If this extension is absent, then the message will be considered received without any information security labels.

NOTE: If this heading extension is used, then a textual indication is not needed to convey the classification level and security categories that apply to the information conveyed in that body part. This will facilitate automated processing of the label in recipient systems. If the content label is an aggregate of all the individual information label in the message it may simplify checking integrity of the access control label at national guard processors. This will be required to be specified as part of the system security policy.

NOTE: The security-information-labels heading extension is now deprecated. Its use is, therefore, discouraged. See STANAG 4406 Annex B for instruction on the use of its replacement, the ESSSecurityLabel.

ANNEX A2 – Military per Recipient Specifier Extensions

This annex contains definitions of military per recipient specifier extensions which are defined using the IPMS-EXTENSION macro.

A2.1 ACP 127 notification request

The **ACP 127 notification request** per recipient specifier extension, by its presence indicates the type of notification requested from an ACP 127 gateway.

```
-- The following definitions are made in order to support
-- informing the originator of a message that the subject message
-- has reached a gateway to an ACP 127 domain.

acp127-notification-request IPMS-EXTENSION
      VALUE Acp127NotificationType
      ::= id-nato-mmhs-mm-acp127-notification-request

Acp127NotificationType ::= BIT STRING {
      acp127-nn (0),      -- negative notification
      acp127-pn (1),      -- positive notification
      acp127-tn (2) }     -- transfer notification
```

An MM-UA on receiving the request may ignore the extension.

ANNEX A3 – Military OTHERNOTIFICATIONTYPEFIELD Extensions

This annex contains definitions of military notification extensions which are defined using the IPMS-EXTENSION macro.

A3.1 ACP 127 notification response

The extension is only generated by ACP 127 gateways.

The **ACP 127 notification response** notification extension, by its presence indicates the result of an attempt to transfer a message into an ACP 127 domain.

```
acp127-notification-response IPMS-EXTENSION
      VALUE Acp127NotificationResponse
      ::= id-nato-mmhs-mm-acp127-notification-response

Acp127NotificationResponse ::= SET {
      acp127-notification-type      [0]   Acp127NotificationType,
      receipt-time        [1]  ReceiptTimeField,
            -- ReceiptTimeField as defined in 8.3.1 of ITU-T X.420
      addressListInicator [2]  AddressListIndicator OPTIONAL,
      acp127-recipient    [3]  Acp127Recipient OPTIONAL,
      acp127-supp-info    [4]  Acp127SuppInfo OPTIONAL}

AddressListIndicator ::= SEQUENCE OF AddressListDesignator
            -- AddressListDesignator as defined in A1.11

Acp127Recipient ::= PrintableString (SIZE (1..ub-military-
bigstring))

Acp127SuppInfo ::= PrintableString  (SIZE (1..ub-military-
bigstring))
```

ANNEX B – Extended Body Part Types

The following extended body parts are defined in addition to those extended body parts defined in Annex B of X.420

B1 Military extended body part types

B1.1 ADatP3

An **Adatp3** body part represents an information object, which is used to convey military ADatP3 messages. It has Parameters and Data components.

```
adatp3-body-part EXTENDED-BODY-PART-TYPE
      PARAMETERS ADatP3Parameters    IDENTIFIED BY
            id-nato-mmhs-et-adatp3-parameters
      DATA               ADatP3Data
      ::= id-nato-mmhs-et-adatp3

ADatP3Parameters ::= INTEGER DEFAULT (0)

ADatP3Data ::= CHOICE{
      lineOriented       [0]  IMPLICIT IA5String,
      setOriented        [1]  IMPLICIT SEQUENCE OF IA5String}
```

B1.2 Corrections

A **correction** body part represents an information object, which is used to convey corrections to information in another body part. The corrections body part is only used when interoperating with ACP 127 domains. It has Parameters and Data components.

```
corrections-body-part EXTENDED-BODY-PART-TYPE
      PARAMETERS CorrectionsParameters    IDENTIFIED BY
            id-nato-mmhs-et-corrections-parameters
      DATA               CorrectionsData
      ::= id-nato-mmhs-et-corrections


CorrectionsParameters ::= INTEGER

CorrectionsData ::= IA5String
```

B1.3 Forwarded encrypted

(NU)A **forwarded encrypted** body part represents an information object, which is used to convey information about an encrypted message which has been forwarded prior to any decryption having taken place. It has Parameters and Data components.

```
forwarded-encrypted-body-part EXTENDED-BODY-PART-TYPE
      PARAMETERS ForwardedEncryptedParameters   IDENTIFIED BY
            id-nato-mmhs-et-forwarded-encrypted-parameters
      DATA               ForwardedEncryptedData
      ::= id-nato-mmhs-et-forwarded-encrypted

-- A forwarded-encrypted-body must contain the delivery
information,
-- containing the content type which will indicate whether the
forwarded
-- encrypted message is an MM or IPM. All security related
information
-- (i.e., token) of the original message must be forwarded.

ForwardedEncryptedParameters ::= SET {
      delivery-time       [0]  MessageDeliveryTime OPTIONAL,
            -- MessageDeliveryTime as defined in Figure 2/X.411,
Part 11 of 26.
      delivery-envelope   [1]  OtherMessageDeliveryFields }
            -- OtherMessageDeliveryFields as defined in Figure
2/X.411, part 9 of 26.

ForwardedEncryptedData ::= BIT STRING
```

B1.4 MM message

A **MM message** body part represents an information object that is used to convey a forwarded message which is not encrypted. It has Parameters and Data components.

```
mm-message-body-part EXTENDED-BODY-PART-TYPE
      PARAMETERS MMMessageParameters      IDENTIFIED BY
                        id-nato-mmhs-et-mm-message-parameters
      DATA                    MMMessageData
      ::= id-nato-mmhs-et-mm-message

-- An mm-message-body-part can either carry a forwarded MM or a
forwared
-- IPM. In the case of a message-body-part, as defined in X.420,
it can
-- only carry an IPM.

MMMessageParameters ::= SET {
      delivery-time       [0]  MessageDeliveryTime OPTIONAL,
            -- MessageDeliveryTime as defined in Figure 2/X.411,
Part 11 of 26.
```

```
      delivery-envelope   [1]  OtherMessageDeliveryFields }
            -- OtherMessageDeliveryFields as defined in Figure
2/X.411, Part 9 of 26.

MMMessageData ::= MM
```

B1.5 ACP127DATA

An **ACP127DATA** body part represents an information object, which is used to convey data pattern traffic. The ACP127DATA body part is only used when interoperating with ACP 127 domains. It has Parameters and Data components.

```
acp127data-body-part EXTENDED-BODY-PART-TYPE
      PARAMETERS ACP127DataParameters     IDENTIFIED BY
                           id-nato-mmhs-et-acp127data-parameters
      DATA                      ACP127DataData
      ::= id-nato-mmhs-et-acp127data

ACP127DataParameters ::= INTEGER

ACP127DataData ::= IA5String (SIZE(1..ub-data-size))
```

ANNEX C – Message Store Attributes

The following definitions of MS attributes are in addition to those specified in Annex C of X.420.

It should be noted that names of attributes that contain the term "IPM", defined in Annex C of X.420, should be read as the term "MM". For example, "ipm-entry-type should be read as "mm-entry-type". Note, the object identifiers for ipm and mm attributes will remain identical, as defined by the civil X.420 standards.

Table C-3 – [ITU-T X.420 | ISO/IEC 10021-7] Summary of MS Attributes

Attribute	V L	MM	LA	S
A				
ACP 127 Message Identifier	S O	C	N	N
ACP 127 Notification Request	S O	C	Y	Y
ACP 127 Notification Response	S O	C	Y	Y
Address List Designator	M O	C	Y	Y
B				
Body Part Security Label	M O	C	Y	Y
C				
Codress Message	S O	C	Y	Y
Copy Precedence	S O	C	Y	N
D				
Distribution Codes	S O	C	Y	N
Distribution Extensions	M O	C	Y*	Y*
E				
Exempted Address	M O	C	Y	N
Extended Authorization Info	S O	C	N	N
H				
Handling Instructions	S O	C	Y	Y
M				
Message Type	S O	C	Y	N
Message Instructions	S O	C	Y	N
O				
Other Recipients Designator	M O	C	Y	Y
Originator Reference	S O	C	Y	Y

Attribute	V L	MM	LA	S
Originator PLAD	S O	C	N	N
P				
Primary Precedence	S O	C	Y	Y
Pilot Information	M O	C	Y	Y
S				
Security Information Labels	S O	C	Y	Y
SIC Codes	M O	C	Y	Y

* = The dist-value field shall be disregarded for the purpose of matching, unless the syntax of the field is recognized based on the values of the dist-type field.

C.2.5 Military Heading Extensions

The following attributes are in addition to those attributes specified in C.2.5 of X.420.

Attributes bearing the names of heading fields with those fields as their values.

```
-- Military Heading Fields

exempted-address ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX ExemptedAddress
      MATCHES FOR EQUALITY
      MULTI VALUE
      ::= id-nato-mmhs-hat-exempted-address

extended-authorisation-info ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX ExtendedAuthorisationInfo
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-extended-authorisation-info

distribution-codes ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX DistributionCodes
      MATCHES FOR EQUALITY
      MULTI VALUE
      ::= id-nato-mmhs-hat-distribution-codes

handling-instructions ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX HandlingInstructions
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-handling-instructions

sic-codes ATTRIBUTE
```

```
      WITH ATTRIBUTE-SYNTAX Sic
      MATCHES FOR EQUALITY
      MULTI VALUE
      ::= id-nato-mmhs-hat-sic-codes

distribution-extensions ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX DistributionExtensionField
      MATCHES FOR EQUALITY
            -- The dist-value field shall be disregarded for the
purpose of matching,
            -- unless the syntax of the field is recognized based
on the value of the
            -- dist-type field.
      MULTI VALUE
      ::= id-nato-mmhs-hat-distribution-extensions

message-instructions ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX MessageInstructions
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-message-instructions

codress-message ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX CodressMessage
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-codress-message

originator-reference ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX OriginatorReference
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-originator-reference

primary-precedence ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX MMHSPrecedence
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-primary-precedence

copy-precedence ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX MMHSPrecedence
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-copy-precedence

message-type ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX MessageType
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-message-type

address-list-indicator ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX AddressListDesignator
      MATCHES FOR EQUALITY
```

```
      MULTI VALUE
      ::= id-nato-mmhs-hat-address-list-indicator

other-recipients-indicator ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX OtherRecipientDesignator
      MATCHES FOR EQUALITY
      MULTI VALUE
      ::= id-nato-mmhs-hat-other-recipients-indicator

pilot-forwarding-info ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX PilotInformation
      MATCHES FOR EQUALITY
      MULTI VALUE
      ::= id-nato-mmhs-hat-pilot-forwarding-info

acp127-message-identifier ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX Acp127MessageIdentifier
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-acp127-message-identifier

originator-plad ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX OriginatorPlad --modified
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-originator-plad

acp127-notification-request ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX Acp127NotificationType
            -- an extension of Recipient Specifier
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-acp127-notification-request

body-part-security-label ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX BodyPartSecurityLabel
      MATCHES FOR EQUALITY
      MULTI VALUE
      ::= id-nato-mmhs-hat-body-part-security-label

security-information-labels ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX SecurityInformationLabels
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-security-information-labels
```

NOTE: The body-part-security-label and security-information-labels attributes are now deprecated. Their use is, therefore, discouraged. See STANAG 4406 Annex B for instruction on the use of the ESSSecurityLabel.

C3.1 ACP 127 Notification Fields

The following attribute is an additional attribute for ACP notifications.

```
acp127-notification-response ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX Acp127NotificationResponse
      MATCHES FOR EQUALITY
      MULTI VALUE         -- The reponse is multi-value
      ::= id-nato-mmhs-nat-acp127-notification-response
```

ANNEX D – Reference Definition of Object Identifiers

The Military Object Identifiers defined below are a super-set of the civil IPMS Object Identifiers defined in Annex D to X.420/IS 10021-7, all of which are imported into the military messaging system.

```
MMSObjectIdentifiers {iso(1) identified-organization(3) nato(26)
stanags(0) mmhs(4406)
      object-identifiers (0) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Prologue
-- Export everything

IMPORTS --nothing-- ;

ID ::= OBJECT IDENTIFIER

-- Military Messaging

id-mmhs ID ::= {iso(1) identified-organization(3) nato(26)
stanags(0)
      mmhs(4406) object-identifiers(0) }

-- Categories of object identifiers

id-mod            ID ::= {id-mmhs 0}      -- mm module
id-mm             ID ::= {id-mmhs 2}      -- heading extension
id-hat            ID ::= {id-mmhs 3}      -- heading attributes
for MS
id-mcont          ID ::= {id-mmhs 4}      -- content types
id-policy         ID ::= {id-mmhs 5}      -- NATO policy
identifier
id-cat            ID ::= {id-mmhs 6}      -- special category
identifiers
id-et             ID ::= {id-mmhs 7}      -- military defined
extended body part types
id-mmts           ID ::= {id-mmhs 8}      -- mts object
identifiers
id-nat            ID ::= {id-mmhs 9}      -- military defined
notification attributes
id-mot            ID ::= {id-mmhs 10}     -- military object types
id-mpt            ID ::= {id-mmhs 11}     -- military port types
id-ref            ID ::= {id-mmhs 12}     -- refinements
id-informationlabel       ID ::= {id-mmhs 13}

-- Modules

-- MMS information objects
id-mod-upper-bounds       ID ::= {id-mod 0}
id-mod-mms                ID ::= {id-mod 1}
```

```
id-mod-functional-objects ID ::= {id-mod 2}
id-mod-abstract-service   ID ::= {id-mod 3}
id-mod-heading-extension  ID ::= {id-mod 6}
id-mod-extended-body-part-types     ID ::= {id-mod 7}
id-mod-message-store-attributes     ID ::= {id-mod 8}
id-mod-per-recipient-specifier-extensions ID ::= {id-mod 11}
id-mod-other-notification-type-extensions ID ::= {id-mod 12}

-- Object types

id-mot-mmme               ID ::= {id-mot 0}
id-mot-mms-user           ID ::= {id-mot 1}
id-mot-mms                ID ::= {id-mot 2}
id-mot-mms-ua             ID ::= {id-mot 3}
id-mot-mms-ms             ID ::= {id-mot 4}
id-mot-acp127au           ID ::= {id-mot 5}
id-mot-pdau               ID ::= {id-mot 6}

-- port types

id-mpt-origination        ID ::= {id-mpt 0}
id-mpt-reception          ID ::= {id-mpt 1}
id-mpt-management         ID ::= {id-mpt 2}

-- Refinements

id-ref-primary            ID ::= {id-ref 0}
id-ref-secondary          ID ::= {id-ref 1}

-- Military Defined body parts

id-nato-mmhs-et-adatp3    ID ::= {id-et 0}
id-nato-mmhs-et-corrections   ID ::= {id-et 1}
id-nato-mmhs-et-adatp3-parameters         ID ::= {id-et 2}
id-nato-mmhs-et-corrections-parameters    ID ::= {id-et 3}
id-nato-mmhs-et-forwarded-encrypted       ID ::= {id-et 6}
id-nato-mmhs-et-forwarded-encrypted-parameters  ID ::= {id-et 7}
id-nato-mmhs-et-mm-message    ID ::= {id-et 9}
id-nato-mmhs-et-mm-message-parameters     ID ::= {id-et 10}
id-nato-mmhs-et-mm-acp127data ID ::= {id-et 12}
id-nato-mmhs-et-mm-acp127data-parameters  ID ::= {id-et 13}

-- Military Defined Heading Fields

id-nato-mmhs-mm-primary-precedence        ID ::= {id-mm 0}
id-nato-mmhs-mm-copy-precedence           ID ::= {id-mm 1}
id-nato-mmhs-mm-message-type  ID ::= {id-mm 2}
id-nato-mmhs-mm-address-list-indicator    ID ::= {id-mm 3}
id-nato-mmhs-mm-exempted-address          ID ::= {id-mm 4}
id-nato-mmhs-mm-extended-authorisation-info     ID ::= {id-mm 5}
id-nato-mmhs-mm-distribution-codes        ID ::= {id-mm 6}
id-nato-mmhs-mm-handling-instructions     ID ::= {id-mm 7}
id-nato-mmhs-mm-message-instructions      ID ::= {id-mm 8}
id-nato-mmhs-mm-codress-message           ID ::= {id-mm 9}
id-nato-mmhs-mm-originator-reference      ID ::= {id-mm 10}
```

```
id-nato-mmhs-mm-other-recipients-indicator      ID ::= {id-mm 11}
id-nato-mmhs-mm-pilot-forwarding-info     ID ::= {id-mm 12}
id-nato-mmhs-mm-acp127-message-identifier ID ::= {id-mm 13}
id-nato-mmhs-mm-originator-plad           ID ::= {id-mm 14}
id-nato-mmhs-mm-information-labels        ID ::= {id-mm 17}
                              -- This value is deprecated.

-- the following are per-recipient
id-nato-mmhs-mm-acp127-notification-request     ID ::= {id-mm 15}

-- the following are per other-notification-type
id-nato-mmhs-mm-acp127-notification-response    ID ::= {id-mm 16}

-- Military Defined Heading Attributes for MS

id-nato-mmhs-hat-primary-precedence       ID ::= {id-hat 0}
id-nato-mmhs-hat-copy-precedence          ID ::= {id-hat 1}
id-nato-mmhs-hat-message-type ID ::= {id-hat 2}
id-nato-mmhs-hat-address-list-indicator   ID ::= {id-hat 3}
id-nato-mmhs-hat-exempted-address         ID ::= {id-hat 4}
id-nato-mmhs-hat-extended-authorisation-info    ID ::= {id-hat 5}
id-nato-mmhs-hat-distribution-codes       ID ::= {id-hat 6}
id-nato-mmhs-hat-handling-instructions    ID ::= {id-hat 7}
id-nato-mmhs-hat-message-instructions     ID ::= {id-hat 8}
id-nato-mmhs-hat-codress-message          ID ::= {id-hat 9}
id-nato-mmhs-hat-originator-reference     ID ::= {id-hat 10}
id-nato-mmhs-hat-other-recipients-indicator     ID ::= {id-hat 11}
id-nato-mmhs-hat-pilot-forwarding-info    ID ::= {id-hat 12}
id-nato-mmhs-hat-acp127-message-identifier      ID ::= {id-hat 13}
id-nato-mmhs-hat-originator-plad          ID ::= {id-hat 14}

   - the following are per-recipient
id-nato-mmhs-hat-acp127-notification-request    ID ::= {id-hat 15}
id-nato-mmhs-hat-sic-codes    ID ::= {id-hat 16}
id-nato-mmhs-hat-distribution-extensions  ID ::= {id-hat 17}
id-nato-mmhs-hat-body-part-information-label    ID ::= {id-hat 18}
                              -- This value is deprecated.

id-nato-mmhs-hat-security-information-labels    ID ::= {id-hat 19}
                              -- This value is deprecated.


-- Military Defined special category identifiers

id-nato-mmhs-cat         ID ::= {id-cat 0}
                              -- This value is deprecated.
id-nato-mmhs-cat-atomal   ID ::= {id-cat 1}
                              -- This value is deprecated.
id-nato-mmhs-cat-cryptosecurity           ID ::= {id-cat 2}
                              -- This value is deprecated.
id-nato-mmhs-cat-specialhandlingintel     ID ::= {id-cat 3}
                              -- This value is deprecated.
id-nato-mmhs-cat-ussiopesi    ID ::= {id-cat 4}
                              -- This value is deprecated.
id-nato-mmhs-cat-eyesonly ID ::= {id-cat 5}
```

```
                                -- This value is deprecated.
id-nato-mmhs-cat-exclusive    ID ::= {id-cat 6}
                                -- This value is deprecated.
id-nato-mmhs-cat-information-label        ID ::= {id-cat 7}
                                -- This value is deprecated.
id-nato-mmhs-informationlabel-atomal      ID ::= {id-
informationlabel 1}
                                -- This value is deprecated.
id-nato-mmhs-informationlabel-cryptosecurity    ID ::= {id-
informationlabel 2}
                                -- This value is deprecated.
id-nato-mmhs-informationlabel-specialhandlingintel    ID ::= {id-
informationlabel 3}
                                -- This value is deprecated.
id-nato-mmhs-informationlabel-ussiopesi   ID ::= {id-
informationlabel 4}
                                -- This value is deprecated.
id-nato-mmhs-informationlabel-eyesonly    ID ::= {id-
informationlabel 5}
                                -- This value is deprecated.
id-nato-mmhs-informationlabel-exclusive   ID ::= {id-
informationlabel 6}
                                -- This value is deprecated.

-- Military Defined Notification Extension

id-nato-mmhs-nat-acp127-notification-response   ID ::= {id-nat 0}

-- Military Message content types (for use by MS only)

id-mct-p772       ID ::= {id-mcont 1}

END -- of MMHSObjectIdentifiers
```

ANNEX E – Reference Definition of Abstract Information Objects

This annex, a supplement to section 2 of the MBS, defines the abstract information objectfor military messaging.

```
MMSInformationObjects { iso(1) identified-organization(3) NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) module(0) mms(1)
}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prologue
-- Exports Everything
IMPORTS

-- IPM Information Object

Body, CommonFields, Heading, NonReceiptFields,
OtherNotificationTypeFields, ReceiptFields
---
FROM IPMSInformationObjects { joint-iso-ccitt
      mhs-motis(6) ipms(1) modules(0) information-objects(2) }

-- MTS abstract service

ORName
---
FROM MTSAbstractService { joint-iso-ccitt
      mhs-motis(6) mts(3) modules(0) mts-abstract-service(1) };

-- Information Object

InformationObject ::= CHOICE {
      mm      [0]  MM,
      mn      [1]  MN}

-- MM (Military Message)

MM ::= SEQUENCE {
      mmheading         Heading,
      mmbody            Body}

-- The mandatory support on the IPMIdentifier components is more
important
-- in MMS than in IPMS. The user component, ORName of the
originating UA is
-- mandatory. Local IPMIdentifier is made up of 2 concatenated
string
-- separated by a space both generated by the originating UA, a
serial
-- number and the filing time (the time the message generation is
finished)
-- in UTC time format. The minimum length of 15 is because both a
```

```
date/time
-- stamp in UTC format including seconds and a serial number, plus
the space
-- delimiter are mandatory. The smallest acceptable UTC date/time
stamp
-- is 13 (ddmmyyhhmmssZ).

-- MN (Military Notification receipt/non receipt / other
notification types)

MN ::= SET {
      COMPONENTS OF CommonFields,
      choice [0] CHOICE {
      mn-non-receipt-fields   [0]   NonReceiptFields,
      mn-receipt-fields  [1]  ReceiptFields,
      mn-other-notification-type-fields   [2]
      OtherNotificationTypeFields } }

MRN ::= MN                -- with MN-receipt-fields chosen

MNRN ::= MN               -- with MN-non-receipt-fields chosen

MON ::= MN                -- with MN-other-notification-type-
fields chosen

-- All military specific body parts are defined as extended body
parts.
-- The military specific body parts are defined in Annex A
-- of this part of the MBS.

END -- of MMS InformationObjects
```

ANNEX F – Reference Definition of Functional Objects

This annex, a supplement to §§ 10, 11 and 16 of the MBS, defines for reference purposes the functional objects of military messaging. It uses the OBJECT and REFINE macros of Recommendation X.407.

```
MMSFunctionalObjects { iso(1) identified-organization(3) NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) module(0)
functional-objects(2) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prologue
-- Exports Everything
IMPORTS

-- MMS abstract service
management, origination, reception
---
FROM MMSAbstractService { iso(1) identified-organization(3)
NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) module(0)
      abstract-service(3) }

-- MMS object identifiers
id-mot-acp127au,id-mot-mmme,  id-mot-mms, id-mot-mms-ms,
id-mot-mms-ua, id-mot-mms-user, id-mot-pdau, id-ref-primary,
id-ref-secondary
---
FROM MMSObjectIdentifiers { iso(1) identified-organization(3)
NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) }

-- MS abstract service
retrieval
---
FROM MSAbstractService { joint-iso-ccitt
      mhs-motis(6) ms(4) modules(0) abstract-service(1) }

-- MTS abstract service
administration, delivery, mTS, submission
---
FROM MTSAbstractService { joint-iso-ccitt
      mhs-motis(6) mts(3) modules(0) mts-abstract-service(1) }

-- Abstract service definition conventions
OBJECT, REFINE
---
FROM AbstractServiceNotation { joint-iso-ccitt
      mhs-motis(6) asdc(2) modules(0) notation(1) };


-- «Root» object type
```

```
mmme OBJECT
      ::= id-mot-mmme


-- Primary refinement

mmme-refinement REFINE mmme AS
      mms
            origination   [S]  PAIRED WITH mms-user
            reception     [S]  PAIRED WITH mms-user
            management    [S]  PAIRED WITH mms-user
      mms-user RECURRING
      ::= id-ref-primary


-- Primary object types

mms-user OBJECT
      PORTS {
            origination   [C],
            reception     [C],
            management    [C] }
      ::= id-mot-mms-user

mms OBJECT
      PORTS {
            origination   [S],
            reception     [S],
            management    [S] }
      ::= id-mot-mms


-- Secondary refinement

mms-refinement REFINE MMS AS
      mTS
            submission    [S] PAIRED WITH mms-ua, mms-ms
            delivery      [S] PAIRED WITH mms-ua, mms-ms
            administration    [S] PAIRED WITH mms-ua, mms-ms
      mms-ua RECURRING
            origination   [S] VISIBLE
            reception     [S] VISIBLE
            management    [S] VISIBLE
      mms-ms RECURRING
            submission    [S] PAIRED WITH mms-ua
            retrieval     [S] PAIRED WITH mms-ua
            administration    [S] PAIRED WITH mms-ua
      acp127au RECURRING
            origination   [S] VISIBLE
            reception     [S] VISIBLE
            management    [S] VISIBLE
      pdau RECURRING
            reception     [S] VISIBLE
      ::= id-ref-secondary
```

```
-- Secondary objects

mms-ua OBJECT
      PORTS {
            origination   [S],
            reception     [S],
            management    [S],
            submission    [C],
            delivery      [C],
            retrieval     [C],
            administration    [C] }
      ::= id-mot-mms-ua

mms-ms OBJECT
      PORTS {
            submission    [S],
            retrieval     [S],
            administration    [S],
            submission    [C],
            delivery      [C],
            administration    [C] }
      ::= id-mot-mms-ua

pdau OBJECT
      PORTS {
            reception     [S] }
      ::= id-mot-pdau

acp127au OBJECT
      PORTS {
            origination   [S],
            reception     [S],
            management    [S] }
      ::= id-mot-acp127au

END --of MMSFunctionalObjects
```

ANNEX G – Reference Definition of Abstract Service

This annex, a supplement to clauses 12 and 13 of the MBS, defines for reference purposes the MMS abstract service. It uses the PORT, ABSTRACT-OPERATION and ABSTRACT-ERROR macros of Recommendation X.407.

```
MMSAbstractService { iso(1) identified-organization(3) NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) module(0)
abstract-service(3) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
--Prologue
-- Exports Everything
IMPORTS

-- IPMS information objects
AutoForwardComment, Heading
---
FROM IPMSInformationObjects { joint-iso-ccitt
      mhs-motis(6) ipms(1) modules(0) information-objects(2) }

-- MMS information objects
MM, MN, MNRN, MRN, MON InformationObject
---
FROM MMSInformationObjects { iso(1) identified-organization(3)
NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) module(0) mms(1)
}

-- MMS object identifiers
id-mpt-management, id-mpt-origination, id-mpt-reception
---
FROM MMSObjectIdentifiers { iso(1) identified-organization(3)
NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) }

-- MTS abstract service
MessageDeliveryEnvelope, MessageSubmissionEnvelope,
MessageSubmissionIdentifier, MessageSubmissionTime,
ORName, ProbeSubmissionenvelope, ProbeSubmissionIdentifier,
ProbeSubmissionTime, RecipientImproperlySpecified,
ReportDeliveryEnvelope, SupplementaryInformation
---
FROM MTSAbstractService { joint-iso-ccitt
      mhs-motis(6) mts(3) modules(0) mts-abstract-service(1) }

-- Abstract service definition conventions
ABSTRACT-ERROR, ABSTRACT-OPERATION, PORT
---
FROM AbstractServiceNotation { joint-iso-ccitt
      mhs-motis(6) asdc(2) modules(0) notation(1) };
```

```
-- Ports
origination PORT
      CONSUMER INVOKES {
            OriginateProbe,
                  --  Although, national implementation may
                  -- support probes within their own domain,
probes are not
                  -- permitted across national boundaries
            OriginateMM,
            OriginateMRN }
      ::= id-pt-origination

reception PORT
      CONSUMER INVOKES {
            ReceiveReport,
            ReceiveMM,
            ReceiveMRN,
            ReceiveMNRN,
            ReceiveMON }
      ::= id-pt-reception

management port
      CONSUMER INVOKES {
            ChangeAutoDiscard,
            ChangeAutoAcknowledgment,
            ChangeAutoForwarding }
      ::= id-pt-management


-- Origination abstract operations

-- Probes are prohibited across national boundaries.

OriginateProbe ::= ABSTRACT-OPERATION
      ARGUMENT SET {
            envelope      [0]  ProbeSubmissionEnvelope,
            content       [1]  MM }
      RESULT SET {
            submission-identifier   [0]
      ProbeSubmissionIdentifier,
            submission-time   [1]   ProbeSubmissionTime }
      ERROR {
            SubscriptionError,
            RecipientImproperlySpecified }

OriginateMM ::= ABSTRACT-OPERATION
      ARGUMENT SET {
            envelope      [0]  MessageSubmissionEnvelope,
            content       [1]  MM }
      RESULT SET {
            submission-identifier   [0]
      MessageSubmissionIdentifier,
            submission-time   [1]   MessageSubmissionTime }
      ERROR {
```

```
            SubscriptionError,
            RecipientImproperlySpecified }

OriginateMRN ::= ABSTRACT-OPERATION
      ARGUMENT SET {
            envelope      [0]  MessageSubmissionEnvelope,
            content       [1]  MRN }
      RESULT SET {
            submission-identifier   [0]
      MessageSubmissionIdentifier,
            submission-time   [1]   MessageSubmissionTime }
      ERROR {
            SubscriptionError,
            RecipientImproperlySpecified }


-- Reception abstract operations

ReceiptReport ::= ABSTRACT-OPERATION
      ARGUMENT SET {
            envelope      [0]  ReportDeliveryEnvelope,
            undelivered-object      [1]   InformationObject
OPTIONAL }
      RESULT
      ERROR { }

ReceiptMM ::= ABSTRACT-OPERATION
      ARGUMENT SET {
            envelope      [0]  MessageDeliveryEnvelope,
            content       [1]  MM }
      RESULT
      ERROR { }

ReceiptMRN ::= ABSTRACT-OPERATION
      ARGUMENT SET {
            envelope      [0]  MessageDeliveryEnvelope,
            content       [1]  MRN }
      RESULT
      ERROR { }

ReceiptMNRN ::= ABSTRACT-OPERATION
      ARGUMENT SET {
            envelope      [0]  MessageDeliveryEnvelope,
            content       [1]  MNRN }
      RESULT
      ERROR { }

ReceiptMON ::= ABSTRACT-OPERATION
      ARGUMENT SET {
            envelope      [0]  MessageDeliveryEnvelope,
            content       [1]  MON }
      RESULT
      ERROR { }

-- Management abstract operations
```

```
-- It should be noted that in cases where an implementation has
dual
-- IPM and MM functionality, the management abstract operations
may be used
-- for support of both types of messaging.

ChangeAutoDiscard ::= ABSTRACT-OPERATION
      ARGUMENT SET {
            auto-discard-expired-MMs      [0]   BOOLEAN,
            auto-discard-obsolete-MMs     [1]   BOOLEAN }
      RESULT
      ERRORS { }

ChangeAutoAcknowledgment ::= ABSTRACT-OPERATION
      ARGUMENT SET {
            auto-acknowledge-MMs            [0]  BOOLEAN,
            auto-acknowledge-suppl-receipt-info [1]
      SupplementaryInformation }
      RESULT
      ERRORS {
            SubscriptionError }

ChangeAutoForwarding ::= ABSTRACT-OPERATION
      ARGUMENT SET {
            autoforward-MMs   [0]   BOOLEAN,
            auto-forward-recipients [1]   SEQUENCE OF ORName
OPTIONAL,
            auto-forward-heading    [2]   Heading OPTIONAL,
            auto-forward-comment    [3]   AutoForwardComment
OPTIONAL }
      RESULT
      ERRORS {
            SubscriptionError,
            RecipientImproperlySpecified }

-- Abstract errors

SubscriptionError ::= ABSTRACT-ERROR
      PARAMETER SET {
            problem       [0]  SubscriptionProblem }

SubscriptionProblem ::= ENUMERATED {
      mms-eos-not-subcribed (0),
      mts-eos-not-subcribed (1) }

END --of MMSAbstractService
```

ANNEX H1 – Reference Definition of Military Heading Extensions

This annex, a supplement to Annex A1, defines for reference purposes the military heading extensions defined for military messaging. It uses the IPMS-EXTENSION macro of clause 7.2.17.

```
MMSHeadingExtensions { iso(1) identified-organization(3) NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) module(0)
heading-extensions(6) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prologue
-- Exports Everything
IMPORTS

-- IPMS information objects
IPMS-EXTENSION, ORDescriptor
---
FROM IPMSInformationObjects { joint-iso-ccitt  mhs-motis(6)
ipms(1)
      modules(0) information-objects(2) }

-- MMS upper bounds
lb-military-sic, ub-military-number-of-sics, ub-military-sic
---
FROM MMSUpperBounds { iso(1) identified-organization(3) NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) module(0) upper-
bounds(0) }

-- MMS object identifiers
id-nato-mmhs-mm-acp127-message-identifier,
id-nato-mmhs-mm-address-list-indicator,
id-nato-mmhs-mm-codress-message,
id-nato-mmhs-mm-copy-precedence, id-nato-mmhs-mm-distribution-
codes,
id-nato-mmhs-mm-exempted-address,
id-nato-mmhs-mm-extended-authorisation-info,
id-nato-mmhs-mm-handling-instructions,
id-nato-mmhs-mm-information-labels,
id-nato-mmhs-mm-message-instructions, id-nato-mmhs-mm-message-
type,
id-nato-mmhs-mm-originator-reference, id-nato-mmhs-mm-originator-
plad,
id-nato-mmhs-mm-other-recipients-indicator,
id-nato-mmhs-mm-pilot-forwarding-info,
id-nato-mmhs-mm-primary-precedence
---
FROM MMSObjectIdentifiers { iso(1) identified-organization(3)
NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) }

-- MTS abstract service
```

```
MessageSecurityLabel
---
FROM MTSAbstractService {joint-iso-ccitt  mhs-motis(6) mts(3)
      modules(0) mts-abstract-service(1) };

-- exempted address

exempted-address IPMS-EXTENSION
      VALUE SEQUENCE OF ExemptedAddress
      ::= id-nato-mmhs-mm-exempted-address

ExemptedAddress ::= ORDescriptor


-- extended authorisation information

extended-authorisation-info IPMS-EXTENSION
      VALUE ExtendedAuthorisationInfo
      ::= id-nato-mmhs-mm-extended-authorisation-info

      ExtendedAuthorisationInfo ::= UTCTime
            -- UTCTime as defined in 8.5.4 of ITU-T X.411


-- Distribution codes
-- will carry subject indicator codes and leave room for
expansion.

distribution-codes IPMS-EXTENSION
      VALUE DistributionCodes
      ::= id-nato-mmhs-mm-distribution-codes

DistributionCodes ::= SET {
      sics               [0]  SEQUENCE SIZE
                                    (1..ub-military-number-of-
sics) OF
                                    Sic OPTIONAL,
      dist-Extensions    [1]  SEQUENCE OF
                                    DistributionExtensionField
OPTIONAL }

Sic ::= PrintableString (SIZE (lb-military-sic..ub-military-sic))

DistributionExtensionField ::= SEQUENCE {
      dist-type          OBJECT IDENTIFIER,
      dist-value         ANY DEFINED BY dist-type }


-- Handling instructions

handling-instructions IPMS-EXTENSION
      VALUE HandlingInstructions
      ::= id-nato-mmhs-mm-handling-instructions

HandlingInstructions ::= SEQUENCE OF MilitaryString
```

```
MilitaryString ::= PrintableString (SIZE(1..ub-military-string))


-- Message instructions
-- will carry operating signals

message-instructions IPMS-EXTENSION
      VALUE MessageInstructions
      ::= id-nato-mmhs-mm-message-instructions

MessageInstructions ::= SEQUENCE OF MilitaryString


-- Codress message
-- Needed for transition or as long as codress messages need to be
carried.

codress-message IPMS-EXTENSION
      VALUE CodressMessage
      ::= id-nato-mmhs-mm-codress-message

CodressMessage ::= INTEGER


-- Originator reference
-- only used if a user designated identifier string becomes
important.

originator-reference IPMS-EXTENSION
      VALUE OriginatorReference
      ::= id-nato-mmhs-mm-originator-reference

OriginatorReference ::= MilitaryString


-- Primary reference

primary-precedence IPMS-EXTENSION
      VALUE MMHSPrecedence
      ::= id-nato-mmhs-mm-primary-precedence

MMHSPrecedence ::= INTEGER {deferred (0), routine (1), priority
(2), immediate (3),
      flash (4), override (5)}

-- Note: Values 0 to 15 are reserved for NATO defined precedence
levels.
-- Values 16 to 31 are reserved for national user.


-- Copy precedence

copy-precedence IPMS-EXTENSION
      VALUE MMHSPrecedence
```

```
      ::= id-nato-mmhs-mm-copy-precedence

-- Note: Values 0 to 15 are reserved for NATO defined precedence
levels.
-- Values 16 to 31 are reserved for national user.

-- Message type

message-type IPMS-EXTENSION
      VALUE MessageType
      ::=id-nato-mmhs-mm-message-type

MessageType ::= SET{
      type               [0]  TypeMessage,
      identifier         [1]  MessageIdentifier OPTIONAL }

TypeMessage ::= INTEGER {exercise(0), operation(1), project(2),
drill(3) }

-- Note: Values 0 to 127 are reserved for NATO defined Message
Type
-- identifiers. Values above 128 to 255 are not defined by NATO
and may
-- be used nationally or bilaterally.

MessageIdentifier ::= MilitaryString


-- Address list indicator

address-list-indicator IPMS-EXTENSION
      VALUE SEQUENCE OF AddressListDesignator
      ::=id-nato-mmhs-mm-address-list-indicator

AddressListDesignator ::=SET {
      type               [0]  INTEGER
                                 { primaryAddressList(0),
copyAddressList(1) },
      listName           [1]  ORDescriptor,
      notificationRequest [2]  AddressListRequest OPTIONAL,
      replyRequest       [3]  AddressListRequest OPTIONAL }

AddressListRequest ::= INTEGER { action(0), info(1), both(2) }

-- Other recipients indicator

other-recipients-indicator IPMS-EXTENSION
      VALUE SEQUENCE OF OtherRecipientDesignator
      ::=id-nato-mmhs-mm-other-recipients-indicator

OtherRecipientDesignator ::= SET {
      type               [0]  INTEGER { primary(0), copy(1) },
      designator         [1]  MilitaryString }
```

```
-- pilot forwarding information

pilot-forwarding-info IPMS-EXTENSION
      VALUE SEQUENCE OF PilotInformation
      ::= id-nato-mmhs-mm-pilot-forwarding-info

PilotInformation ::= SEQUENCE {
      pilotPrecedence     [0]  MMHSPrecedence OPTIONAL,
            -- Note: Values 0 to 15 are reserved for NATO defined
precedence levels.
            -- Values 16 to 31 are reserved for national use.
      pilotRecipient      [1]  SEQUENCE OF ORDescriptor OPTIONAL,
      pilotSecurity       [2]  MessageSecurityLabel OPTIONAL,
      pilotHandling       [3]  SEQUENCE OF MilitaryString OPTIONAL}


-- Acp127 message identifier
-- a string to store routing indicator, station serial number and
julian file
-- time seperated by spaces.

acp127-message-identifier IPMS-EXTENSION
      VALUE Acp127MessageIdentifier
      ::= id-nato-mmhs-mm-acp127-message-identifier

Acp127MessageIdentifier ::= MilitaryString


-- Originator PLAD

originator-plad IPMS-EXTENSION
      VALUE OriginatorPlad
      ::= id-nato-mmhs-mm-originator-plad

OriginatorPlad ::= MilitaryString

-- Information label

security-information-labels IPMS-EXTENSION
      VALUE SecurityInformationLabels
      ::= id-nato-mmhs-mm-information-labels

SecurityInformationLabels ::= SEQUENCE {
      content-security-label  [0]   SecurityLabel,
            -- SecurityLabel as defined in 8.5.9 of ITU-T X.411
      heading-security-label  [1]   SecurityLabel OPTIONAL,
      body-part-security-labels     [2]   SEQUENCE OF
BodyPartSecurityLabel OPTIONAL }

BodyPartSecurityLabel  :: SET {
      body-part-security-label      [0]   SecurityLabel,
      body-part-sequence-number     [1]   BodyPartSequenceNumber
OPTIONAL }

BodyPartSequenceNumber ::= INTEGER
```

```
--  Note: If all body parts of the message are labelled, each
--  element in the body sequence above shall correspond to the
--  same numbered element of the Body sequence, and the body
--  part sequence number may be absent. (i.e. the first element
--  of this field shall correspond to the first body part, etc.
--  Otherwise the body part sequence number shall be present
--  and shall correspond to the sequence of the body part
--  to which the security label relates. (i.e. the value of the
--  body part sequence number shall correspond to sequence in
which
--  the originator encoded the body parts of the message).

-- NOTE: The security-information-labels heading extension is now
-- deprecated. Its use is, therefore, discouraged. See STANAG 4406
-- Annex B for instruction on the use of its replacement, the
-- ESSSecurityLabel.

END -- of Military heading extensions used in MMS
```

ANNEX H2 – Reference Definition of per recipient specifier Extensions

This annex, a supplement to Annex A2, defines for reference purposes the PerRecipientSpecifier extensions defined for military messaging. It uses the IPMS-EXTENSION macro of clause 7.2.17.

```
MMSPerRecipientSpecifierExtensions { iso(1) identified-
organization(3) NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) module(0)
      per-recipient-specifier-extensions(11) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prologue
-- Exports Everything
IMPORTS

-- IPMS information objects
IPMS-EXTENSION
---
FROM IPMSInformationObjects { joint-iso-ccitt  mhs-motis(6)
ipms(1)
      modules(0) information-objects(2) }

-- MMS object identifiers
id-nato-mmhs-mm-acp127-notification-request
---
FROM MMSObjectIdentifiers { iso(1) identified-organization(3)
NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) };

-- ACP127 notification request
-- The following definitions are made in order to support
-- informing the originator of a message that the subject message
-- has reached a gateway to an ACP 127 domain.

acp127-notification-request IPMS-EXTENSION
      VALUE Acp127NotificationType
      ::= id-nato-mmhs-mm-acp127-notification-request

Acp127NotificationType ::= BIT STRING {
      acp127-nn (0),      -- negative notification
      acp127-pn (1),      -- positive notification
      acp127-tn (2)}      -- transfer notification

END -- of MMS per recipient pecifier extensions
```

ANNEX H3 – Reference Definition of OtherNotificationType Extensions

This annex, a supplement to Annex A3, defines for reference purposes the OtherNotificationType extensions defined for military messaging. It uses the IPMS-EXTENSION macro of clause 7.2.17.

```
MMSOtherNotificationTypeExtensions { iso(1) identified-
organization(3) NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) module(0)
      other-notification-type-extensions(12) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prologue
-- Exports Everything
IMPORTS

-- IPMS information objects
IPMS-EXTENSION, ReceiptTimeField
---
FROM IPMSInformationObjects { joint-iso-ccitt  mhs-motis(6)
ipms(1)
      modules(0) information-objects(2) }

-- MMS upper bounds
ub-military-bigstring
---
FROM MMSUpperBounds { iso(1) identified-organization(3) NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) module(0) upper-
bounds(0) }

-- MMS object identifiers
id-nato-mmhs-mm-acp127-notification-response
---
FROM MMSObjectIdentifiers { iso(1) identified-organization(3)
NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) }


-- MMS heading extensions
AddressListDesignator
---
FROM MMSHeadingExtensions { iso(1) identified-organization(3)
NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) module(0)
      heading-extensions(6) }

-- MMS per recipient specifier extensions
Acp127NotificationType
---
FROM MMSPerRecipientSpecifierExtensions { iso(1) identified-
organization(3)
      NATO(26) STANAGS(0) MMHS(4406) object-identifiers(0)
```

```
module(0)
      per-recipient-specifier-extensions(11) };

--ACP127 notification response
acp127-notification-response IPMS-EXTENSION
      VALUE Acp127NotificationResponse
      ::= id-nato-mmhs-mm-acp127-notification-response

Acp127NotificationResponse ::= SET {
      acp127-notification-type      [0]   Acp127NotificationType,
      receipt-time        [1]  ReceiptTimeField,
      addressListIndicator    [2]   AddressListIndicator OPTIONAL,
      acp127-recipient    [3]  Acp127Recipient OPTIONAL,
      acp127-supp-info    [4]  Acp127SuppInfo OPTIONAL }

AddressListIndicator ::= SEQUENCE OF AddressListDesignator

Acp127Recipient ::= PrintableString (SIZE (1..ub-military-
bigstring))

Acp127SuppInfo ::= PrintableString  (SIZE (1..ub-military-
bigstring))

END -- of MMS OtherNotificationType extensions
```

ANNEX I1 – Reference Definition of Extended Body Part Types

This annex, a supplement to Annex B.1 defines for reference purposes the extended body part types defined for military messaging.

Note, all extended body parts defined in Annex I of X.420 are also valid in an MM environment.

```
MMSExtendedBodyPartTypes { iso(1) identified-organization(3)
NATO(26) STANAGS(0)
      MMHS(4406) object-identifiers(0) module(0) extended-body-
part-types(7) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prologue
-- Exports Everything
IMPORTS

-- IPMS information objects
EXTENDED-BODY-PART-TYPE
---
FROM IPMSInformationObjects { joint-iso-ccitt  mhs-motis(6)
ipms(1)
      modules(0) information-objects(2) }

-- MMS information objects
MM
---
FROM MMSInformationObjects { iso(1) identified-organization(3)
NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) module(0) mms(1)
}

-- MMS upper lower bounds
ub-data-size
---
FROM MMSUpperBounds { iso(1) identified-organization(3) NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) module(0) upper-
bounds(0) }

-- MTS Abstract Service
MessageDeliveryTime, OtherMessageDeliveryFields
---
FROM MTSAbstractService { joint-iso-ccitt  mhs-motis(6) mts(3)
      modules(0) mts-abstract-service(1) }

-- MMS object identifiers
---
id-nato-mmhs-et-adatp3,
id-nato-mmhs-et-adatp3-parameters,
id-nato-mmhs-et-acp127data,
id-nato-mmhs-et-acp127data-parameters,
```

```
id-nato-mmhs-et-corrections,
id-nato-mmhs-et-corrections-parameters,
id-nato-mmhs-et-forwarded-encrypted,
id-nato-mmhs-et-forwarded-encrypted-parameters,
id-nato-mmhs-et-mm-message,
id-nato-mmhs-et-mm-message-parameters
---
FROM MMSObjectIdentifiers { iso(1) identified-organization(3)
NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) };


-- extended adatp3 bodypart
adatp3-body-part EXTENDED-BODY-PART-TYPE
      PARAMETERS  ADatP3Parameters IDENTIFIED BY
                        id-nato-mmhs-et-adatp3-parameters
      DATA                ADatP3Data
      ::= id-nato-mmhs-et-adatp3

ADatP3Parameters ::= INTEGER DEFAULT (0)

ADatP3Data ::= CHOICE{
      lineOriented        [0]  IMPLICIT IA5String,
      setOriented         [1]  IMPLICIT SEQUENCE OF IA5String }

-- extended corrections body part

corrections-body-part EXTENDED-BODY-PART-TYPE
      PARAMETERS  CorrectionsParameters IDENTIFIED BY
                        id-nato-mmhs-et-corrections-parameters
      DATA                CorrectionsData
      ::= id-nato-mmhs-et-corrections

CorrectionsParameters ::= INTEGER

CorrectionsData ::= IA5String

-- extended forwarded encrypted body part

forwarded-encrypted-body-part EXTENDED-BODY-PART-TYPE
      PARAMETERS  ForwardedEncryptedParameters IDENTIFIED BY
                        id-nato-mmhs-et-forwarded-encrypted-
parameters
      DATA                ForwardedEncryptedData
      ::= id-nato-mmhs-et-forwarded-encrypted


-- A forwarded-encrypted-body must contain the delivery
information,
-- containing the content type which will indicate whether the
forwarded
-- encrypted message is an MM or IPM. All security related
information --
-- (i.e., token) of the original message must be forwarded.
```

```
ForwardedEncryptedParameters ::= SET {
      delivery-time       [0]  MessageDeliveryTime OPTIONAL,
      delivery-envelope   [1]  OtherMessageDeliveryFields }
                                    -- 2/X.411, part 9 of 26.

ForwardedEncryptedData ::= BIT STRING

-- extended MM message body part

mm-message-body-part EXTENDED-BODY-PART-TYPE
      PARAMETERS  MMMessageParameters IDENTIFIED BY
                        id-nato-mmhs-et-mm-message-parameters
      DATA                MMMessageData
      ::= id-nato-mmhs-et-mm-message

-- An mm-message-body-part can either carry a forwarded M1M or a
forwarded
-- IPM. In the case of a message-body-part, as defined in X.420,
-- it can only carry an IPM.

MMMessageParameters ::= SET {
      delivery-time       [0]  MessageDeliveryTime OPTIONAL,
      delivery-envelope   [1]  OtherMessageDeliveryFields }

MMMessageData ::= MM

-- extended acp127data body part

acp127data-body-part EXTENDED-BODY-PART-TYPE
      PARAMETERS  ACP127DataParameters IDENTIFIED BY
                        id-nato-mmhs-et-acp127data-parameters
      DATA                ACP127DataData
      ::= id-nato-mmhs-et-acp127data

ACP127DataParameters ::= INTEGER

ACP127DataData ::= IA5String (SIZE(1..ub-data-size))


END -- of MMS ExtendedBodyPartTypes
```

ANNEX J1 – Reference Definition of Message Store Attributes

This annex is a supplement to annex C and defines, for reference purposes, the MS attributes specific to military messaging (MM-MS). The MM-MS attributes are a super-set of Interpersonal Messaging attributes defined in ITU-T X.420/IS 10021-7, as such only the delta is defined here.

```
MMSMessageStoreAttributes { iso(1) identified-organization(3)
NATO(26) STANAGS(0)
      MMHS(4406) object-identifiers(0) module(0) message-store-
attributes(8) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prologue
-- Exports Everything
IMPORTS

-- MMS heading extensions
Acp127MessageIdentifier,
AddressListDesignator,
BodyPartSecurityLabel,
CodressMessage,
DistributionCodes,
DistributionExtensionField,
Sic,
ExemptedAddress,
ExtendedAuthorisationInfo,
HandlingInstructions,
MessageInstructions,
MessageType,
MMHSPrecedence,
MMSecurityInformationLabels,
OriginatorPlad,
OriginatorReference,
OtherRecipientDesignator,
PilotInformation
---
FROM MMSHeadingExtensions { iso(1) identified-organization(3)
NATO(26) STANAGS(0)
      MMHS(4406) object-identifiers(0) module(0) heading-
extensions(6) }

 -- MMS per recipient specifier extensions
Acp127NotificationType
---
FROM MMSPerRecipientSpecifierExtensions { iso(1) identified-
organization(3)
      NATO(26) STANAGS(0) MMHS(4406) object-identifiers(0)
      module(0) per-recipient-specifier-extensions(11) }

-- MMS other notification type extensions
Acp127NotificationResponse
```

```
---
FROM MMSOtherNotificationTypeExtensions { iso(1) identified-
organization(3) NATO(26)
      STANAGS(0) MMHS(4406) object-identifiers(0) module(0)
      other-notification-type-extensions(12) }

-- MMS object identifiers
id-nato-mmhs-hat-acp127-notification-request,
id-nato-mmhs-hat-acp127-message-identifier,
id-nato-mmhs-hat-address-list-indicator,
id-nato-mmhs-hat-body-part-security-label,
id-nato-mmhs-hat-copy-precedence,
id-nato-mmhs-hat-codress-message,
id-nato-mmhs-hat-distribution-codes,
id-nato-mmhs-hat-distribution-extensions,
id-nato-mmhs-hat-extended-authorisation-info,
id-nato-mmhs-hat-exempted-address,
id-nato-mmhs-hat-handling-instructions,
id-nato-mmhs-hat-message-type,
id-nato-mmhs-hat-message-instructions,
id-nato-mmhs-hat-originator-reference,
id-nato-mmhs-hat-originator-plad,
id-nato-mmhs-hat-other-recipients-indicator,
id-nato-mmhs-hat-pilot-forwarding-info,
id-nato-mmhs-hat-primary-precedence,
id-nato-mmhs-hat-security-information-labels,
id-nato-mmhs-hat-sic-codes,
id-nato-mmhs-nat-acp127-notification-response
---
FROM MMSObjectIdentifiers { iso(1) identified-organization(3)
NATO(26) STANAGS(0)
      MMHS(4406) object-identifiers(0) };


exempted-address ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX ExemptedAddress
      MATCHES FOR EQUALITY
      MULTI VALUE
      ::= id-nato-mmhs-hat-exempted-address

extended-authorisation-info ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX ExtendedAuthorisationInfo
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-extended-authorisation-info

distribution-codes ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX DistributionCodes
      MATCHES FOR EQUALITY
      MULTI VALUE
      ::= id-nato-mmhs-hat-distribution-codes

handling-instructions ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX HandlingInstructions
      MATCHES FOR EQUALITY
```

```
      SINGLE VALUE
      ::= id-nato-mmhs-hat-handling-instructions

sic-codes ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX Sic
      MATCHES FOR EQUALITY
      MULTI VALUE
      ::= id-nato-mmhs-hat-sic-codes

distribution-extensions ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX DistributionExtensionField
      MATCHES FOR EQUALITY
            -- The dist-value field shall be disregarded for the
purpose of
            -- matching, unless the syntax of the field is
recognized based on the
            -- value of the dist-type field.
      MULTI VALUE
      ::= id-nato-mmhs-hat-distribution-extensions

message-instructions ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX MessageInstructions
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-message-instructions

codress-message ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX CodressMessage
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-codress-message

originator-reference ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX OriginatorReference
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-originator-reference

primary-precedence ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX MMHSPrecedence
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-primary-precedence

copy-precedence ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX MMHSPrecedence
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-copy-precedence

message-type ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX MessageType
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-message-type
```

```
address-list-indicator ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX AddressListDesignator
      MATCHES FOR EQUALITY
      MULTI VALUE
      ::= id-nato-mmhs-hat-address-list-indicator

other-recipients-indicator ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX OtherRecipientDesignator
      MATCHES FOR EQUALITY
      MULTI VALUE
      ::= id-nato-mmhs-hat-other-recipients-indicator

pilot-forwarding-info ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX PilotInformation
      MATCHES FOR EQUALITY
      MULTI VALUE
      ::= id-nato-mmhs-hat-pilot-forwarding-info

acp127-message-identifier ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX Acp127MessageIdentifier
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-acp127-message-identifier

originator-plad ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX OriginatorPlad -- modified
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-originator-plad

acp127-notification-request ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX Acp127NotificationType
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-acp127-notification-request

body-part-security-label ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX BodyPartSecurityLabel
      MATCHES FOR EQUALITY
      MULTI VALUE
      ::= id-nato-mmhs-hat-body-part-security-label

security-information-labels ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX SecurityInformationLabels
      MATCHES FOR EQUALITY
      SINGLE VALUE
      ::= id-nato-mmhs-hat-security-information-labels

-- NOTE: The body-part-security-label and security-information-
label
-- attributes are now deprecated.  Their use is, therefore,
-- discouraged. See STANAG 4406 Annex B for instruction
-- on the use of the ESSSecurityLabel.
```

```
-- NOTIFICATIONS

-- ACP 127 Notification Response

acp127-notification-response ATTRIBUTE
      WITH ATTRIBUTE-SYNTAX Acp127NotificationResponse
      MATCHES FOR EQUALITY
      MULTI VALUE
      ::= id-nato-mmhs-nat-acp127-notification-response

END -- of MMSMessagesStoreAttributes
```

ANNEX K – REFERENCE DEFINITION OF MMS UPPER BOUNDS

This annex defines, for reference purposes, the upper bounds of various variable-length information items whose abstract syntaxes are defined in the ASN.1 modules of prior annexes.

```
MMSUpperBounds { iso(1) identified-organization(3) NATO(26)
STANAGS(0)
      MMHS(4406) object-identifiers(0) module(0) upper-bounds(0) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prologue
-- Exports Everything
IMPORTS -- nothing --;

-- Upper Bounds
ub-military-string        INTEGER ::= 69
ub-military-number-of-sics    INTEGER ::= 8
lb-military-sic           INTEGER ::= 3
ub-military-sic           INTEGER ::= 8

ub-military-bigstring     INTEGER ::= 128
ub-data-size              INTEGER ::= 65535
                               -- size of ACP127DATADATA

END -- of MMSUpperBouds
```

ANNEX B

INTEROPERABILITY OF SECURE MMHS

This annex defines the security services and the implementation requirements to ensure interoperability of the security solution for Military Messaging. This annex is the same as Annex B of STANAG 4406.

ANNEX B: INTEROPERABILITY OF SECURE MMHS

[Conforming systems SHALL comply with this annex.]

1. BACKGROUND

This Annex defines the long term security solution for STANAG 4406. The Long Term Solution provides an interoperability mechanism based on a single common protocol selected to satisfy the security requirements for Allied interoperability. The Long Term Solution replaces the legacy protocols and the Interim Solution defined as PCT (Protecting Content Type) in STANAG 4406 Ed.1 Annex B.

This annex describes how the document [NATOSMIMEProfile] is to be used in order to achieve interoperability between the security functionality of the MMHS. The [NATOSMIMEProfile] document further defines the use of the IETF security standards S/MIME and refers to several other documents in defining the security mechanism to be used for STANAG 4406 Ed.2. In order to have a complete picture of the security mechanisms, this Annex B should therefore be read together with the related documents (see section 8 for references). Since no specification for X.400 use of S/MIME existed, NATO needed to develop new material. However, if this material were developed solely within NATO, it could yield a separate class of military products that would be distinctly different than their COTS counterparts. Developing an IETF RFC would keep the work in the view of industry, and would increase the likelihood of influencing COTS. Another reason was a desire for independence from the underlying message handling technology. The S/MIME specifications as of February 2000 provided a specification for use of CMS with SMTP/MIME message handling. This was not suitable for support of existing MMHS protocols, which are based on X.400.

Addressing CMS use with X.400 within the IETF allows specifications to more generically refer to CMS and S/MIME to provide security to either the current or future MMHS protocols. Sponsoring NATO nations have presented two RFCs to the IETF forum (see [X400Wrap] and [X400Transport]).

The ultimate objective was to achieve use of COTS S/MIME products to satisfy all MMHS security requirements. However, it was recognised that some residual military-specific features was required. A third specification, the NATO profile of S/MIME, was therefore developed. This profile is as content-independent as possible, and addresses military use of S/MIME in general.

2. SCOPE

This Annex defines and mandates the use of a Solution for security interoperability between Allies' MMHS. The scope of this solution is limited to exchange of X.400 message content (e.g. P772).

3. TERMINOLOGY

The key words "MUST", "SHALL", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY" in this document are to be interpreted as described in RFC 2119 [MUSTSHOULD].

4. DEFINITIONS

For the purposes of this document, the following definitions apply.

Certificate: A type that binds an entity's distinguished name to a public key with a digital signature.

7-bit data: Text data with lines less than 998 characters long, where none of the characters have the 8th bit set, and there are no NULL characters. <CR> and <LF> occur only as part of a <CR><LF> end of line delimiter.

8-bit data: Text data with lines less than 998 characters, and where none of the characters are NULL characters. <CR> and <LF> occur only as part of a <CR><LF> end of line delimiter.

Binary data: Arbitrary data.

Transfer Encoding: A reversible transformation made on data so 8-bit or binary data may be sent via a channel that only transmits 7-bit data.

Receiving agent: Software that interprets and processes S/MIME CMS objects.

Sending agent: Software that creates S/MIME CMS objects.

S/MIME agent: User software that is a receiving agent, a sending agent, or both.

Military Messaging: Exchange of Messages as defined by STANAG 4406 and ACP 123.

5. BACKWARDS COMPATIBILITY WITH PCT

See Annex G of this STANAG.

6. ARCHITECTURE OF LONG TERM SOLUTION

The Military Message Handling System (MMHS) Long Term Solution (LTS) should be based on commercial S/MIME standards because of the long-range goal of using an acceptable commercial protocol, and the belief that the most likely commercial protocol is currently the Secure Multipurpose Internet Mail Extensions (S/MIME). Use of a commercial protocol offers advantages in cost, schedule, life-cycle availability, and integration into other products and access to the latest technology. The ultimate objective is to achieve use of COTS S/MIME products to satisfy all MMHS security requirements. However, it is recognized that some residual military-specific features may be required for some period of time. These will result in a military S/MIME profile or military-specific configuration of the COTS products. The MMHS Native S/MIME will hereinafter be referred to as Native S/MIME.

6.1 Triple Wrapping Structure

The Native S/MIME interoperability architecture MAY be based on use of the S/MIME “triple-wrap” scenario. Different nations and organizations MAY utilize the triple wrappings in different ways to provide flexible interoperability. The full triple wrapping is composed of the following:

- In order to reduce the message size, an X.400 message MAY be compressed using an OPTIONAL *CompressedData* wrapper as described in [COMPRData]. This will not only reduce the transmission time, but will also reduce the signing and encryption time of the message.

- An inner *SignedData* wrapper providing a digital signature over the message plus a set of attributes such as a security label.

- An intermediate *EnvelopedData* wrapper providing encrypted transfer of the inner *SignedData*.

- An outer *SignedData* wrapper providing integrity protection and authentication of the *EnvelopedData* wrapper and support for services such as mail list expansion.

Please see the [NATOSMIMEProfile] for details regarding conformance to this Annex B.

The Military Message Content (shown in Exhibit 1) may consist of an valid instance of the P772 or other X.400 content type. Note that the definition of the *MMSInformationObjects* in Annex A allows a P772 content type to assume the form of either a military message (MM) or a military notification (MN). S/MIME protections can be applied equally to either an MM or MN. An MN is an X.400 receipt, and should not be confused with an S/MIME ESS Signed Receipt. The same interpretation applies to other supported X.400 content types (e.g., P2/P22) that employ their own notification messages.

6.2 Interoperability Architecture

The interoperability solution described in this Annex, is designed for use between the Allied domains. There are several ways for nations to implement a compatible internal security solution. Exhibit 2 illustrates three examples of implementations, in domains A, B and C, within the interoperability architecture.

(Note: only application level security is addressed here; network level security may be required for confidentiality, depending on the implementations and the policies in force.)

Depending on the implementations, messages transiting between Allied domains can be either triple-wrapped or signed-only:

- Domain A implements only the signature part of S/MIME.
- **Incoming Messages**: when a triple-wrapped message arrives, the border device removes the outer layers, but the innermost layer is unmodified.
- **Outgoing Messages**: depending on the implementation, outgoing messages are signed-only and additionally may have outer layers added by the border device.
- Domain B implements Native S/MIME internally.

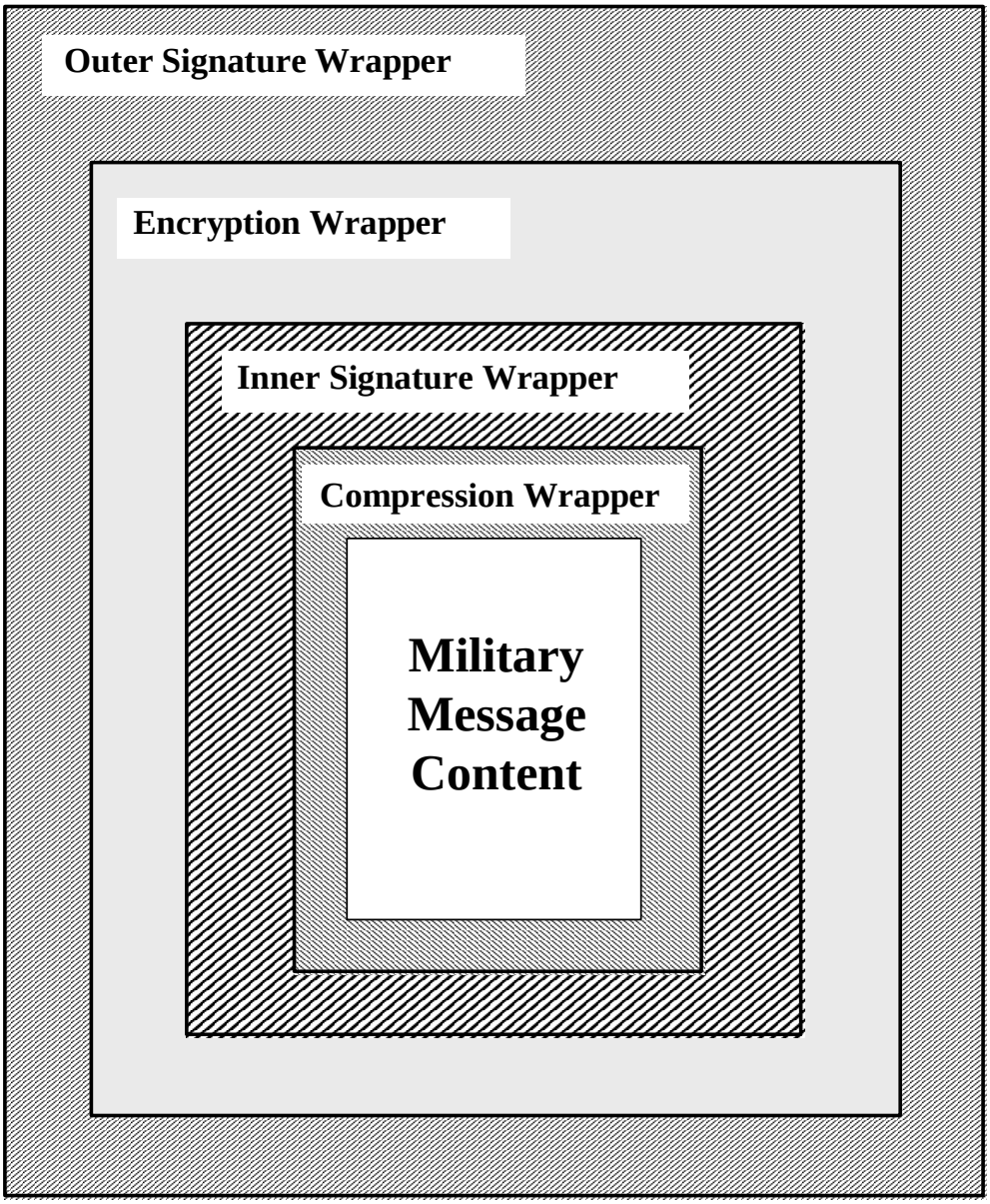


Exhibit 1 – S/MIME Triple Wrapped Message with Compression Wrapper

- **Incoming Messages**: when a border device receives an incoming signed-only message it will generate the outer layers for processing internally. Incoming triple-wrapped messages are unchanged.

- **Outgoing Messages**: triple-wrapped messages exiting Domain B are unchanged.

- Domain C implements a triple-wrapped S/MIME solution with an alternate encryption.

- **Incoming Messages**: the outer layers of incoming messages, if any, are replaced by national outer layers by a border device, which also removes the outer layers of outgoing messages, depending on the implementation.

- **Outgoing Messages**: outgoing messages are signed-only or may have outer layers added by the border device.

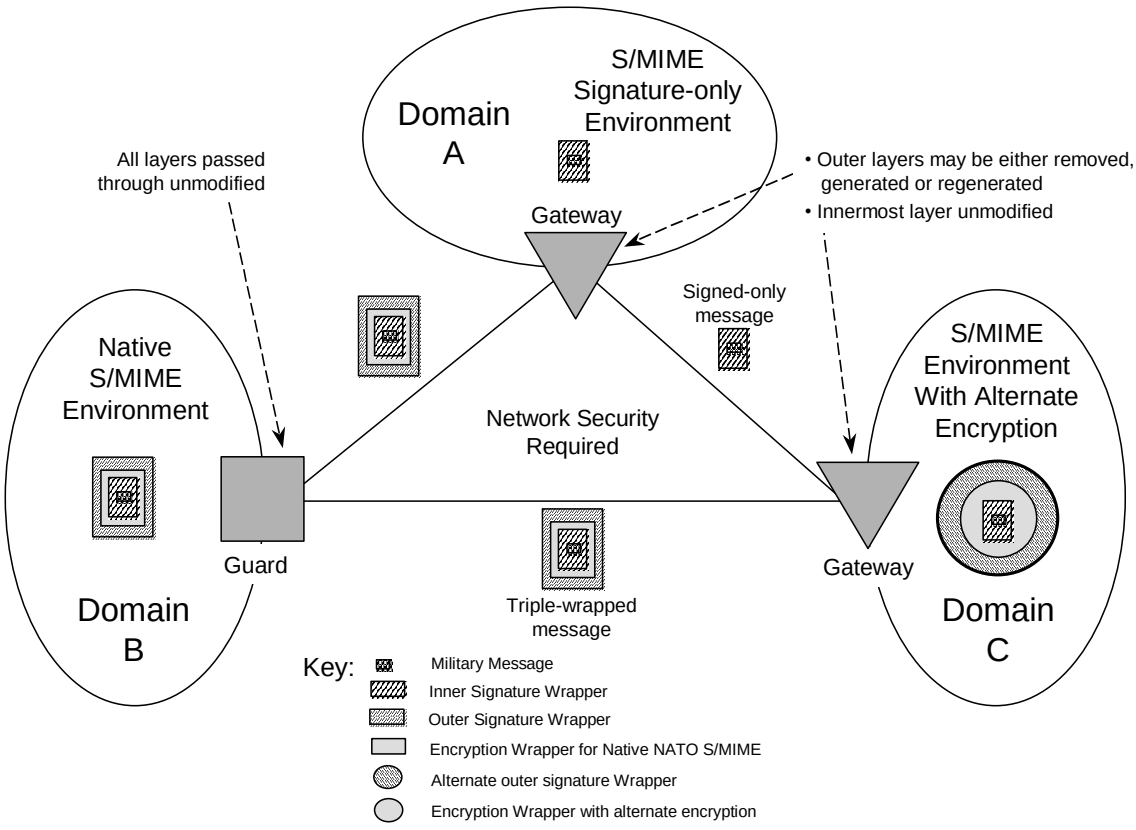


Exhibit 2 – MMHS Security Long Term Interoperability Architecture

7. SECURITY SERVICES VERSUS S/MIME MECHANISMS

The following security services are defined in this Annex. For each of the security services the conformance requirements for the service on both the originating side and the reception side is shown. As an example; the notation (M/M) means that it is Mandatory required to support the service on both sides.

- Access Control (M/M)
- Authentication of Origin (M/M)
- Non-repudiation of Origin (M/M)
- Message Integrity (M/M)
- Message Data Separation (O/O)
- Security Labels (M/M)
- Non-repudiation of Receipt (O/M)
- Secure Mailing Lists (M/M)
- Message Counter Signature (O/O)
- Certificate Binding (O/O)
- Compressed Data (O/O)

The following sections describes each of the services and how they are to be implemented using the related S/MIME mechanisms.

7.1 Access Control

Access control is a means of enforcing the authorization of users to access a message. The sensitivity information in a security label can be compared with a user's authorizations to determine if the user is allowed to access the content of the message. Access controls are performed in each MMHS domain in accordance with the security policy in force. MMHS systems must enforce their own native security policies, plus any other security policies described by their treaty obligations. To adequately address these requirements, standardized machine-readable data structures has been established for security labels. Traditional printed markings may also be used as appropriate. Security labels SHALL be implemented according to section 7.6 of this Annex.

This effectively means that national MMHS implementations MUST be able to transfer messages with either national or NATO security policies and labels,

and that some user workstations SHOULD be able to handle both national and NATO messages. For NATO traffic, between NATO and NATO countries and between NATO countries, NATO security labels SHALL be supported for access control.

7.2 Authentication of Origin

The Authentication service gives assurance of the identity of some entity (a person or a system). It is the means of gaining confidence that an originator of a message is who he claims to be.

The implementation of this service SHALL follow the specifications given in the document “The NATO Profile for the Use of S/MIME CMS and ESS” section 3.3 [NATOSMIMEProfile].

This profile will, together with a trusted mechanism for handling certificates and CRLs (e.g. PKI), implement the service for authentication of origin.

7.3 Non-repudiation of Origin

The Non-repudiation of origin service protects against the originator to a message exchange later falsely denying that the exchange occurred or the time the exchange occurred.

The implementation of this service SHALL follow the specifications given in the document “The NATO Profile for the Use of S/MIME CMS and ESS” section 3.3 [NATOSMIMEProfile].

This profile will, together with a trusted mechanism for handling certificates and CRLs (e.g. PKI), implement the service for non-repudiation of origin.

7.4 Message Integrity

The Message Integrity service provides an indication to message recipients whether the message has been modified, deleted or substituted without authorisation. Also provides integrity over any signed attributes attached to the message.

The implementation of this service SHALL follow the specifications given in “The NATO Profile for the Use of S/MIME CMS and ESS” section 3.3 [NATOSMIMEProfile].

This profile will, together with a trusted mechanism for handling certificates and CRLs (e.g. PKI), implement the service for message integrity.

7.5 Message Data Separation

The Message Data Separation service cryptographically separates data contained in one message from that contained in another message. The *Message Data Separation* 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 implementation of this service SHALL follow the specifications given in "The NATO Profile for the Use of S/MIME CMS and ESS" section 3.4 [NATOSMIMEProfile].

This profile will, together with a trusted mechanism for handling certificates and CRLs (e.g. PKI), implement the service for message data separation.

In some scenarios this service will not go from the originators UA to the recipients UA, but will be terminated at a gateway. Some domains have such requirements in order to inspect the message for viruses or to enforce inspection control over the flow of message in and out of a domain. For such scenarios the [DOMSEC] standard gives guidance on how to do the security processing.

7.6 Security Labels

Security Labels provides an indication of the security policy, sensitivity, compartments, and other handling caveats associated with the message. The *Security labels* service can be used for purposes such as access control or a source of routing information.

The implementation of this service SHALL follow the specifications given in "The NATO Profile for the Use of S/MIME CMS and ESS" section 4.3 [NATOSMIMEProfile].

7.7 Non-repudiation of Receipt

The Non-repudiation of Receipt (or Message-notification Binding) service provides a cryptographic binding between an original signed message, and a receipt sent in response to that message. The *Message-notification Binding* service provides assurance to an originator that the message received was the same as the message sent. Note that this form of non-repudiation does not extend beyond receipt. It does not necessarily imply that the recipient read the data or acted upon them in any way.

The implementation of this service SHALL follow the specifications given in "The NATO Profile for the Use of S/MIME CMS and ESS" section 4.2 [NATOSMIMEProfile].

This profile will, together with a trusted mechanism for handling certificates and CRLs (e.g. PKI), implement the service for non-repudiation of receipt.

7.8 Secure Mailing Lists

This 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 Mail List (ML). The *Secure Mailing List* service provides for a more efficient management of large MLs, and includes a mechanism to prevent mail loops.

The implementation of this service SHALL follow the specifications given in "The NATO Profile for the Use of S/MIME CMS and ESS" section 4.4 [NATOSMIMEProfile].

This profile will, together with a trusted mechanism for handling certificates and CRLs (e.g. PKI), implement the service for secure mail lists.

7.9 Message Counter-signature

Message counter-signature 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 implementation of this service SHALL follow the specifications given in "The NATO Profile for the Use of S/MIME CMS and ESS" section 3.5 [NATOSMIMEProfile].

This profile will, together with a trusted mechanism for handling certificates and CRLs (e.g. PKI), implement the service for Countersignature.

7.10 Certificate Binding

This service allows for a certificate, which is sent with the message to be cryptographically bound to the message.

The implementation of this service SHALL follow the specifications given in "The NATO Profile for the Use of S/MIME CMS and ESS" section 4.5 [NATOSMIMEProfile].

This profile will, together with a trusted mechanism for handling certificates and CRLs (e.g. PKI), implement the service for certificate binding.

7.11 Compressed Data

The Compressed Data service reduces message size, which has several security benefits. Data compression helps to prevent possible attacks by eliminating data redundancy. Data compression also reduces the amount of time required for encryption. Minimizing the message size helps to protect transfer system availability and may provide an element of robustness in the event of denial of service attacks.

The implementation of this service SHALL follow the specifications given in "The NATO Profile for the Use of S/MIME CMS and ESS" [NATOSMIMEProfile].

8. REFERENCES

[x400Wrap] Bonatti, C., Eggen, A., Hoffman, P., "Securing X.400 Content with S/MIME" IETF RFC 3854, July 2004.

[x400Transport] Bonatti, C., Hoffman, P., "Transporting S/MIME Objects in X.400", IETF RFC 3855, July 2004.

[NATOSMIMEProfile] "The NATO Profile for the Use of S/MIME CMS and ESS", AC/322(SC/4)AHWG/6 (AppSy), STANAG 4631.

[MUSTSHOULD] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP14, RFC 2119, March 1997.

[COMPRData] Gutmann, P., "Compressed Data Content Type for CMS", RFC 3274, June 2002.

[DOMSEC] Dean, T., Ottaway, W., "Domain Security Services Using S/MIME", IETF RFC 3183, October 2001.

ANNEX C

STANDARDIZED PROFILES AMH1N(D) – COMMON UNRESTRICTED MESSAGING

Standardized Profile

TITLE: Information technology – Standardized Profiles AMH1n(D) – Military Message Handling Systems – Common Unrestricted Messaging Part 1: MHS Service Support

This document forms part of a multipart Standardized Profile (SP) for Common Unrestricted Messaging for Military Message Handling Systems (MMHS). It is outside the scope of the current Taxonomy Framework for International Standardized Profiles (ISP). This SP is a delta to the Civilian MHS Common Messaging ISP 10611 and includes only the additional requirements for the MMHS. This document is content-type independent.

Introduction

This Standardized Profile (SP) is defined within the context of functional standardization, in accordance with the principles specified by ISO/IEC TR 10000, "Framework and Taxonomy of International Standardized Profiles". The context of functional standardization is one part of the overall field of Information Technology (IT) standardization activities – covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards to promote system interoperability and to provide a basis for the development of uniform, internationally recognized system tests.

One of the most important roles for a SP is to serve as the basis for the development of recognized tests. SPs also guide implementors in developing systems that fit the needs of the MMHS. SPs are produced not simply to 'legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other SPs is crucial to the successful realization of this goal.

This part of AMH1n(D) provides a functional description and specification of MMHS service support and associated functionality as covered by the AMH1n(D) set of profiles. It identifies what additional service support and functionality can be supported by each type of MHS component in a Military Messaging environment (i.e., covering the services supported by an MM-UA, plus any additional MTA and MM-MS aspects), divided into basic requirements and zero or more optional functional groups. Such specifications are in many cases applicable to more than one MHS protocol or are otherwise concerned with component functionality which although it can be verified via protocol, is not just related to protocol support. The specification of this part is therefore designed for reference by the following parts (which specify conformance requirements by protocol for each MHS component) and is additional to the protocol-specific requirements specified in those parts. Thus, although this part contains normative requirements, there is no separate conformance to this part (i.e., it is not identified in the MHS taxonomy) since such requirements are only significant when referenced in the context of a particular protocol profile.

This part of AMH1n(D) contains one normative appendix:

Appendix A Elements of Service for ACP 123

Information technology – Standardized Profiles AMH1n(D) – Military Message Handling Systems – Common Unrestricted Messaging

Part 1: MHS Service Support

1 Scope

1.1 General

This part of AMH1n(D) contains the overall specifications of the support of MHS Elements of Service and other aspects of MHS functionality which are specific to the Military Message Handling System (MMHS) which are generally not appropriate for consideration only from the perspective of a single MHS protocol. These specifications form part of the Common Unrestricted Messaging application functions, as defined in the parts of AMH1n(D), and are based on the Common Messaging content type-independent specifications in ISO/IEC ISP 10611. Such specifications are in many cases applicable to more than one MHS protocol or are otherwise concerned with component functionality which, although it can be verified via protocol, is not just related to protocol support. They are therefore designed to be referenced in the Common Unrestricted Messaging application profiles AMH1n(D) Part 2 (Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MMHS), AMH1n(D) Part 3 (AMH11(D)), AMH1n(D) Part 4 (AMH12(D)) and AMH1n(D) Part 5 (AMH13(D)), which specify the support of specific MHS protocols and associated functionality.

This SP makes use of the Common Messaging AMH1. It specifies the additional requirements needed to support the MMHS Common Unrestricted Messaging environment.

The specifications in this part of AMH1n(D) are divided into **basic requirements**, which are required to be supported by all MMHS implementations claiming conformance to this profile, and a number of optional **functional groups**, which cover significant discrete areas of related functionality which are not required to be supported by all implementations.

1.2 Position within the taxonomy

This part of AMH1n(D) is the first part, as common text, of a multipart SP for AMH1n(D) Military Message Handling Systems. The multipart SP consists of the following parts:

Part 1 – MHS Service Support

Part 2 – Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MMHS
Part 3 – AMH11(D) – MMHS Requirements for Message Transfer (P1)
Part 4 – AMH12(D) – MMHS Requirements for MTS Access (P3)
Part 5 – AMH13(D) – MMHS Requirements for MS Access (P7)

This part of AMH1n(D) does not, on its own, specify any profiles.

This SP must be combined with the multipart ISP identified in ISO/IEC TR 10000-2 as "AMH1, Message Handling Systems – Common Messaging" (see also ISO/IEC TR 10000-1, 8.2 for the definition of multipart ISPs).

The multipart AMH1 ISP consists of the following parts:

Part 1 – MHS Service Support
Part 2 – Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS
Part 3 – AMH11 – Message Transfer (P1)
Part 4 – AMH12 – MTS Access (P3)
Part 5 – AMH13 – MS Access (P7)

It may be combined with any approved T-Profiles (see ISO/IEC TR 10000) specifying the OSI connection-mode Transport service.

2 References

The following documents are additional documents referenced to those cited in ISO/IEC 10611-1.

The following documents contain provisions which, through reference in this text, constitute provisions of this part of AMH1n(D). At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of AMH1n(D) are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by SPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

Technical corrigenda to the base standards referenced are listed in appendix B of ISO/IEC 10611-1.

NOTE – References in the body of this part of AMH1n(D) to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

ACP 123(B): *Common Messaging Strategy and Procedures.*

ISO/IEC 10611-1: 1994, *Information technology – International Standardized Profiles – Message Handling Systems – Common Messaging – Part 1: MHS Service Support.*

ISO/IEC 10021-1:1990/Am.2, *Information technology – Message-Oriented Text Interchange System (MOTIS) – Part 1: System and Service Overview, Amendment 1 Message Store Extensions 1994.*

ISO/IEC 10021-2:1990/Am.1, *Information technology – Message-Oriented Text Interchange System (MOTIS) – Part 2: Overall Architecture; Amendment 1: Representation of O/R Addresses for Human Exchange 1994.*

ISO/IEC 10021-2:1990/Am.2, *Information technology – Message-Oriented Text Interchange System (MOTIS) – Part 2: Overall Architecture; Amendment 2: Minor Enhancements: Multinational Organizations and Terminal-form Addresses 1994.*

ISO/IEC 10021-4:1990/Am.1, *Information technology – Message-Oriented Text Interchange System* (MOTIS) *– Part 4: Message Transfer System: Abstract Service Definition and Procedures; Amendment 1: Minor Enhancements: Notification-type and Directory Substitution 1994.*

MHS Implementors' Guide, Version 11, July 1994 (ITU-T Special Rapporteur's Group on Message Handling Systems and ISO/IEC JTC1/SC18/WG4 SWG on Messaging).

(Application for copies of these documents should be addressed to the American National Standards Institute, 11 West 42nd Street, NY, NY 10036 or to ISO, Van Demonstrate 94, 1013 CN Amsterdam, Netherlands.)

3 Definitions

For the purposes of this part of AMH1n(D), the following definitions apply.

Terms used in this part of AMH1n(D) are as defined in the referenced base standards, and in ISO/IEC 10611-1.

3.3 Profile object identifiers

No additional requirements.

4 Abbreviations and Acronyms

ANNEX C TO ACP123(B)

The following are additional abbreviations and acronyms to those defined in ISO/IEC ISP 10611-1.

ACP	Allied Communication Publication
ACP127	ACP 127 Interworking
ACSE	Association Control Service Element
CCITT	International Telegraph and Telephone Consultative Committee
CSP	Common Security Protocol
DDA	Domain Defined Attributes
EMS	Express Mail Service
IEC	International Electrotechnical Commission
ISO	International Standards Organization
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
JTC1	Joint Technical Committee
MH	Message Handling
MM	Military Message
MM-	Military Messaging
MM-MS	Military Messaging Message Store
MM-UA	Military Messaging User Agent
MMHS	Military Message Handling System
MMS	Military Messaging Service
NATO	North Atlantic Treaty Organization
P1	MTS Transfer Protocol
P3	MTS Access Protocol
P7	MS Access Protocol
P772	MMS Protocol
PDS	Physical Delivery System
ROSE	Remote Operations Service Element
RTSE	Reliable Transfer Service Element
SC	Sub committee
S/MIME	Secure Multipurpose Internet Mail Extensions
SP	Standardized Profiles
SPICS	Standardized Profiles Implementation Conformance Statement
STANAG	Standardization Agreement
SWG	Special Working Group

Support level for Elements of Service (see 3.2):

m	mandatory support
o	optional support
c	conditional support
i	out of scope
-	not applicable

x prohibited

5 Conformance

No conformance requirements are specified in this part of AMH1n(D).

NOTE – This part of AMH1n(D) is a reference specification of the basic requirements and functional groups covered by the AMH1n(D) set of profiles and is additional to the protocol-specific requirements specified in the following parts of this SP. Although this part of AMH1n(D) contains normative requirements, there is no separate conformance to this part (i.e., it is not identified in the MHS taxonomy) since such requirements are only significant when referenced in the context of a particular protocol.

Conformance requirements are specified by protocol for each MHS component in the following parts of AMH1n(D) with reference to the specifications in this part. Support of the functionality as specified in this part may only be verifiable where the effect of implementation can be determined at a standardized external interface – i.e. via a standard OSI communications protocol. Further, the provision of Elements of Service and other functionality at a service interface will not necessarily be verifiable unless such interface is realized in the form of a standard OSI communications protocol. Other forms of exposed interface (such as a human user interface or a standardized API) may be provided, but are not required for conformance to this version of AMH1n(D).

6 Basic requirements

Appendix A specifies the basic requirements for support of MHS Elements of Service (EoS) for conformance to AMH1n(D) – i.e., the level of support required by all MMHS implementations, as appropriate to each type of MHS component – i.e., MTA, MM-MS or MM-UA (as MTS-user or MS-user, as relevant).

6.1 Content and encoded information types

It shall be stated in the ISPICS which content type and encoded information type values are supported.

6.2 Message Length

If the implementation imposes any constraints on the size of the message content or envelope, then all such constraints shall be stated in the ISPICS.

6.3 Number of Recipients

It shall be stated in the ISPICS if there is any limit on the number of recipients that can be specified in a message envelope.

7 Functional groups

Appendix A also specifies any additional requirements for support of MHS EoS if support of an optional functional group (FG) is claimed, as appropriate to each type of MHS component (i.e., MTA or MTS-user). The following clauses summarize the functionality supported by each of the optional FGs and identify any particular requirements or implementation considerations which are outside the scope of formal conformance to AMH1n(D). A summary of the functional groups, identifying which may be supported (Y) and which are not applicable (N) for each type of MHS component (i.e., MTA, MM-MS MM-UA – whether as MTS-user or as MS-user is not distinguished), is given in the following table.

Following the Y or N is an indication of the support classification (mandatory, optional, out of scope, or prohibited) for the functional group in the context of this profile.

The following clauses summarize the functionality supported by each of the optional FGs and specifies which FGs must be supported at the MTS level to support this SP.

Table 1 – Summary of AMH1n(D) optional functional groups

Functional Group	MTA	MS	MM-UA
Conversion (CV)	Y(o)	N	N[1]
Distribution List (DL)	Y(o)	N	N
Physical Delivery (PD)	Y(o)	N	Y(o)
Redirection (RED	Y(m)	N	N[1]
Latest Delivery (LD)	Y(m)	N	N
Return of Contents (RoC)	Y(x)	Y(x)	Y(x)
Security (SEC)	Y(o)	Y(o)	N
Use of Directory (DIR)	Y(m)	N	N
84 Interworking (84IW)	Y(o)	N	N[1]
ACP 127 Interworking (ACP127)	N	Y(o)	Y(o)

Note:

1 MM-UA Functionality may be further defined in content type-dependent profiles.

7.1 Conversion (CV)

The Conversion FG covers support of those EoS which provide the functionality required to perform the action of encoded information type conversion. Support of

the CV FG is applicable to an MTA. Support of the CV FG by an MTA covers support of the Explicit Conversion EoS only.

NOTE – Support of EoS associated with conversion prohibition is a basic MTA requirement, but this does not imply a capability to perform conversion.

An MTA implementation conforming to the CV FG shall conform to the Common Messaging CV FG as specified in ISO/IEC ISP 10611 in the MMHS (i.e., the ability to perform conversion of MM content is required).

7.2 Distribution List (DL)

Support for the Distribution List FG is optional in this SP.

An Implementation conforming to the DL FG shall conform to the Common Messaging DL FG as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA in the MMHS.

7.3 Physical Delivery (PD)

The Physical Delivery FG is concerned with access to physical delivery (i.e., postal, courier, etc) services. The PD FG comprises two separate and distinct parts:

support of PD EoS on origination and submission;
support of a collocated physical delivery access unit (PDAU).

Support of PD EoS on submission is applicable for either an MTA or a UA. Support of a PDAU is only applicable for an MTA.

An implementation conforming to the PD FG shall conform to the Common Messaging PD FG as specified in ISO/IEC ISP 10611. An MM-UA conforming to the PD FG shall also make the PD EoS available to the MMHS user for origination. There are no additional requirements for an MTA in the MMHS.

7.4 Redirection (RED)

Support for the Redirection FG is mandatory.

An implementation conforming to the RED FG shall conform to the Common Messaging RED FG as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA in the MMHS.

7.5 Latest Delivery (LD)

Support for Latest Delivery FG for an MTA is mandatory in this SP.

An implementation conforming to the LD FG shall conform to the Common Messaging LD FG as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA in the MMHS.

7.6 Return of Content (RoC)

Support for the Return of Content FG is prohibited for this SP.

7.7 Security (SEC)

Secure Multipurpose Internet Mail Extensions (S/MIME) will provide security for Messaging in the MMHS. Therefore support for any of the classes in the Security FG as defined in the Common Messaging SEC FG as specified in ISO/IEC ISP 10611 is optional in this SP.

For additional information about the Security classes and the Security FG see the Common Messaging ISP 10611-1 MHS Service Support.

7.8 Use of Directory (DIR)

Support for the Directory FG is mandatory in this SP.

An implementation conforming to the DIR FG shall conform to the Common Messaging DIR FG as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA in the MMHS.

7.9 84 Interworking (84IW)

Support for the 84 Interworking FG is optional in this SP.

An implementation conforming to the 84IW FG shall conform to the Common Messaging 84IW FG as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA in the MMHS.

7.10 ACP 127 Interworking (ACP127)

The ACP 127 Interworking FG covers interworking between implementations conforming to MMHS and the older messaging system following ACP 127 guidelines. Interworking takes place by way of a gateway doing conversion between the two formats. However, if this FG is supported, the MMHS implementation supports those optional services and protocol elements in P772 whose sole purpose is to provide interworking for ACP 127 messages during the transition.

This FG requires support on reception for these services including User Interface display requirements. These services even in the case of the FG will not be originated by the MM-UA but may instead be added at the gateway during conversion and information returned with the gateway notification response.

It is recommended that support for this FG be a configurable option, so it may be turned off when no longer required.

8 Naming and addressing

Support for numeric addresses and directory names is mandatory in addition to the naming and addressing capabilities as specified in clause 8 of ISO/IEC ISP 10611-1. In addition, implementations will support the Domain Defined Attributes (DDA) acp-plad and acp-ri for both origination and reception. (Support of these DDAs to identify the MM-UA itself is not required.)

9 Error and exception handling

An implementation claiming conformance to the error and exception handling shall do so as specified in ISO/IEC ISP 10611-1, clause 9.

10 Content Type support

MTAs shall support transfer of content types independent of the content type. An implementation claiming conformance to the this profile shall, at a minimum, support the transfer of the MM content type indicated by id-mmhs-content OBJECT IDENTIFIER ::= { iso(1) identified-organizations(3) nato(26) nato-standard(0) MMHS(4406) object-ids(0) content-type(4) mm88(1) }.

Appendix A

(normative)

ELEMENTS OF SERVICE FOR ACP 123

In the event of a discrepancy becoming apparent in the body of this part of AMH1n(D) and the tables in this appendix, this appendix is to take precedence. Only the additional EoS requirements to those defined in the Base (ISO/IEC 10611-1) and this SP are listed.

This appendix specifies the support constraints and characteristics of what shall or may appear in the implementation columns of a IO-ICS of ACP 123. This appendix is broadly based on the current version of ISO/IEC ISP for AMH1.

In each table, the "Basic" column reflects the level of support required for conformance to AMH1n(D)- i.e. the minimum level of support required by all MTA, MM-MS, and MM-UA implementations supporting this profile (see clause 6). The "Functional Group" column specifies any additional support requirements if support of an optional functional group is claimed (see clause 7). Each column is then further subdivided into support for origination ("Orig") and reception ("Rec".) as defined in clause 3.2, together with the abbreviated name of the functional group ("FG") in the case of the second column. The origination and reception columns are further subdivided to distinguish the support required for an MTA from that for an MTS-user (the latter refers only to the use of MT services, not whether such services are made available to the MHS user, and may be further qualified in a content type-dependent profile.

A.1 MT Elements of Service

Table A.1 – Elements of Service Belonging to The Basic MT Service

Elements of Service	Basic					Functional Group					
	Orig.		Proc.	Rec.		FG	Orig.		Proc.	Rec.	
	MTS-user	MTA		MTA	MTS-user		MTS-user	MTA		MTA	MTS-user
Content Type Indication[2]											

Notes:

2 At a minimum, an implementation must support the content type for MM (P772) which is identified by id-mmhs-content OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) nato(26) nato-standard(0) MMHS(4406) object-ids(0) content-type(4) mm88(1) }

Table A.2 – MT Service Optional User Facilities

Elements of Service	Basic					Functional Group					
	Orig.		Proc.	Rec.		FG	Orig.		Proc.	Rec.	
	MTS-user	MTA		MTA	MTS-user		MTS-user	MTA		MTA	MTS-user
Alternate Recipient Allowed	m	m	m	m							
Alternate Recipient Assignment			m								
Content Confidentiality[14]											
Content Integrity[14]											
Conversion Prohibition in Case of loss of Information											
Deferred Delivery[21]											
Deferred Delivery Cancellation[21]	c[17]										
Designation of Recipient by Directory Name[18]	m	m	m								
DL Expansion History Indication					m						
Explicit Conversion						CV	m				
Hold for Delivery					c[15]						
Latest Delivery Designation	m	m	m								
Message Origin Authentication[14]											
Message Security Labelling[14]											
Message Sequence Integrity[19]											
Non-repudiation of Delivery[14]											
Non-repudiation of Origin[14]											
Non-repudiation of Submission[14]											
Originator Requested Alternate Recipient	m	m	m								
Prevention of Non-delivery Notification	m[20]										
Probe[16]	ix	x	x[23]								
Probe Origin Authentication[14]											
Proof of Delivery[14]											
Proof of Submission[14]											
Redirection Disallowed by Originator	m	m	m								
Redirection of Incoming Messages			m	m	m						
Report Origin											

Table A.2 – MT Service Optional User Facilities

Elements of Service	Basic					Functional Group					
	Orig.		Proc.	Rec.		FG	Orig.		Proc.	Rec.	
	MTS-user	MTA		MTA	MTS-user		MTS-user	MTA		MTA	MTS-user
Authentication[14]											
Return of Content	ix[22]	x	x								
Secure Access Management	m	m	m	m	m						

Notes:

14 Support is according to the security class for which support is claimed – see clause A.1 of ISO/IEC ISP 10611-1. S/MIME will provide the basic security for the MMHS. Therefore support for any of the classes in the Security FG is optional in this SP. Therefore the SEC FG requirements are not enumerated in this table.

15 Support of the Hold for Delivery EoS is mandatory when using the P3 protocol. Implementation is a local matter in the case of a collocated MTS-user and may be dependent on local policy.

16 Although support for Probes is required for MTAs in the base X.400 standard, it is recommended that support by MTS-users is not required. This profile further makes Probes dynamically prohibited.

17 If Deferred Delivery is supported, Deferred Delivery cancellation must also be supported.

18 Origination of the Designation of Recipient by Directory Name EoS implies (for those recipients who have been assigned Directory Names in a Directory Service supported by the originating management domain) that the Directory Name may be specified for recipients. Reception of this service implies display (to the user) of any Directory Names contained in the message.

19 Not part of SEC FG because it requires bilateral agreement to work.

20 The ability to request this service on a particular message may be dependent on the precedence requested.

21 Messages should be held in the originating MTA to provide support for Deferred Delivery and Deferred Delivery Cancellation.

22 Prohibition of this EoS means that bit 3 of the *per-message-indicators* envelope field shall be cleared (zero) and that bit 2 of the *notification-requests* heading field shall be cleared. It implies that the *returned-mm* notification field shall never be originated.

23 Reception of Probe at the MTA will be logged as a security violation and no delivery or non-delivery report will be returned.

Table A.3 – Elements of Service Belonging to The Base MH/PD Service Intercommunication

Elements of Service	Basic					Functional Group					
	Orig.		Proc.	Rec.		FG	Orig.		Proc.	Rec.	
	MTS-user	MTA		MTA	PDAU		MTS-user	MTA		MTA	PDAU
Basic Physical Rendition					-						
Ordinary Mail					-						
Physical Forwarding Allowed					-						
Undeliverable Mail					-						

Table A.3 – Elements of Service Belonging to The Base MH/PD Service Intercommunication

Elements of Service	Basic					Functional Group					
	Orig.		Proc.	Rec.		FG	Orig.		Proc.	Rec.	
	MTS-user	MTA		MTA	PDAU		MTS-user	MTA		MTA	PDAU
with Return of Physical Message											
Additional Physical Rendition					-						
Counter Collection					-						
Counter Collection with Advice					-						
Delivery via Bureaufax Service					-						
EMS (Express Mail Service)					-	PD	m				
Physical Delivery Notification by MHS					-						
Physical Deliery Notification by PDS					-						
Physical Forwarding Prohibited					-						
Registered Mail					-						
Registered Mail to Addressee in Person					-						
Request for Forwarding Address					-						
Special Delivery					-	PD	m				

Table A.5 – Security Services

No additional requirements.

A.2 MS Elements of Service

A Message Store is optional in the MMHS profiles, however, if one is implemented the following Elements of Service apply.

The following tables specify additional requirements for support of MS EoS by an MM-MS and the requirements for use of such services by an MS-user in the MMHS (i.e., an MM-UA) for conformance to AMH1n(D).

In the following tables, the "Profile" column reflects the basic requirements for conformance to AMH1n(D) – i.e., the minimum level of support required by all MM-UA and MM-MS implementations conforming to this profile (see clause 6). The "Functional Group" column specifies any additional support requirements if support of an optional functional group is claimed (see clause 7), together with the abbreviated name of the functional group ("FG").

Table A.6 – Base Message Store

Elements of Service	Profile		Functional Group		
	UA	MS	FG	UA	MS
MS Register	m				
Stored Message Listing	m				
Stored Message Summary	m				

Table A.7 – MS Optional User Facilities

Elements of Service	Profile		Functional Group		
	UA	MS	FG	UA	MS
Stored Message Alert	m	m			
Stored Message Auto-forward	m	m			

A.3 Additional Information

A.3.1 MT Elements of Service support

The tables in ACP 123, annex B, appendix A, clause A.8.1.2 and A.8.1.3, shall be completed to indicate, for each MT Element of Service, whether it is available to the MHS user and, if so, how this is achieved. For each EoS for which support is claimed, the implementor will check the column which indicates how the EoS is supported in a given instance. If appropriate the Comments column can be filled in to provide additional information as to how the EoS is selected.

ACP 123 goes beyond X.400 by stating which MT Elements of Service are to be supported as user options and which have requirements for display at the user interface. If support for these are claimed, the EoS must be selectable at the user interface for a given message. These requirements are indicated with the following codes in the Profile column in the following table:

s the user must be able to select the service and its associated information on origination

D this information must be displayed to the user, if it is present

Table A.8 – MT Elements of Service support

Ref	Element of Service	Profile

Table A.8 – MT Elements of Service support

Ref	Element of Service	Profile
1	Access Management	
2	Alternate Recipient Allowed	s
3	Alternate Recipient Assignment	
4	Content Confidentiality	
5	Content Integrity	
6	Content Type Indication	
7	Conversion Prohibition	s
8	Conversion Prohibition in Case of Loss of Information	s[1]
9	Converted Indication	D
10	Deferred Delivery	s
11	Deferred Delivery Cancellation	s
12	Delivery Notification	D
13	Delivery Time Stamp Indication	D
14	Designation of Recipient by Directory Name	sD
15	Disclosure of Other Recipients	
16	DL Expansion History Indication	D
17	DL Expansion Prohibitied	s
18	Explicit Conversion	s
19	Grade of Delivery Selection	
20	Hold for Delivery	
21	Implicit Conversion	
22	Latest Delivery Designation	s
23	Message Flow Confidentiality	
24	Message Identification	
25	Message Origin Authentication	
26	Message Security Labelling	D[2]
27	Message Sequence Integrity	
28	Multi-Destination Delivery	s
29	Non-delivery Notification	sD
30	Non-repudiation of Delivery	
31	Non-repudiation of Origin	
32	Non-repudiation of Submission	
33	Original Encoded Information Types Indication	
34	Originator Requested Alternate Recipient	sD
35	Prevention of Non-delivery Notification	s
36	Probe	
37	Probe Origin Authentication	
38	Proof of Delivery	
39	Proof of Submission	
40	Redirection Disallowed by Originator	s

Table A.8 – MT Elements of Service support

Ref	Element of Service	Profile
41	Redirection of Incoming Messages	s
42	Report Origin Authentication	
43	Requested Preferred Delivery Method	
44	Restricted Delivery	
45	Return of Content	
46	Secure Access Management	
47	Submission Time Stamp Indication	**D**
48	Use of Distribution List	**s**
49	User/UA Capabilities Registration	

Notes:

1 If Explicit Conversion is supported the user shall have the ability to select this service.

2 Note that this is the X.400 provided service rather than any nationally defined security mechanism. This classification is not intended to imply any requirement to originate or understand the semantics of this security label.

Table A.9 – MH/PD Elements of Service support

Ref	Element of Service	Profile
1	Additional Physical Rendition	
2	Basic Physical Rendition	
3	Counter Collection	
4	Counter Collection with Advice	
5	Delivery via Bureaufax Service	
6	EMS (Express Mail Service)	
7	Ordinary Mail	
8	Physical Delivery Notification by MHS	
9	Physical Delivery Notification by PDS	
10	Physical Forwarding Allowed	
11	Physical Forwarding Prohibited	
12	Registered Mail	
13	Registered Mail to Addresses in Person	
14	Request for Forwarding Address	
15	Special Delivery	
16	Undeliverable Mail with Return of Physical Message	

A.3.2 MS Elements of Service support

The table in ACP 123, annex B, appendix A, clause A.8.1.4, shall be completed to indicate, for each MS Element of Service, whether it is available to the MHS user and, if so, how this is achieved. For each EoS for which support is claimed, the implementor will check the column which indicates how the EoS is supported in a given instance. If appropriate the Comments column can be filled in to provide additional information as to how the EoS is selected.

ACP 123 goes beyond X.400 by stating which MS Elements of Service are to be supported as user options and which have requirements for display at the user interface. If support for these are claimed, the EoS must be selectable at the user interface for a given message. These requirements are indicated with the following codes in the Profile column in the following table:

s the user must be able to select the service and its associated information on origination

D this information must be displayed to the user, if it is present

Table A.10 – MS Elements of Service support

Ref	Element of Service	Profile
1	MS Register	
2	Stored Message Alert	s
3	Stored Message Auto-forward	s
4	Stored Message Deletion	s
5	Stored Message Fetching	s
6	Stored Message Listing	s
7	Stored Message Summary	s

Standardized Profile

TITLE: Information technology Standardized Profiles AMH1n(D) – Military Message Handling Systems – Common Unrestricted Messaging – Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MMHS

This document forms part of a multipart Standardized Profile (SP) for Common Unrestricted Messaging for Military Message Handling Systems (MMHS). It is outside the scope of the current Taxonomy Framework for International Standardized Profiles (ISP). This SP is a delta to the Civilian MHS Common Messaging ISP 10611 and includes only the additional requirements for the MMHS. This document is content-type independent.

Introduction

This Standardized Profile (SP) is defined within the context of functional standardization, in accordance with the principles specified by ISO/IEC TR 10000, "Framework and Taxonomy of International Standardized Profiles". The context of functional standardization is one part of the overall field of Information Technology (IT) standardization activities – covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards to promote system interoperability and to provide a basis for the development of uniform, internationally recognized system tests.

One of the most important roles for a SP is to serve as the basis for the development of recognized tests. SPs also guide implementors in developing systems that fit the needs of the MMHS. SPs are produced not simply to 'legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other SPs is crucial to the successful realization of this goal.

This part of AMH1n(D) specifies how the Remote Operations Service Element, the Reliable Transfer Service Element, the Association Control Service Element, the Presentation Layer, and the Session Layer standards shall be used to provide the required OSI upper layer functions for MMHS. The text for this SP is based on ISO/IEC ISP 10611.

This part of AMH1n(D) contains three normative appendices:

Appendix A SPICS Requirements List - Specific Upper Layer Requirements for ACSE, Presentation and Session

Appendix B SPICS Requirements List for RTSE

Appendix C SPICS Requirements List for ROSE

Information technology – Standardized Profiles AMH1n(D) – Military Message Handling Systems – Common Unrestricted Messaging

Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MMHS

1 Scope

1.1 General

This part of AMH1n(D) specifies how the Remote Operations Service Element (ROSE), the Reliable Transfer Service Element (RTSE), the Association Control Service Element (ACSE), the Presentation Layer, and the Session Layer standards shall be used to provide the required OSI upper layer functions for MMHS (See also figure 1). These specifications are therefore the common basis for the MMHS application functions, as defined in the other parts of AMH1n(D), and for content type-dependent SPs for MHS that will be developed.

1.2 Position within the taxonomy

This part of AMH1n(D) is the second part of a multipart SP for AMH1n(D) Military Message Handling Systems – Common Unrestricted Messaging.

This part of AMH1n(D) does not, on its own, specify any profiles.

1.3 Scenario

The model used is one of two end systems running an end-to-end association using either or both of RTSE and ROSE, and the ACSE, Presentation and Session services and protocols (see figure 1).

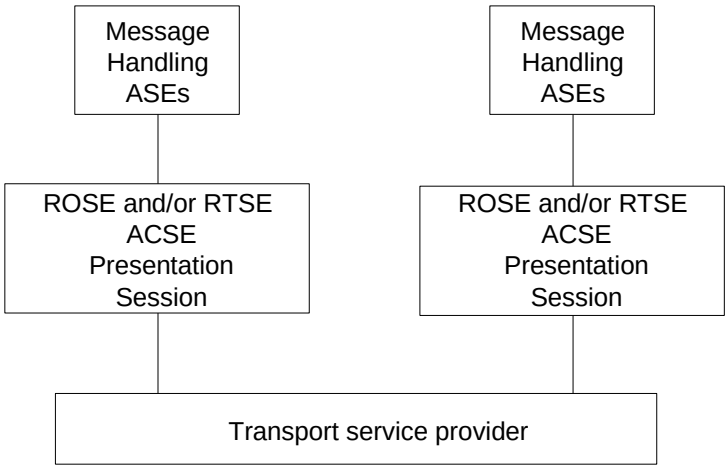


Figure 1 – Model of the supportive layers

The OSI upper layer services and protocols to support the Message Handling Systems functions covered by the AMH1n(D) set of profiles are specified in the set of standards identified in table 1.

Table 1 – AMH1n(D) profile model

Application Layer	MHS	ISO /IEC 10021-6
	ROSE	ISO/IEC 9072-2
	RTSE	ISO/IEC 9066-2
	ACSE	see ISO/IEC ISP 11188-1
Presentation Layer		see ISO/IEC ISP 11188-1
Session Layer		see ISO/IEC ISP 11188-1

2 Normative references

The following documents are additional documents referenced to those cited in ISO/IEC 10611-1.

The following documents contain provisions that, through reference in this text, constitute provisions of this part of AMH1n(D). At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of AMH1n(D) are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by SPs to such documents is that they may be specific to a particular

edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

Amendments and corrigenda to the base standards referenced are listed in annex D of ISO/IEC ISP 11188-1.

NOTE – References in the body of this part of AMH1n(D) to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations, as noted below, unless otherwise stated.

ACP 123(B): *Common Messaging Strategy and Procedures.*

ISO/IEC ISP 10611-2: 1994, *Information technology – International Standardized Profiles – Messaging Handling Systems – Common Messaging – Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MMHS.*

(Application for copies of these documents should be addressed to the American National Standards Institute, 11 West 42nd Street, NY, NY 10036 or to ISO, Van Demonstrate 94, 1013 CN Amsterdam, Netherlands.)

3 Definitions

To specify the support level of arguments, results and other protocol features for this part of AMH1n(D), the following terminology is defined.

The specification of levels of support uses the classification defined in ISO/IEC ISP 10611-2.

4 Abbreviations

The following are additional abbreviations to those defined in ISO/IEC ISP 10611-2.

AARE	A-associate-response
AARQ	A-associate-request
ACP	Allied Communications Publications
CCITT	International Telegraph and Telephone Consultative Committee
IEC	International Electrotechnical Commission
ISO	International Standards Organization
MHS	Message Handling System
MMHS	Military Message Handling System
OSI	Open Systems Interconnection
SP	Standardized Profiles
SPICS	Standardized Profiles Implementation Conformance Statement

Support level for protocol features (see clause 4.2 of ISO/IEC ISP 11188-1):

m mandatory support

5 Conformance

This part of AMH1n(D) states requirements upon implementations to achieve interworking. A claim of conformance to this part of AMH1n(D) is a claim that all requirements in the relevant base standards are satisfied, that all the requirements in ISO/IEC ISP 11188-1 are satisfied, and that all requirements in the following clauses and in the appendices of this part of AMH1n(D) are satisfied. Appendices A, B and C state the relationship between these requirements and those of the base standards.

5.1 Conformance statement

The subsequent parts of AMH1n(D) specify the requirements for support of particular MHS application contexts. The requirements for conformance to this part of AMH1n(D) are, as appropriate to the MHS application context(s) for which support is claimed, in accordance with ISO/IEC 10021-6.

For each implementation claiming conformance to this part of AMH1n(D), an appropriate set of ISPICS shall be made available stating support or non-support of each option identified in this part of AMH1n(D). The ISPICS Proforma in ISO/IEC 10611-2 shall be used to generate the ISPICS.

5.2 Relationship with base standards

5.2.1 ROSE conformance

No additional requirements.

5.2.2 RTSE conformance

Implementations claiming support of any MMHS application context which includes the Reliable Transfer Service Element (RTSE) shall implement normal mode. RTSE is only required for reliable application contexts (i.e., mts-reliable-access, mts-forced-reliable-access, and ms-reliable-access). Implementation of X.410-1984 mode is optional. All mandatory

support (m) features (as specified in clause 7) shall also be implemented unless those features are part of an unimplemented optional feature. They shall state which optional support (o) features are implemented.

5.2.3 ACSE conformance

To conform to the Association Control Service Element (ACSE) protocol used in this part of AMH1n(D), implementations shall implement Normal mode. Implementation of X.410-1984 mode is optional. All mandatory support (m) features (as specified in clause 8) shall also be implemented unless those features are part of an unimplemented optional feature. They shall state which optional support (o) features are implemented.

5.2.4 Presentation layer conformance

To conform to the Presentation protocol used in this part of AMH1n(D), implementations shall implement normal mode. Implementation of X.410-1984 mode is optional. All mandatory support (m) features (as specified in clause 9) shall also be implemented unless those features are part of an unimplemented optional feature. They shall state which optional support (o) features are implemented.

5.2.5 Transfer syntax conformance

No additional requirements.

5.2.6 Session layer conformance

No additional requirements.

6 Remote Operations Service Element (ROSE)

No additional requirements.

7 Reliable Transfer Service Element (RTSE)

No additional requirements.

7.1 Dialogue-mode

Two-way alternate dialogue-mode shall be supported for any P1 application context.

7.2 Checkpointing

No additional requirements.

7.3 Mode

Normal mode must be supported because the P1 mts-transfer application context is mandated in AMH1n(D) Part 3.

7.4 Elements of procedure

It is recommended that the RTSE association recovery procedure (clause 7.8.3 of ISO/IEC 9066-2) should not be used in a secure messaging environment, since the authentication of the RTSE association may be compromised (this is currently the subject of an RTSE defect report). It is permissible, however, to use the RTSE activity resumption procedure (clause 7.8.1 of ISO/IEC 9066-2) on an existing, authenticated, RTSE association.

8 Association Control Service Element (ACSE)

No additional requirements.

9 Presentation layer

No additional requirements.

10 Session layer

No additional requirements.

10.1 Session version

Session version 2 must be supported because the P1 mts-transfer application context is mandated in AMH1n(D) part 3.

Appendix A

(normative)

SPICS Requirements List

Specific Upper Layer Requirements for ACSE,

Presentation and Session

A.1 General

In the event of a discrepancy becoming apparent in the body of this part of AMH1n(D) and the tables in this appendix, this appendix is to take precedence.

The tables of this appendix specify the level of support for the Session, Presentation and ACSE protocols, as required by the Standardized Profiles AMH1n(D). Where features of these protocols are not specified in the tables of this appendix then the requirements for conformance to this part of AMH1n(D) are as specified in the corresponding annex of ISO/IEC ISP 10611-2. Any elements which are marked as * (i.e., referencing SP's choice) in the corresponding annex of ISO/IEC ISP 10611 and which are not resolved in this appendix ae to be considered as for the purposes of conformance to this part of AMH1n(D).

A.2 Classification of requirements

The "Profile" column reflects the level of support required by this SP. The specification of levels of support uses the classification defined in ISO/IEC ISP 10611-2.

A.3 Association Control Service Element

A.3.1 Supported roles

A.3.1.1 Association establishment

No additional requirements.

A.3.2 Protocol mechanisms

Ref	Protocol Mechanism	Profile
1	Normal mode	m
4	Supports operation of Session v2	m

A.3.3 Supported APDU parameters

No Additional requirements.

A.4 Presentation protocol

No additional requirements.

A.5 Session protocol

A.5.1 Protocol versions implemented

Ref	Version	Profile
2	Version 2	m

A.5.2 Functional units

No additional requirements.

A.5.3 Protocol mechanisms

No additional requirements.

Appendix B

(normative)

SPICS Requirements List for RTSE

B.1 General

In the event of a discrepancy becoming apparent in the body of this part of AMH1n(D) and the tables in this appendix, this appendix is to take precedence.

The tables of this appendix specify the level of support for the RTSE protocol, as required by the Defense Standardized Profiles AMH1n(D). This appendix is completely based on ISO/IEC ISP 10611. It uses only a selection of the tables from that Profile which are necessary for the specification of SP requirements. Where features of this protocol are not specified in the tables of this appendix then the requirements for conformance to this part of AMH1n(D) are as specified in ISO/IEC ISP 10611-2.

In each table, the "Base" column reflects the level of support required for conformance to the base standard and the "Profile" column reflects the level of support required by this SP. The specification of levels of support uses the classification defined in ISO/IEC ISP 10611-2.

B.2 Initiator/responder capability

No additional requirements.

B.3 Major capabilities

B.3.1 Protocol Mechanisms

Ref	Protocol Mechanism	Profile
1	Normal mode	m

B.3.2 Dialogue mode

No additional requirements.

B.4 Additional Information

No additional requirements.

Appendix C

(normative)

SPICS Requirements List for ROSE

C.1 General

No additional requirements.

C.2 Application entity requirements

No additional requirements.

Standardized Profile

TITLE: Information technology – Standardized Profiles AMH1n(D) – Military Message Handling Systems – Common Unrestricted Messaging Part 3: AMH11(D) – MMHS Requirements for Message Transfer (P1)

This document forms part of a multipart Standardized Profile (SP) for Common Unrestricted Messaging for Military Message Handling Systems (MMHS). It is outside the scope of the current Taxonomy Framework for International Standardized Profiles (ISP). This SP is a delta to the Civilian MHS Common Messaging ISP 10611 and includes only the additional requirements for the MMHS. This document is content-type independent.

Introduction

This Standardized Profile (SP) is defined within the context of functional standardization, in accordance with the principles specified by ISO/IEC TR 10000, "Framework and Taxonomy of International Standardized Profiles". The context of functional standardization is one part of the overall field of Information Technology (IT) standardization activities – covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards to promote system interoperability and to provide a basis for the development of uniform, internationally recognized system tests.

One of the most important roles for a SP is to serve as the basis for the development of recognized tests. SPs also guide implementors in developing systems that fit the needs of the MMHS. SPs are produced not simply to 'legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other SPs is crucial to the successful realization of this goal.

This part of AMH1n(D) covers MMHS requirements for Message Transfer (P1). It specifies any additional P1 support to that specified in ISO/IEC ISP 10611 and defines conformance requirements for an MTA which supports transfer with respect to support of P1 and associated functionality (requiring conformance to AMH11 and by reference to the common MMHS specifications in part 1).

This part of AMH1n(D) contains one normative appendix.

> Appendix A (normative) SPICS Requirements List for AMH1n(D) Part 3 (AMH11(D))

Information technology – Standardized Profiles AMH1n(D) – Military Message Handling Systems – Common Unrestricted Messaging

Part 3: AMH11(D) – MMHS Requirements for Message Transfer (P1)

1 Scope

1.1 General

This part of AMH1n(D) covers message transfer between Message Transfer Agents (MTAs) in the MMHS using the P1 Message Transfer Protocol (see also figure 1). These specifications form part of the Common Unrestricted Messaging application functions, as defined in the parts of AMH1n(D), and are based on the Common Messaging content type-independent specifications in ISO/IEC ISP 10611-3.

1.2 Position within the taxonomy

This part of AMH1n(D) is the third part of a multipart SP for AMH1n(D) Military Message Handling Systems.

This part of AMH1n(D) specifies the following profile:

AMH11(D) – MMHS Requirements for Message Transfer (P1)

This SP must be combined with the multipart ISP identified in ISO/IEC TR 10000-2 as "AMH1, Message Handling Systems – Common Messaging" (see also ISO/IEC TR 10000-1, 8.2 for the definition of multipart ISPs).

It may be combined with any approved T-Profiles (see ISO/IEC TR 10000) OSI connection-mode Transport service.

1.3 Scenario

The model used is one of two or more MTAs intercommunicating within a Message Transfer System (MTS) using the P1 protocol, as shown in figure 1.

Figure 1 – AMH11(D)scenario

The AMH11(D) profile covers all aspects of the MTA Abstract Service, as defined in clause 12 of ISO/IEC 10021-4 when realized using the P1 protocol in the MMHS.

2 References

The following documents are additional documents referenced to those cited in ISO/IEC 10611-1.

The following documents contain provisions which, through reference in this text, constitute provisions of this part of AMH1n(D). At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of AMH1n(D) are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by SPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

Technical corrigenda to the base standards referenced are listed in appendix B of ISO/IEC ISP 10611-3.

NOTE – References in the body of this part of AMH1n(D) to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

ACP 123(B): *Common Messaging Strategy and Procedures.*

ISO/IEC ISP 10611-3: 1994, *Information technology – International Standardized Profiles – Message Handling Systems – Common Messaging – Part 3: AMH11 – Message Transfer (P1).*

ISO/IEC 10021-1:1990/Am.2, *Information technology – Message-Oriented Text Interchange System (MOTIS) – Part 1: System and Service Overview, Amendment 1 Message Store Extensions 1994.*

ISO/IEC 10021-2:1990/Am.1, *Information technology – Message-Oriented Text Interchange System (MOTIS) – Part 2: Overall Architecture; Amendment 1: Representation of O/R Addresses for Human Exchange 1994.*

ISO/IEC 10021-2:1990/Am.2, *Information technology – Message-Oriented Test Interchange System (MOTIS) – Part 2: Overall Architecture; Amendment 2: Minor Enhancements: Multinational Organizations and Terminal-form Addresses 1994.*

ISO/IEC 10021-4:1990/Am.1, *Information technology – Message-Oriented Text Interchange System (MOTIS) – Part 4: Message Transfer System: Abstract Service Definition and Procedures; Amendment 1: Minor Enhancements: Notification-type and Directory Substitution 1994.*

MHS Implementors' Guide, Version 11, July 1994 (ITU-T Special Rapporteur's Group on Message Handling Systems and ISO/IEC JTC1/SC18/WG4 SWG on Messaging).

(Application for copies of these documents should be addressed to the American National Standards Institute, 11 West 42nd Street, NY, NY 10036 or to ISO, Van Demonstrate 94, 1013 CN Amsterdam, Netherlands.)

3 Definitions

For the purposes of this part of AMH1n(D), the following definitions apply.

Terms used in this part of AMH1n(D) are as defined in the referenced base standards, in addition, the terms defined in ISO/IEC 10611-3 apply.

4 Abbreviations and Acronyms

The following are additional abbreviations to those defined in ISO/IEC ISP 10611-3.

ACP	Allied Communication Publication
AIG	Address Indicator Group
CAD	Collective Address Designator
CCITT	International Telegraph and Telephone Consultative Committee
CSP	Common Security Protocol
IEC	International Electrotechnical Commission
ISO	International Standards Organization
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
JTC1	Joint Technical Committee
MM	Military Message
MMHS	Military Message Handling System
MMS	Military Messaging Service
MTS	Message Transfer System
MTSE	Message Transfer Service Element
P1	MTS Transfer Protocol
P772	MMS Protocol
PICS	Protocol Implementation Conformance Statement
PLAD	Plain Language Address Designator
RI	Routing Indicator

RTSE	Remote Transfer Service Element
SC	Subcommittee
SEC	Security
SMA	Signal Message Address
S/MIME	Secure Multipurpose Internet Mail Extensions
SP	Standardized Profiles
SPICS	Standardized Profiles Implementation Conformance Statement
SWG	Special Working Group
WG	Working Group

Support level for protocol elements and features (see 3.2):

m	mandatory full support
m-	mandatory minimal support
o	optional
r	required, dynamically mandatory
x	prohibited

5 Conformance

This part of AMH1n(D) states requirements upon implementations to achieve interworking. A claim of conformance to this part of AMH1n(D) is a claim that all requirements in the relevant base standards are satisfied, and that all requirements in the following clauses and in appendix A of this part of AMH1n(D) are satisfied. Appendix A states the relationship between these requirements and those of the base standards.

5.1 Conformance statement

For each implementation claiming conformance to profile AMH11(D), an ISPICS shall be made available stating support or non-support of each option identified in this part of AMH1n(D). The ISPICS Proforma in ISO/IEC 10611-5 shall be used to generate the ISPICS.

The scope of conformance to profile AMH11(D) is restricted to MTAs. A claim of conformance to AMH11(D) shall support profile AMH111. Support of the profile AMH112 is optional. Profiles AMH111 and AMH112, as obtained in ISO/IEC ISP 10611-3, are jointly referenced as AMH11 in this part of AMH1n(D) except where distinction is necessary.

5.2 MHS conformance

This part of AMH1n(D) specifies implementation options or selections such that conformant implementations will satisfy the conformance requirements of ISO/IEC 10021 and/or the CCITT X.400 Recommendations.

Implementations conforming to profile AMH11(D) shall as a minimum conform to the basic requirements of profile AMH11, as specified in ISP/IEC ISP 10611-3.

Implementations conforming to profile AMH11(D) shall additionally implement all the mandatory support (m) features identified as basic requirements in appendix A. They shall also support corresponding MHS Elements of Service and associated procedures as specified in AMH1n(D) Part 1, as appropriate to the scope of this profile.

Implementations conforming to profile AMH11(D) shall state whether or not they support any of the optional functional groups as specified in AMH1n(D) Part 1 which are applicable to the scope of this profile. For each functional group for which support is claimed, an implementation shall additionally implement all the mandatory support features (m) identified or that functional group in appendix A. They shall also support corresponding MHS Elements of Service and associated procedures as specified in AMH1n(D) Part 1, as appropriate to the scope of this profile.

Implementations conforming to profile AMH11(D) shall state the P1 application context(s) for which conformance is claimed.

5.3 Underlying layers conformance

Implementations conforming to profile AMH11(D) shall also meet the requirements for support of underlying layers as specified in subclause 5.3 of ISO/IEC ISP 10611-3.

Appendix A

(normative)

SPICS REQUIREMENTS LIST FOR

AMH1n(D) Part 3 (AMH11(D))

In the event of a discrepancy becoming apparent in the body of this part of AMH1n(D) and the tables in this appendix, this appendix is to take precedence.

This appendix specifies the support constraints and characteristics of AMH1n(D) Part 3 on what shall or may appear in the implementation columns of a ISPICS. Such requirements are additional to those specified in annex A of ISO/IEC 10611-3 (reference numbers correspond to items in that annex).

Clause A.1 specifies the basic requirements for conformance to profile AMH11(D). Clause A.2 specifies additional requirements to those specified in A.1 for each of the optional functional groups if conformance to such a functional group is claimed.

In each table, the "Profile" column reflects the level of support required for conformance to this SP (using the classification and notation defined in clause 3.2). The supplier of an implementation for which conformance to profile AMH11(D) is claimed should complete the Support column of the tables in annex A of ISO/IEC ISP 10611-3 in accordance with the requirements contained therein together with any additional requirements in this appendix.

A.1 Basic requirements

The following are additional requirements beyond those stated in ISO/IEC 10611-3.

A.1.1 Initiator/responder capability

No additional requirements.

A.1.2 Supported application contexts

Conformance to AMH111 is mandatory.

A.1.3 Supported operations

A.1.3.2Message Transfer Service Element (MTSE)

Ref	Operation	Profile

Ref	Operation	Profile
3	Probe Transfer	x[1]

Note:

1 Reception of a Probe at the MTA will be logged as a security violation and no delivery or non-delivery report will be returned.

A.1.4 Operation arguments/results

A.1.4.2Message Transfer

Ref	Element	Profile
1.1.4	content-type	m
1.1.6	priority	mr
1.1.11.4	latest-delivery-time	m
1.2.5.1	originator-requested-alternate-recipient	m
1.2.5.13	redirection-history	m

A.1.5 Common data types

Ref	Element	Profile
6.1.2.4.3	other-actions	m
6.1.2.4.3.1	redirected	m

A.1.6 Extension data types

Ref	Element	Profile
5.3.4.3	other-actions	m
5.3.4.3.1	redirected	m

A.1.7 O/R names

Ref	Element	Profile
1	mnemonic O/R Address	m
2	numeric O/R Address	m
6	directory-name	m

A.1.7.1 Mnemonic O/R address

Ref	Element	Profile
2	built-in-domain-defined-attributes	m
2.1	acp-plad[1]	m-

Ref	Element	Profile
2.2	acp-ri[2]	m-

Notes:

1 This element can be any acp-address including, but not limited to, PLADs, SMAs, AIGs, and CADs.

2 This element can be any RI, including collective RIs.

A.1.7.2Numeric O/R address

Ref	Element	Profile
2	built-in-domain-defined-attributes	m
2.1	acp-plad[1]	m-
2.2	acp-ri[2]	m-

Notes:

1 This element can be any acp-address including, but not limited to, PLADs, SMAs, AIGs, and CADs.

2 This element can be any RI, including collective RIs.

A.1.7.3Terminal O/R address

Ref	Element	Profile
2	built-in-domain-defined-attributes	m
2.1	acp-plad[1]	m-
2.2	acp-ri[2]	m-

Notes:

1 This element can be any acp-address including, but not limited to, PLADs, SMAs, AIGs, and CADs.

2 This element can be any RI, including collective RIs.

A.2 Functional groups

A.2.1 Mandatory functional groups

The following functional groups that are optional in ISO/IEC 10611-3, are mandatory in this profile as specified in this part of AMH1n(D):

Redirection (RED)
Latest Delivery (LD)
Use of Directory (DIR)

There are no additional requirements to those specified for support of these functional groups.

A.2.2 Optional functional groups

The following requirements are additional to those specified in A.1 if support of the optional functional group is claimed.

The Security (SEC), Physical Delivery (PD), Conversion (CV), and Distribution List (DL) FGs may optionally be implemented in this profile; however, there are no additional requirements for support of these FGs other than the requirements stated in ISO/IEC 10611-3.

A.2.3 Prohibited functional groups

The following functional groups that are optional in ISO/IEC 10611-3, are prohibited in this profile as specified in this part of AMH1n(D).

The use of the Return of Contents functional group is prohibited in this profile as specified in AMH1n(D) Part 1.

A.3 Additional Information

No additional requirements.

Standardized Profile

TITLE: Information technology – Standardized Profiles AMH1n(D) – Military Message Handling Systems – Common Unrestricted Messaging – Part 4: AMH12(D) – MMHS Requirements for MTS Access (P3)

This document forms part of a multipart Standardized Profile (SP) for Common Unrestricted Messaging for Military Message Handling Systems (MMHS). It is outside the scope of the current Taxonomy Framework for International Standardized Profiles (ISP). This SP is a delta to the Civilian MHS Common Messaging ISP 10611 and includes only the additional requirements for the MMHS. This document is content-type independent.

Introduction

This Standardized Profile (SP) is defined within the context of functional standardization, in accordance with the principles specified by ISO/IEC TR 10000, "Framework and Taxonomy of International Standardized Profiles". The context of functional standardization is one part of the overall field of Information Technology (IT) standardization activities – covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards to promote system interoperability and to provide a basis for the development of uniform, internationally recognized system tests.

One of the most important roles for a SP is to serve as the basis for the development of recognized tests. SPs also guide implementors in developing systems that fit the needs of the MMHS. SPs are produced not simply to 'legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other SPs is crucial to the successful realization of this goal.

This part of AMH1n(D) covers MMHS requirements for MTS Access (P3). It specifies any additional P3 support to that specified in ISO/IEC ISP 10611 and defines conformance requirements for an MTA which supports remote access for MMHS use, and for a remote MTS-user in the MMHS (i.e., MM-UA or MM-MS), with respect to support of P3 and associated functionality (requiring conformance to AMH12 and by reference to the common MMHS specifications in part 1).

This part of AMH1n(D) contains one normative appendix.

> Appendix A (normative) SPICS Requirements List for AMH1n(D) Part 4 (AMH12(D))

Information technology – Standardized Profiles AMH1n(D) – Military Message Handling Systems – Common Unrestricted Messaging

Part 4: AMH12(D) – MMHS Requirements for MTS Access Protocol (P3)

1 Scope

1.1 General

This part of AMH1n(D) covers access to a Message Transfer System (MTS) in the MMHSusing the P3 MTS Access Protocol (see also figure 1). These specifications form part of the Common Unrestricted Messaging application functions as defined in the parts of AMH1n(D), and are based on the Common Messaging content type-independent specifications in ISO/IEC ISP 10611-4.

1.2 Position within the taxonomy

This part of AMH1n(D) is the fourth part of a multipart SP for AMH1n(D) Military Message Handling Systems.

This part of AMH1n(D) specifies the following profile:

AMH12(D) – MMHS Requirements for MTS Access (P3)

This SP must be combined with the multipart ISP identified in ISO/IEC TR 10000-2 as "AMH1, Message Handling Systems – Common Messaging" (see also ISO/IEC TR 10000-1, 8.2 for the definition of multipart ISPs).

It may be combined with any approved T-Profiles (see ISO/IEC TR 10000) specifying OSI connection-mode Transport service.

1.3 Scenario

The model used is one of access to an MTS by an MMHS MTS-user – specifically, the interconnection between a message transfer agent (MTA) and an MTS-user using the P3 protocol, as shown in figure 1. Error! Switch argument not specified.

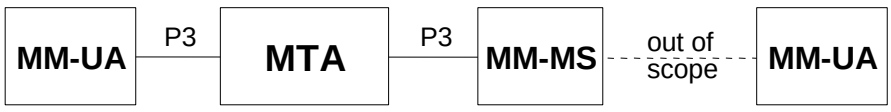


Figure 1 – AMH12(D) scenario

The AMH12(D) profile covers all aspects of the MTS Abstract Service, as defined in clause 8 of ISO/IEC 10021-4 when realized using the P3 protocol in the MMHS.

2 References

The following documents are additional documents referenced to those cited in ISO/IEC 10611-1.

The following documents contain provisions which, through reference in this text, constitute provisions of this part of AMH1n(D). At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of AMH1n(D) are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by SPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

Technical corrigenda to the base standards referenced are listed in appendix B of ISO/IEC ISP 10611-4.

NOTE – References in the body of this part of AMH1n(D) to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

ACP 123(B): *Common Messaging Strategy and Procedures.*

ISO/IEC ISP 10611-4: 1994, *Information technology – International Standardized Profiles – Message Handling Systems – Common Messaging – Part 4: AMH12 – MTS Access (P3).*

ISO/IEC 10021-1:1990/Am.2, *Information technology – Message-Oriented Text Interchange System (MOTIS) – Part 1: System and Service Overview, Amendment 1 Message Store Extensions 1994.*

ISO/IEC 10021-2:1990/Am.1, *Information technology – Message-Oriented Text Interchange System (MOTIS)* – Part 2: *Overall Architecture; Amendment 1: Representation of* O/R *Addresses for Human Exchange 1994.*

ISO/IEC 10021-2:1990/Am.2, *Information technology – Message-Oriented Text Interchange System (MOTIS)* – Part 2: *Overall Architecture; Amendment 2: Minor Enhancements: Multinational Organizations and Terminal-form Addresses 1994.*

ISO/IEC 10021-4:1990/Am.1, *Information technology – Message-Oriented Text Interchange System (MOTIS)* – Part 4: *Message Transfer System: Abstract Service Definition and Procedures; Amendment 1: Minor Enhancements: Notification-type and Directory Substitution 1994.*

MHS Implementors' Guide, Version 11, July 1994 *(ITU-T Special Rapporteur's Group on Message Handling Systems and ISO/IEC JTC1/SC18/WG4 SWG on Messaging).*

(Application for copies of these documents should be addressed to the American National Standards Institute, 11 West 42nd Street, NY, NY 10036 or to ISO, Van Demonstrate 94, 1013 CN Amsterdam, Netherlands.)

3 Definitions

For the purposes of this part of AMH1n(D), the following definitions apply.

Terms used in this part of AMH1n(D) are defined in the referenced base standards, in addition, the terms defined in ISO/IEC 10611-4 apply.

4 Abbreviations and Acronyms

The following are additional abbreviations to those defined in ISO/IEC ISP 10611-4.

ACP	Allied Communication Publication
AIG	Address Indicator Group
CAD	Collective Address Designator
CCITT	International Telegraph and Telephone Consultative Committee
CSP	Common Security Protocol
IEC	International Electrotechnical Commission
ISO	International Standards Organization
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
JTC1	Joint Technical Committee
MHS	Message Handling Systems
MM	Military Message
MM-	Military Messaging
MM-MS	Military Messaging Message Store
MM-UA	Military Messaging User Agent
MMHS	Military Message Handling System
MMS	Military Messaging Service
MSSE	Message Submission Service Element
MTS	Message Transfer System
P3	MTS Access Protocol

P773	MMS Protocol
PICS	Protocol Implementation Conformance Statement
PLAD	Plain Language Address Designator
RI	Routing Indicator
SC	Subcommittee
SMA	Signal Message Address
S/MIME	Secure Multipurpose Internet Mail Extensions
SP	Standardized Profiles
SPICS	Standardized Profiles Implementation Conformance Statement
SWG	Special Working Group
WG	Working Group

Support level for protocol elements and features (see 3.2):

m	mandatory full support
m-	mandatory minimal support
c	conditional
r	required, dynamically mandatory
x	excluded

5 Conformance

This part of AMH1n(D) states requirements upon implementations to achieve interworking. A claim of conformance to this part of AMH1n(D) is a claim that all requirements in the relevant base standards are satisfied, and that all requirements in the following clauses and in appendix A of this part of AMH1n(D) are satisfied. Appendix A states the relationship between these requirements and those of the base standards.

5.1 Conformance statement

For each implementation claiming conformance to profile AMH12(D), a ISPICS shall be made available stating support or non-support of each option identified in this part of AMH1n(D). The ISPICS Proforma in ISO/IEC 10611-4 shall be used to generate the ISPICS.

The scope of conformance to profile AMH12(D) covers both MTAs and MTS-users. A claim of conformance to profile AMH12(D) shall state whether an implementation claims conformance as an MTA, as a MM-UA, or as an MM-MS which is not collocated with an MTA.

A claim of conformance to profile AMH12(D) shall confirm that the implementation supports profile AMH12 as specified in ISO/IEC 10611-4.

5.2 MHS conformance

This part of AMH1n(D) specifies implementation options or selections such that conformant implementations will satisfy the conformance requirements of ISO/IEC 10021 and the CCITT X.400 Recommendations.

Implementations conforming to profile AMH12(D) shall as a minimum conform to the basic requirements of profile AMH12, as specified in ISO/IEC 10611-4, as appropriate to the type of implementation (i.e., MTA or MTS-user) for which conformance is claimed.

Implementations conforming to profile AMH12(D) shall additionally implement all the mandatory support (m) features identified as basic requirements in appendix A. They shall also support corresponding MHS Elements of Service and associated procedures as specified in AMH1n(D) Part 1, as appropriate to the scope of this profile.

Implementations conforming to profile AMH12(D) shall state whether or not they support any of the optional functional groups as specified in AMH1n(D) Part 1 which are applicable to the scope of this profile. For each functional group for which support is claimed, an implementation shall additionally implement all the mandatory support (m) features identified for that functional group in appendix A. They shall also support corresponding MHS Elements of Service and associated procedures as specified in AMH1n(D) Part 1, as appropriate to the scope of this profile.

Implementations conforming to profile AMH12(D) shall state the P3 application context(s) for which conformance is claimed.

5.3 Underlying layers conformance

Implementations conforming to profile AMH12(D) shall also meet the requirements for support of underlying layers as specified in subclause 5.3 of ISO/IEC ISP 10611-4.

Appendix A

(normative)

SPICS Requirements List

for AMH1n(D) Part 4 (AMH12(D))

In the event of a discrepancy becoming apparent in the body of this part of AMH1n(D) and the tables in this appendix, this appendix is to take precedence.

This appendix specifies the support constraints and characteristics of AMH1n(D) Part 4 on what shall or may appear in the implementation columns of a ISPICS. Such requirements are additional to those specified in annex A of ISO/IEC 10611-4 (reference numbers correspond to items in that annex).

Clause A.1 specifies the basic requirements for conformance to profile AMH12(D). Clause A.2 specifies additional requirements to those specified in A.1 for each of the optional functional groups if conformance to such a functional group is claimed.

In each table, the "Profile" column reflects the level of support required for conformance to this SP (using the classification and notation defined in clause 3.2). The supplier of an implementation for which conformance to profile AMH12(D) is claimed should complete the ISPICS referred to by annex A of ISO/IEC 10611-4 in accordance with the requirements contained therein together with any additional requirements in this appendix for the type of implementation (i.e., MTA or MTS-user) in question.

(Note: Some parts of appendix A require completion of the IO-ICS in ACP 123)

A.1 Basic requirements

A.1.1 Supported application contexts

No additional requirements.

A.1.2 Supported operations

A.1.2.2Message Submission Service Element (MSSE)

Ref	Operation	MTS-user	MTA
		Profile	Profile
2	ProbeSubmission	x	x[1]
3	CancelDeferredDelivery	c[2]	

Notes:

1 Reception of Probe at the MTA will be logged as a security violation and no delivery or non-delivery report will be returned.

2 Mandatory if Deferred Delivery is supported, else optional.

A.1.3 Operation arguments/results

No additional requirements.

A.1.4 MessageSubmissionEnvelope

Ref	Element	MTS-user Profile	MTA Profile
5	priority	mr	mr
8.4	latest-delivery-time		m
9.4.1	originator-requested-alternate-recipient	m	m

A.1.5 ProbeSubmissionEnvelope

Probes are dynamically prohibited in this profile as specified in this part of AMH1n(D).

A.1.6 MessageDeliveryEnvelope

Ref	Element	MTS-user Profile	MTA Profile
3.4	priority		mr
3.12.19	dl-expansion-history-indication	m	

A.1.7 ReportDeliveryEnvelope

No additional requirements.

A.1.8 Common data types

Ref	Element	MTS-user Profile	MTA Profile
4.2	extended	m	
5.3	alternate-recipient-allowed	m	

Ref	Element	MTS-user Profile	MTA Profile
5.4	content-return-request	m[1]	m

Note:

1 The content-return-request shall be present and set to not request return of content.

A.1.9 Extension data types

No additional requirements.

A.1.10 O/R names

Ref	Element	MTS-user Profile	MTA Profile
1	mnemonic O/R Address		m
2	numeric O/R Address	m	m
6	directory-name	m	m

A.1.10.1 Mnemonic O/R address

Ref	Element	MTS-user Profile	MTA Profile
2	built-in-domain-defined-attributes	m	m
2.1	acp-plad[1]	m-	m-
2.2	acp-ri[2]	m-	m-

Notes:

1 This element can be any acp-address including, but not limited to, PLADs, SMAs, AIGs, and CADs.

2 This element can be any RI, including collective RIs.

A.1.10.2 Numeric O/R address

Ref	Element	MTS-user Profile	MTA Profile
2	built-in-domain-defined-attributes	m	m
2.1	acp-plad[1]	m-	m-
2.2	acp-ri[2]	m-	m-

Notes:

Notes:

1 This element can be any acp-address including, but not limited to, PLADs, SMAs, AIGs, and CADs.

2 This element can be any RI, including collective RIs.

A.1.10.3 Terminal O/R address

Ref	Element	MTS-user Profile	MTA Profile
2	built-in-domain-defined-attributes	m	m
2.1	acp-plad[1]	m-	m-
2.2	acp-ri[2]	m-	m-

Notes:

1 This element can be any acp-address including, but not limited to, PLADs, SMAs, AIGs, and CADs.

2 This element can be any RI, including collective RIs.

A.2 Functional groups

A.2.1 Mandatory functional groups

The following functional groups that are optional in ISO/IEC 10611-4, are mandatory in this profile as specified in this part of AMH1n(D):

Redirection (RED)
Latest Delivery (LD)
User of Directory (DIR)

There are no additional requirements to those specified for support of these functional groups.

A.2.2 Optional functional groups

The following requirements are additional to those specified in A.1 if support of the functional group is claimed.

The Security (SEC), Physical Delivery (PD), Conversion (CV), and Distribution List (DL) FGs may optionally be implemented in this profile; however, there are no additional for support of these FGs other than the requirements stated in ISO/IEC 10611-4.

A.2.3 Prohibited functional groups

The following functional groups that are optional in ISO/IEC 10611-4, are prohibited in this profile as specified in this part of AMH1n(D). The use of the Return of Contents functional group is prohibited in this profile as specified in AMH1n(D) Part 1.

A.3 Additional information

No additional requirements.

Standardized Profile

TITLE: Information technology – Standardized Profiles AMH1n(D) – Military Message Handling Systems – Common Unrestricted Messaging – Part 5: AMH13(D) – MMHS Requirements for MS Access (P7)

This document forms part of a multipart Standardized Profile (SP) for Common Unrestricted Messaging for Military Message Handling Systems (MMHS). It is outside the scope of the current Taxonomy Framework for International Standardized Profiles (ISP). This SP is a delta to the Civilian MHS Common Messaging ISP 10611 and includes only the additional requirements for the MMHS. This document is content-type independent.

Introduction

This Standardized Profile (SP) is defined within the context of functional standardization, in accordance with the principles specified by ISO/IEC TR 10000, "Framework and Taxonomy of International Standardized Profiles". The context of functional standardization is one part of the overall field of Information Technology (IT) standardization activities – covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards to promote system interoperability and to provide a basis for the development of uniform, internationally recognized system tests.

One of the most important roles for a SP is to serve as the basis for the development of recognized tests. SPs also guide implementors in developing systems that fit the needs of the MMHS. SPs are produced not simply to 'legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other SPs is crucial to the successful realization of this goal.

This part of AMH1n(D) covers access to an MM-MS using the P7 MS Access Protocol in the MMHS. It specifies any additional P7 support to that specified in ISO/IEC ISP 10611-5 and defines conformance requirements for an MS which supports remote access for MMHS use, and for a remote MS-user in the MMHS (i.e., MM-UA), with respect to support of P7 and associated functionality (requiring conformance to AMH13 and by reference to the common MMHS specifications in part 1).

This part of AMH1n(D) contains one normative appendix.

> Appendix A (normative) SPICS Requirements List for AMH1n(D) Part 5 (AMH13(D))

Information technology – Standardized Profiles AMH1n(D) – Military Message Handling Systems – Common Unrestricted Messaging

Part 5: AMH13(D) – MMHS Requirements for MS Access Protocol (P7)

1 Scope

1.1 General

This part of AMH1n(D) covers access to a Message Store (MS) in the MMHS using the P7 MS Access Protocol (see also figure 1). These specifications form part of the Common Unrestricted Messaging application functions, as described in the parts of AMH1n(D), and are based on the Common Messaging content type-independent specifications in ISO/IEC ISP 10611-5.

1.2 Position within the taxonomy

This part of AMH1n(D) is the fifth part of a multipart SP for AMH1n(D) Military Message Handling Systems.

This part of AMH1n(D) specifies the following profile:

AMH13(D) – MMHS Requirements for MS Access (P7)

This SP must be combined with the multipart ISP identified in ISO/IEC TR 10000-2 as "AMH1, Message Handling Systems – Common Messaging" (see also ISO/IEC TR 10000-1, 8.2 for the definition of multipart ISPs).

It may be combined with any approved T-Profiles (see ISO/IEC TR 10000) the OSI connection-mode Transport service.

1.3 Scenario

The model used is one of access to an Military Messaging Message Store (MM-MS) by an MM MS-user – specifically, the interconnection between an MM-MS and an MS-user (i.e., an MM-UA) using the P7 protocol, as shown in figure 1.

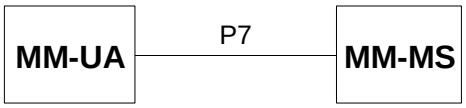


Figure 1 – AMH13(D) scenario

The AMH13(D) profile covers all aspects of the MS Abstract Service, as defined in ISO/IEC 10021-5, when realized using the P7 protocol in the MMHS.

2 References

The following documents are additional documents referenced to those cited in ISO/IEC 10611-1.

The following documents contain provisions which, through reference in this text, constitute provisions of this part of AMH1n(D). At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of AMH1n(D) are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by SPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

Technical corrigenda to the base standards referenced are listed in appendix B of ISO/IEC ISP 10611-5.

NOTE – References in the body of this part of AMH1n(D) to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

ACP 123(B): *Common Messaging Strategy and Procedures.*

ISO/IEC ISP 10611-5: 1994, *Information technology – International Standardized Profiles – Message Handling Systems – Common Messaging – Part 5: AMH13 – MS Access (P7).*

ISO/IEC 10021-1:1990/Am.2, *Information technology – Message-Oriented Text Interchange System (MOTIS)* – Part 1: *System and Service Overview, Amendment 1 Message Store Extensions 1994.*

ISO/IEC 10021-2:1990/Am.1, *Information technology – Message-Oriented Text Interchange System (MOTIS)* – Part 2: *Overall Architecture; Amendment 1: Representation of O/R Addresses for Human Exchange 1994.*

ISO/IEC 10021-2:1990/Am.2, *Information technology – Message-Oriented Text Interchange System (MOTIS)* – Part 2: *Overall Architecture; Amendment 2: Minor Enhancements: Multinational Organizations and Terminal-form Addresses 1994.*

ISO/IEC 10021-4:1990/Am.1, *Information technology – Message-Oriented Text Interchange System (MOTIS)* – Part 4: *Message Transfer System: Abstract Service Definition and Procedures; Amendment 1: Minor Enhancements: Notification-type and Directory Substitution 1994.*

MHS Implementors' Guide, Version 11, July 1994 (ITU-T Special Rapporteur's Group on Message Handling Systems and ISO/IEC JTC1/SC18/WG4 SWG on Messaging).

(Application for copies of these documents should be addressed to the American National Standards Institute, 11 West 42nd Street, NY, NY 10036 or to ISO, Van Demonstrate 94, 1013 CN Amsterdam, Netherlands.)

3 Definitions

For the purposes of this part of AMH1n(D), the following definitions apply.

Terms used in this part of AMH1n(D) are defined in the referenced base standards, in addition, the terms defined in ISO/IEC 10611-5 apply.

4 Abbreviations and Acronyms

The following are additional abbreviations to those defined in ISO/IEC ISP 10611-5.

ACP	Allied Communication Publication
AIG	Address Indicator Group
CAD	Collective Address Designator
CCITT	International Telegraph and Telephone Consultative Committee
CSP	Common Security Protocol
IEC	International Electrotechnical Commision
ISO	International Standards Organization
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
JTC1	Joint Technical Committee
MM	Military Message
MM-	Military Messaging
MM-MS	Military Messaging Message Store
MM-UA	Military Messaging User Agent
MMHS	Military Message Handling System

MMS	Military Messaging Service
MRSE	Message Retrieval Service Element
MSSE	Message Submission Service Element
MTS	Message Transfer System
P7	MS Access Protocol
P772	MMS Protocol
PICS	Protocol Implementation Conformance Statement
PLAD	Plain Language Address Designator
RI	Routing Indicator
RoC	Return of Content
SC	Subcommittee
SMA	Signal Message Address
S/MIME	Secure Multipurpose Internet Mail Extensions
SP	Standardized Profile
SPICS	Standardized Profile Implementation Conformance Statement
SWG	Special Working Group
WG	Working Group

Support level for protocol elements and features (see 3.2):

m	mandatory full support
m-	mandatory minimal support
o	optional support
i	out of scope
x	excluded

5 Conformance

This part of AMH1n(D) states requirements upon implementations to achieve interworking. A claim of conformance to this part of AMH1n(D) is a claim that all requirements in the relevant base standards are satisfied, and that all requirements in the following clauses and in appendix A of this part of AMH1n(D) are satisfied. Annex A states the relationship between these requirements and those of the base standards.

5.1 Conformance statement

For each implementation claiming conformance to profile AMH13(D), a ISPICS shall be made available stating support or non-support of each option identified in this part of AMH1n(D). The ISPICS Proforma in ISO/IEC 10611-5 shall be used to generate the ISPICS.

The scope of conformance to AMH13(D) covers both MM-MSs and MS-users (i.e., MM-UAs). A claim of conformance to profile AMH13(D) shall confirm that the

implementation supports profile AMH13 as specified in ISO/IEC ISP 10611-5 and shall state whether the implementation supports MM-MS or MS-user functionality.

5.2 MHS conformance

This part of AMH1n(D) specifies implementation options or selections such that conformant implementations will satisfy the conformance requirements of ISO/IEC 10021 and the CCITT X.400 Recommendations.

Implementations conforming to profile AMH13(D) shall implement the mandatory support (m) features identified as basic requirements in appendix A. They shall also support corresponding MHS Elements of Service and associated procedures as specified in AMH1n(D) Part 1, as appropriate to the scope of this profile and to the role (i.e., MM-MS or MS-user) for which conformance is claimed.

Implementations conforming to profile AMH13(D) shall state whether or not they support any of the optional functional groups as specified in AMH1n(D) Part 1 which are applicable to the scope of this profile and to the role (i.e., MM-MS or MS-user) for which conformance is claimed. For each functional group for which support is claimed, an implementation shall implement all the mandatory support (m) features identified for that functional group in appendix A. They shall also support corresponding MHS Elements of Service and associated procedures as specified in AMH1n(D) Part 1, as appropriate to the scope of this profile and to the role (i.e., MM-MS or MS-user) for this conformance is claimed.

Implementations conforming to profile AMH13(D) shall state the P7 application context(s)for this conformance is claimed.

5.3 Underlying layers conformance

Implementations conforming to profile AMH13(D) shall also meet the requirements for support of underlying layers as specified in subclause 5.3 of ISO/IEC ISP 10611-5.

Appendix A

(normative)

SPICS Requirements List

for AMH1n(D) Part 5 (AMH13(D))

In the event of a discrepancy becoming apparent in the body of this part of AMH1n(D) and the tables in this appendix, this appendix is to take precedence.

This appendix specifies the support constraints and characteristics of AMH1n(D) Part 5 on what shall or may appear in the implementation columns of a ISPICS. Such requirements are additional to those specified in annex A of ISO/IEC ISP 10611-5 (reference numbers correspond to items in that annex).

Clause A.1 specifies the basic requirements for conformance to profile AMH13(D). Clause A.2 specifies additional requirements to those specified in A.1 for each of the optional functional groups if conformance to such a functional group is claimed.

In each table, the "Profile" column reflects the level of support required for conformance to this SP (using the classification and notation defined in clause 3.2). The supplier of an implementation for which conformance to profile AMH13(D) is claimed should complete the ISPICS referred to by annex A of ISO/IEC ISP 10611-5 in accordance with the requirements contained therein together with any additional requirements in this appendix for the type of implementation (i.e., MM-MS or MS-user) in question.

(Note: Some parts of appendix A require completion of IO-ICS in ACP 123.)

A.1 Basic requirements

A.1.1 Supported application contexts

No additional requirements.

A.1.2 Supported operations

A.1.2.2Message Submission Service Element (MSSE)

Ref	Operation	UA	MS
		Profile	Profile
2	ProbeSubmission	x	x
3	CancelDeferredDelivery	c[1]	

Notes:

1 Mandatory if Deferred Delivery is supported, else optional.

A.1.2.3Message Retrieval Service Element (MRSE)

Ref	Operation	UA	MS
		Profile	Profile
1	Summarize	m	
2	List	m	
5	Register-MS (note 1)	c^1	

Notes:

c^1 If the UA supports a secure means of ms-registration then m, else o.

Note 1: The register-MS operation shall be supported by the MS, it shall be performed via a secure means. UA support is not required if the implementation supports the operation via local function within the MS (i.e. by MS-management, MS configuration or other local means). In any case, users shall never be able to register their own clearance via the ms-register operation. The method by which the implementation supports the register-MS operations in the MS shall be stated in the PICs/PIXIT.

A.1.3 Operation arguments/results

A.1.3.1 MSBind

No additional requirements.

A.1.3.2 MessageSubmission

No additional requirements.

A.1.3.3 ProbeSubmission

No additional requirements.

A.1.3.4 CancelDeferredDelivery

No additional requirements.

A.1.3.5 SubmissionControl

No additional requirements.

A.1.3.6 Summarize

No additional requirements.

A.1.3.7 List

No additional requirements.

A.1.3.8 Fetch

No additional requirements.

A.1.3.9 Delete

No additional requirements.

A.1.3.10 Register-MS

Ref	Operation	UA	MS
		Profile	Profile
1.1	auto-action-registrations	m	m
1.1.2	auto-alert	m	m
1.2	auto-action-deregistrations	m	m
1.2.2	auto-alert	m	m

A.1.3.11 Alert

No additional requirements.

A.1.3.12 Register

No additional requirements.

A.1.3.13 ChangeCredentials

No additional requirements.

A.1.4 MessageSubmissionEnvelope

Ref	Operation	UA	MS
		Profile	Profile

Ref	Operation	UA	MS
		Profile	Profile
5	priority	mr	mr
8.4	latest-delivery-time	m	
9.4.1	originator-requested-alternate-recipient	m	m

A.1.5 ProbeSubmissionEnvelope

Probes are out of scope of this profile as specified in this part of AMH1n(D).

A.1.6 AutoForwardRegistrationParameter

No additional requirements.

A.1.7 AutoAlertRegistrationParameter

No additional requirements.

A.1.8 Common data types

Ref	Operation	UA	MS
		Profile	Profile
11.2	extended	m	
12.3	alternate-recipient-allowed	m[1]	
12.4	content-return-request	m[2]	m

Notes:

1 The dynamic behaviour of the alternate-recipient-allowed element is to set to allow alternate recipients unless specifically set to disallowed by the originator. So as a default, this argument shall be set to alternate-recipient-allowed. (Note: this effectively changes the base standard default to allow alternative recipients).

2 The content-return request shall be present and set to not request return of content.

A.1.9 Extension data types

No additional requirements.

A.1.10 O/R names

Ref	O/R Name Form	UA	MS

		Profile	Profile
2	Numeric O/R Address	m	
6	Directory Name	m	

A.1.10.1 Mnemonic O/R address

Ref	Element	UA	MS
		Profile	Profile
2	built-in-domain-defined-attributes	m	m
2.1	acp-plad[1]	m-	m-
2.2	acp-ri[2]	m-	m-

Notes:

1 This element can be any acp-address including, but not limited to, PLADs, SMAs, AIGs, and CADs.

2 This element can be any RI, including collective RIs.

A.1.10.2 Numeric O/R address

Ref	Element	UA	MS
		Profile	Profile
2	built-in-domain-defined-attributes	m	m
2.1	acp-plad[1]	m-	m-
2.2	acp-ri[2]	m-	m-

Notes:

1 This element can be any acp-address including, but not limited to, PLADs, SMAs, AIGs, and CADs.

2 This element can be any RI, including collective RIs.

A.1.10.3 Terminal O/R address

Ref	Element	UA	MS
		Profile	Profile
2	built-in-domain-defined-attributes	m	m
2.1	acp-plad[1]	m-	m-
2.2	acp-ri[2]	m-	m-

Notes:

1 This element can be any acp-address including, but not limited to, PLADs, SMAs, AIGs, and CADs.

Notes:
2 This element can be any RI, including collective RIs.

A.1.11 General Attributes

No additional requirements.

A.2 Functional groups

A.2.1 Mandatory functional groups

The following functional groups that are optional in ISO/IEC 10611-5, are mandatory in this profile as specified in this part of AMH1n(D):

Latest Delivery (LD)
Use of Directory (DIR)

There are no additional requirements to those specified for support of these functional groups.

A.2.2 Optional functional groups

The following requirements are additional to those specified in A.1 if support of the functional group is claimed.

The Security (SEC) and Physical Delivery (PD) FGs may optionally be implemented in this profile; however, there are no additional requirements for support of these FGs other than the requirements stated in ISO/IEC 10611-5.

A.2.3 Prohibited functional groups

The following functional groups that are optional in ISO/IEC 10611-5, are prohibited in this profile as specified in this part of AMH1n(D). The use of the Return of Contents functional group is prohibited in this profile as specified in AMH1n(D) Part 1.

A.3 Additional information

No additional requirements.

ANNEX D

STANDARDIZED PROFILE FMH11(D) – MM CONTENT (P772)

Standardized Profile

TITLE: Information technology – Standardized Profiles – Military Message Handling Systems – Content Types FMH11(D) – MM Content (P772)

This document is a Standardized Profile (SP) for Military Message Handling Systems (MMHS) covering Military requirements. It is outside the scope of the current Taxonomy Framework for International Standardized Profiles (ISP). This SP is a content specific profile for the Military Message (MM) content type referred to as P772 as defined in the Allied Communication Publication (ACP) 123. This SP only specifies requirements for content specific functionality for any implementation that supports the MM content type.

Introduction

This Standardized Profile (SP) is defined within the context of functional standardization, in accordance with the principles specified by ISO/IEC TR 10000, "Framework and Taxonomy of International Standardized Profiles". The context of functional standardization is one part of the overall field of Information Technology (IT) standardization activities – covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards to promote system interoperability and to provide a basis for the development of uniform, internationally recognized system tests.

One of the most important roles for a SP is to serve as the basis for the development of recognized tests. SPs also guide implementors in developing systems that fit the needs of the MMHS. SPs are produced not simply to 'legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other SPs is crucial to the successful realization of this goal.

FMH11(D) covers content specific functionality for any implementation that supports the MM content type. It specifies support of the MM content 'protocol' in terms of basic requirements and optional functional groups and defines conformance requirements for implementations with respect to support of the MM content and associated functionality.

FMH11(D) contains two normative appendices:

Appendix A	MM Elements of Service
Appendix B	SPICS Requirements List for FMH11(D)

Information technology – Standardized Profiles – Military Message Handling Systems – Content Types

FMH11(D) – MM Content (P772)

1 Scope

1.1 General

FMH11(D) covers the representation of the MM content type (P772) by conforming implementations (see also figure 1). These specifications form part of the MMHS application functions.

1.2 Position within the taxonomy

FMH11(D) specifies the profile which states requirements for the MM content-type.

1.3 Scenario

The model assumes the exchange of military messages (content type P772) by two cooperating implementations. The P772 information objects originated and received by the implementations may be transferred via either:

1. a direct connection between the implementations (i.e., an A-profile);

2. direct connections to a relaying system (which need not comply with this profile);

3. by other bilaterally agreed means.

The specific transfer mechanism used must be mutually agreed but is outside the scope of this profile. This relationship is illustrated in figure 1.

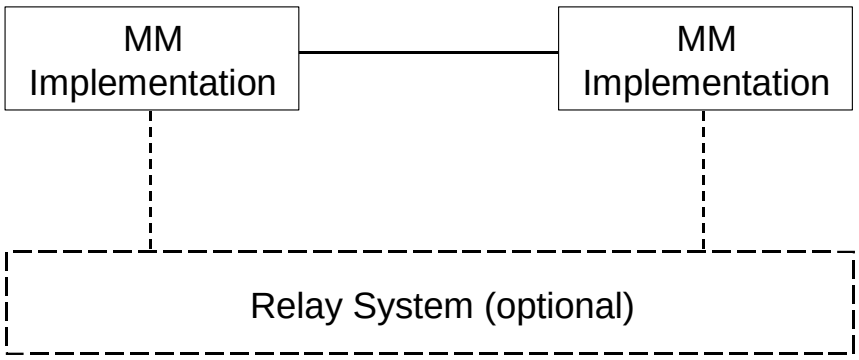


Figure 1 – FMH11(D) scenario

The MHS services and functions covered by the FMH11(D) profile are specified in ACP 123. There are no OSI upper layer services and protocols within the scope of the FMH11(D) profile.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of FMH11(D). At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on FMH11(D) are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by SPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

Technical corrigenda to the base standards referenced are listed in appendix B of the IO-ICS.

NOTE – References in the body of FMH11(D) to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

ACP 123(B): *Common Messaging Strategy and Procedures*.

ISO/IEC TR 10000-1: 1992, *Information technology – Framework and taxonomy of International Standardized Profiles* – Part 1: *Framework.*

ISO/IEC TR 10000-2: 1992, *Information technology – Framework and taxonomy of International Standardized Profiles* – Part 2: *Taxonomy.*

ISO/IEC 10021-1:1990/Am.2, *Information technology – Message-Oriented Text Interchange System (MOTIS)* – Part 1: *System and Service Overview, Amendment 2: Message Store Extensions 1994.*

ISO/IEC 10021-2:1990/Am.1, *Information technology – Message-Oriented Text Interchange System (MOTIS)* – Part 2: *Overall Architecture; Amendment 1: Representation of O/R Addresses for Human Exchange 1994.*

ISO/IEC 10021-2:1990/Am.2, *Information technology – Message-Oriented Text Interchange System (MOTIS) – Part 2: Overall Architecture; Amendment 2: Minor Enhancements: Multinational Organizations and Terminal-form Addresses 1994.*

(Application for copies of these documents should be addressed to the American National Standards Institute, 11 West 42nd Street, NY, NY 10036 or to ISO, Van Demonstrate 94, 1013 CN Amsterdam, Netherlands.)

3 Definitions

For the purposes of FMH11(D), the following definitions apply. Terms used in FMH11(D) are defined in the referenced base standards. In addition, the following terms are defined.

3.1 General

MM base standard: the base standard referred to in this F-profile is ACP 123.

Basic requirement: an Element of Service, protocol element, procedural element or other identifiable feature specified in the base standards which is required to be supported by all MMHS implementations conforming to this SP.

Functional group: a specification of one or more related Elements of Service, protocol elements, procedural elements or other identifiable features specified in the base standards which together support a significant optional area of MHS functionality.

NOTE – A functional group can cover any combination of MHS features specified in the base standards for which the effect of implementation can be determined at an external interface – i.e., via a communications protocol (other forms of exposed interface are outside the scope of this version of FMH11(D)).

3.2 Support classification

To specify the support level of arguments, results and other protocol features for FMH11(D), the following terminology is defined.

The classification of information objects and items (elements) is relative to that of the containing information element, if any. Where the constituent elements of a non-primitive element are not individually specified, then each shall be considered to have the classification of that element. Where the range of values to be supported for an element is not specified, then all values defined in the MM base standard shall be supported.

3.2.1 Static capability

The following classifications are used in FMH11(D) to specify static conformance requirements – i.e., capability.

mandatory support (m): the element or feature shall be supported. An implementation shall be able to generate the element, and/or receive the element and perform all associated procedures (i.e., implying the ability to handle both the syntax and semantics of the element) as relevant, as specified in the MM base standard.

Where support for origination (generation) and reception are not distinguished, then both capabilities shall be assumed.

NOTE – Where required by the base standards, mandatory support also implies that the implementation shall be able to pass the element on the origination port/reception port to/from the corresponding element on the submission port/delivery port/retrieval port.

optional support (o): an implementation is not required to support the element. If support is claimed, the element shall be treated as if it were specified as mandatory support. If support for origination is not claimed, then the element is not generated. If support for reception is not claimed, then an implementation may ignore the element on delivery, but will not treat it as an error.

conditional support (c): the element shall be supported under the conditions specified in FMH11(D). If these conditions are met, the element shall be treated as if it were specified as mandatory support. If these conditions are not met, the element shall be treated as if it were specified as optional support (unless otherwise stated).

out of scope (i): the element is outside the scope of FMH11(D) – i.e., it will not be the subject of a SP conformance test.

3.2.2 Dynamic behaviour

The above classifications are used in FMH11(D) to specify static conformance requirements (i.e., capability); dynamic conformance requirements (i.e., behaviour) are as specified in the MM base standards. However, in a few cases it has been necessary to specify additional dynamic conformance requirements in this profile. These are specified using a second classification code for an element as follows.

required (r): the element shall always be present. An implementation shall ensure that the element is always generated or otherwise used, as appropriate. Absence of the element on reception shall result in termination or rejection of the communication with an appropriate error indication as specified in the MM base standards.

prohibited (x): the element shall not be originated by an implementation claiming conformance to this profile, if the element is received it may be treated as a protocol violation unless otherwise stated.

4 Abbreviations and Acronyms

ACP	Allied Communication Publication
ACP127	ACP 127 Interworking
AMH	Application Message Handling
CCITT	International Telegraph and Telephone Consultative Committee
EoS	Element of Service
FG	Functional group

IEC	International Electrotechnical Commission
IO-ICS	Information Object Implementation Conformance Statement
ISO	International Standards Organization
ISP	International Standardized Profile
IT	Information Technology
ITU	International Telecommunications Union
ITU-T	ITU Telecommunications Standardization Sector
MHS	Message Handling Systems
MM	Military Message
MN	Military Notification
MOTIS	Message-Oriented Text Interchange Systems
MTS	Message Transfer System
ODA	Open Document Architecture
OSI	Open Systems Interconnection
PICS	Protocol Implementation Conformance Statement
PLAD	Plain Language Address Designator
SEC	Security
SP	Standardized Profile
SPICS	Standardized Profile Implementation Conformance Statement

Support level for protocol elements and features (see clause 3.2):

m	mandatory full support
o	optional support
c	conditional support
i	out of scope
r	required, dynamically mandatory
x	prohibited, dynamically excluded

5 Conformance

The scope of conformance to profile FMH11(D) covers content specific functionality for any implementation that supports the MM content type. Conformance to profile FMH11(D) does not imply the provision of a standard OSI communications protocol for access to the MTS.

FMH11(D) states requirements upon implementations to achieve interworking. A claim of conformance to FMH11(D) is a claim that all requirements in the relevant base standards are satisfied, and that all requirements in the following clauses and in appendices A and B of FMH11(D) are satisfied. Appendix B states the relationship between these requirements and those of the base standards.

5.1 Conformance statement

For each implementation claiming conformance to profile FMH11(D), a IO-ICS shall be made available stating support or non-support of each option identified

FMH11(D). The IO-ICS Proforma in annex B of ACP 123 shall be used to generate the IO-ICS.

5.2 MHS conformance

FMH11(D) specifies implementation options or selections such that conformant implementations will satisfy the conformance requirements for ACP 123 military messages.

Implementations conforming to profile FMH11(D) shall implement all the mandatory support (m) features identified as profile requirements in appendices A and B and shall state which optional support (o) features are implemented.

Implementations conforming to profile FMH11(D) shall state whether or not they support any of the optional functional groups as specified in clause 7. For each functional group for which support is claimed, an implementation shall support MM Elements of Service and associated procedures as specified in appendix A of this profile.

6 Basic Requirements

Appendix A specifies the basic requirements for support of MM EoS for conformance to FHM11(D). This clause qualifies the basic requirements for specific MM features.

6.1 Message Length

If an implementation imposes any constraint on the size of the message content, then such constraints shall be stated in the IO-ICS.

6.2 Number of recipients

If an implementation imposes any limit on the number of recipients that can be specified in an MM heading, then such a limit shall be stated in the IO-ICS.

7 Functional Groups

Appendix A also specifies additional requirements for support of MM EoS if support of an optional functional group (FG) is claimed, as appropriate to the MM content type (P772). The following subclause summarizes the functionality supported by the optional FG and identifies particular requirement or implementation considerations which are outside the scope of formal conformance to FMH11(D).

7.1 ACP 127 Interworking (ACP127)

The ACP 127 Interworking FG covers interworking between implementations conforming to MMHS and the older messaging system following ACP 127 guidelines. Interworking takes place by means of a gateway that performs conversion

between the two formats. Such a gateway may originate ACP 123 transitional EoS as part of the conversion process. If conformance to this FG is claimed, the implementation shall support reception of those transitional EoS and related P772 protocol elements as specified in appendices A and B. This FG may improve interworking with ACP 127 systems during a transition period.

This FG requires support on reception for these services including user interface display requirements. Even if support of the ACP127 FG is claimed, these services are not required to be supported on origination.

It is recommended that support for this FG be a configurable option, so it may be turned off when no longer required.

8 Naming and Addressing

Support for the mnemonic and numeric address forms and for directory names is mandatory. In addition, implementations shall support the Domain Defined Attributes (DDA) acp-plad and acp-ri for both origination and reception as defined in ACP 123 annex A.

Appendix A

(normative)

MM Elements of Service

A.1 MM-specific Elements of Service

The following tables specify the requirements for support of MM-specific Elements of Service by a conforming implementation.

In the following tables, the "Profile" column reflects the basic requirements for conformance to FMH11(D) – i.e., the minimum level of support required by all implementations claiming conformance to this profile (see clause 6). The "Functional Group" column specifies any additional support requirements if support of an optional functional group is claimed (see clause 7). Each column is then further subdivided into support for origination ("Orig") and reception ("Rec") as defined in clause 3.2, together with the abbreviated name of the functional group ("FG") in the case of the second column.

Table A.1 – Elements of Service Belonging to the Basic MM Service (MM EoS)

Elements of Service	Profile		Functional Group		
	Orig	Rec	FG	Orig	Rec
Copy Precedence	m	m			
IPM-message Identification	m	m			
Primary Precedence	m	m			
Subject Indication	m	m			
Typed Body	m	m			

Table A.2 MM Optional User Facilities (MM EoS)

Elements of Service	Profile		Functional Group		
	Orig	Rec	FG	Orig	Rec
ACP 127 Message Identifier	o	o	ACP127	o	m
ACP 127 Notification Request	o	i	ACP127	o	i
ACP 127 Notification Response	i	o	ACP127	i	o
Authorizing Users indication	m	m			
Auto-forwarded Indication	o	m			
Blind Copy Recipient Indication	m	m			
Body Part Encryption Indication	o	m			
Clear Service	o	m			

Elements of Service	Profile		Functional Group		
	Orig	Rec	FG	Orig	Rec
Codress Message indicator	o	o	ACP127	o	m
Corrections	o	o	ACP127	o	m
Cross-referencing Indication	m	m			
Distribution Code	m	m			
Exempted Addresses	m	m			
Expiry Date Indication	m	m			
Extended Authorization Info	m	m			
Forwarded Message Indication	m	m			
Handling Instructions	o	o	ACP127	o	m
Importance Indication[3]	i	i			
Incomplete Copy Indication	m	m			
Language Indication	m	m			
Message Instructions	m	m			
Message Type	m	m			
Multi-part Body Indication	m	m			
Non-receipt Notification Request Indication	m	c[1]			
Obsoleting Indication	m	m			
Originator Indication	m	m			
Originator Reference	m	m			
Originator PLAD	o	o	ACP127	o	m
Other Recipient Indicator	m	m			
Pilot Forwarded	o	o	ACP127	o	m
Primary and Copy Recipients Indication	m	m			
Receipt Notification Request Indication[2]	m	m			
Reply Request Indication	m	m			
Replying Message Indication	m	m			
Security Information Labels	o	o			
Sensitivity Indication[3]	i	i			
Use of Address List	m	m			

Notes:

1 If any condition that could result in an NRN is supported, origination for NRN must also be supported. If an implementation can request a Non-receipt notification, it must be able to display it for the user if received.

2 If a Receipt Notification is received, the implementation must be able to display it for the user.

3 The originator's user interface shall not prompt for this EoS. If the protocol that supports this EoS is present upon reception then the EoS shall not be displayed to the user.

Appendix B

(normative)

SPICS REQUIREMENTS LIST FOR FMH11(D)

In the event of a discrepancy becoming apparent in the body of FMH11(D) and the tables in this appendix, this appendix is to take precedence.

This appendix specifies the support constraints and characteristics of FMH11(D) on what shall or may appear in the implementation columns of a completed IO-ICS.

Clause B.1 specifies the basic requirements for conformance to profile FMH11(D).

In each table, the "Profile" column reflects the level of support required for conformance to this SP (using the classification and notation defined in clause 3.2).

The "References" column has cross references to other relevant parts of this appendix. When it specifies another table, that table is an expansion of the line at which the reference occurs. If a line number is specified, only that line is related to the line at which the reference occurs. A number in parenthesis ( ) after a table reference refers to that line in the specified table.

B.1 Basic requirements

B.1.1 Supported information objects

Ref	Element	Profile		References
		Orig	Rec	
1	Military Message (MM)	m	m	
1.1	heading	m	m	see B.1.2
1.2	body	m	m	see B.1.3
2	Military Notification (MN)	m[1]	m	see B.1.4

Notes:

1 If the conditions for which a Non-Receipt Notification would be generated are not supported, the ability to generate a Non-Receipt Notification is optional.

B.1.2 MM heading fields

Ref	Element	Profile		References
		Orig	Rec	
1	this-IPM	mr	m	see B.1.5(3)
2	originator	m	m	see B.1.5(2)
3	authorizing-users	m	m	see B.1.5(2)

Ref	Element	Profile		References
		Orig	Rec	
4	primary-recipients	m	m	see B.1.5(1)
5	copy-recipients	m	m	see B.1.5(1)
6	blind-copy-recipients	m	m	see B.1.5(1)
7	replied-to-IPM	m	m	see B.1.5(3)
8	obsoleted-IPMs	m	m	see B.1.5(3)
9	related-IPMs	m	m	see B.1.5(3)
10	subject	mr	m	
11	expiry-time	m	m	
12	reply-time	m	m	
13	reply-recipients	m	m	see B.1.5(2)
14	importance[1]	ix	i	
15	sensitivity[1]	ix	i	
16	auto-forwarded[2]	c[3]	m	
17	extensions	m	m	
17.1	incomplete-copy	c[4]	m	
17.2	languages	m	m	
17.3	primary-precedence	mr[5]	m	
17.4	copy-precedence	mr[6]	m	
17.5	message-type	mr	m	
17.5.1	type	mr	m	
17.5.2	identifier	m	m	
17.6	address-list-indicator	o	m	
17.6.1	type	m	m	
17.6.2	list-name	m	m	
17.6.3	notification-request	m	m	
17.6.4	reply-request	m	m	
17.7	exempted-address	m	m	
17.8	extended-authorisation-info	m	m	
17.9	distribution-codes	m	m	
17.9.1	sics	m	m	
17.9.2	dist-extensions	o	m	
17.10	message-instructions	m	m	
17.11	codress-message[7]	o	o	
17.12	originator-reference	m	m	
17.13	other-recipient-indicator	m	m	
17.13.1	type	m	m	
17.13.2	designator	m	m	
17.14	handling-instructions[7]	o	o	
17.15	pilot-forwarding-info[7]	o	o	
17.15.1	pilot-precedence	m	m	see B.1.5(4)
17.15.2	pilot-recipient	m	m	see B.1.5(2)
17.15.3	pilot-security	m	m	
17.15.4	pilot-handling	m	m	
17.16	acp127-message-identifier[7]	o	o	

Ref	Element	Profile		References
		Orig	Rec	
17.17	originator-plad[7]	o	o	
17.18	security-information-labels	o	o	

Notes:

1 This protocol element shall not be prompted for or displayed at the user interface. It shall not be originated and if received should be ignored.

2 Support for auto-forwarding is dependent on local policy and may be influenced by security policies.

3 If the implementation supports autoforwarding them m, else o.

4 During forwarding, if the implementation allows elements of the forwarded message to be omitted then m, else o.

5 Presence of this element is required in a message if and only if primary recipients are specified in the message.

6 Presence of this element is required in a message if and only if copy recipients are specified in the message.

7 These elements are for support of EoS that are only needed to support the ACP127 FG.

B.1.3 MM body

Ref	Element	Profile		References
		Orig	Rec	
1	ia5-text	m	m	
1.1	parameters	m	m	
1.1.1	repertoire	m	m	
1.2	data	m	m	
2	voice	o	m	
2.1	parameters	i	i	
2.2	data	m	m	
3	g3-facismile	o	o	
3.1	parameters	m	m	
3.1.1	number-of-pages	o	m	
3.1.2	non-basic-parameters	o	m	
3.1.2.1	two-dimensional	o	m	
3.1.2.2	fine-resolution	o	m	
3.1.2.3	unlimited-length	o	o	
3.1.2.4	b4-length	o	o	
3.1.2.5	a3-width	o	o	
3.1.2.6	b4-width	o	o	
3.1.2.7	uncompressed	o	o	
3.2	data	m	m	

Ref	Element	Profile		References
		Orig	Rec	
4	g4-class-1	o	o	
5	teletex	o	o	
5.1	parameters	m	m	
5.1.1	number-of-pages	o	m	
5.1.2	telex-compatible	o	m	
5.1.3	non-basic-parameters	o	m	
5.2	data	m	m	
6	videotex	o	o	
6.1	parameters	m	m	
6.1.1	syntax	o	m	
6.2	data	m	m	
7	encrypted	o	m	
7.1	parameters	i	i	
7.2	data	m	m	
8	message	m	m	
8.1	parameters	m	m	
8.1.1	delivery-time	m	m	
8.1.2	delivery-envelope	m	m	
8.2	data	m	m	
8.2.1	IPM	m	m	
9	mixed-mode	o	o	
10	bilaterally-defined	o	o	
11	nationally-defined	o	o	
12	externally-defined[1]	m	m	see B.1.3.1

Note:

1 It shall be stated in the IO-ICS whether any other specific extended body part types are supported.

B.1.3.1 Extended body part support

Ref	Element	Profile		References
		Orig	Rec	
1	ia5-text-body-part	m	m	see B.1.3(1)
2	g3-facsimile-body-part	o	o	see B.1.3(3)
3	g4-class-1-body-part	o	o	see B.1.3(4)
4	teletex-body-part	o	o	see B.1.3(5)
5	videotex-body-part	o	o	see B.1.3(6)
6	encrypted-body-part	o	m	
6.1	parameters	o	o	
6.2	data	m	m	
7	message-body-part	m	m	see B.1.3(8)
8	mixed-mode-body-part	o	o	
9	bilaterally-defined-body-part	o	o	

Ref	Element	Profile		References
		Orig	Rec	
10	nationally-defined-body-part	o	o	
11	general-text-body-part[1]	m	m	
12	file-transfer-body-part	m	m	
13	voice-body-part	o	o	
13.1	parameters	o	o	
13.2	data	m	m	
14	oda-body-part	o	o	
15	adatp3-body-part	m	m	
15.1	parameters	m	m	
15.2	data	m	m	
16	corrections-body-part[2]	o	o	
16.1	parameters	o	m	
16.2	data	o	m	
17	forwarded-encrypted-body-part	o	m	
17.1	parameters	m	m	
17.1.1	delivery-time	m	m	
17.1.2	delivery-envelope	m	m	
17.2	data	m	m	
18	mm-message-body-part	m	m	
18.1	parameters	m	m	
18.1.1	delivery-time	m	m	
18.1.2	delivery-envelope	m	m	
18.2	data	m	m	
19	acp127Data-body-part[2]	o	o	
19.1	parameters	o	m	
19.2	data	o	m	
20	forwarded-CSP-Message-Body-Part	o	o	
21	report-body-part	i	i	
22	notification-body-part	i	i	
23	content-body-part	m	m	

Notes:

1 It shall be stated in the IO-ICS which character repertoires are supported for support of the general-text body-part type.

2 These elements are for support of EoS that are only needed to support the ACP127 FG.

B.1.3.2 General text repertoire support

Ref	Repertoire set description	Repetoire identifier(s)	Profile	
			Orig.	Rec.

Ref	Repertoire set description	Repetoire identifier(s)	Profile	
			Orig.	Rec.
1	Basic (ISO 646)	{1,6}	m	m
2	Basic-1 (ISO 8859-1)	{1,6,100}	m	m
3	Basic + Chinese (1)	{1,6,58}	o	o
4	Basic + Chinese (2)	{1,6,165}	o	o
5	Basic + Japanese (1)	{1,6,13,87}	o	o
6	Basic + Japanese (2)	{1,6,13,168}	o	o
7	Basic + Korean	{1,6,149}	o	o
8	Basic-1 + Cryillic (ISO 8859-5)	{1,6,100,144}	o	o
9	Basic-1 + Arabic (ISO 8859-6)	{1,6,100,127}	o	o
10	Basic-1 + Greek (ISO 8859-7)	{1,6,100,126}	o	o
11	Basic-1 + Hebrew (ISO 8859-8)	{1,6,100,138}	o	o
12	Full Latin (1)	{1,6,100,154}	o	o
13	Full Latin (2) (ISO 6937)	{1,6,156}	o	o
14	Teletex Basic Latin (T.61)	{102,103,106,107}	o	o

B.1.4 MN fields

Ref	Element	Profile		References
		Orig	Rec	
1	subject-ipms	m	m	see B.1.5(3)
2	ipn-originator	m	m	see B.1.5(2)
3	ipm-preferred-recipient	m	m	see B.1.5(2)
4	conversion-eits	o	m	
5	notification-extensions	i	i	
6	non-receipt-fields	c[1]	m	
6.1	non-receipt-reason	m	m	
6.2	discard-reason	m	m	
6.3	auto-forward-comment	c[2]	m	
6.4	returned-ipm	ix	i	
6.5	nrn-extensions	i	i	
7	receipt-fields	m	m	
7.1	receipt-time	m	m	
7.2	acknowledgment-mode	m	m	
7.2.1	manual	m	m	
7.2.2	automatic	o	m	
7.3	suppl-receipt-info	o	m	
7.4	rn-extensions	i	i	
8	other-notification-type-fields	o	o	
8.1	acp 127-notification-response[3]	i	o	
8.1.1	acp 127-notification-type	i	o	
8.1.2	receipt-time	i	o	
8.1.3	addressListInicator	i	o	
8.1.4	acp127-recipient	i	o	

Ref	Element	Profile		References
		Orig	Rec	
8.1.5	acp127-supp-info	i	o	

Notes:

1 If any of the base standard conditions for Non-receipt can occur then support of this element is m, else o.

2 If auto-forwarding is supported then support of this element is m, else o.

3 These elements are for support of EoS that are only needed to support the ACP127 FG.

B.1.5 Common data types

Ref	Element	Profile		References
		Orig	Rec	
1	RecipientSpecifier			
1.1	recipient	m	m	see B.1.5(2)
1.2	notification-requests	m	m	
1.2.1	rn	m	m	
1.2.2	nrn	m	m	
1.2.3	ipm-return	ix	i	
1.3	reply-requested	m	m	
1.4	recipient-extensions	o	o	
1.4.1	acp127-notification-request[1]	o	i	
2	ORDescriptor			
2.1	formal-name	m	m	see B.1.5(5)
2.2	free-form-name	m	m	
2.3	telephone-number	o	m	
3	IPMIdentifier			
3.1	user	m	m	see B.1.5(5)
3.2	user-relative-identifier	m	m	
4	MMHSPrecedence			
4.1	deferred (0)	o	m	
4.2	routine (1)	m	m	
4.3	priority (2)	m	m	
4.4	immediate (3)	m	m	
4.5	flash (4)	m	m	
4.6	override (5)	o	m	
4.7	nato-reserved (6-15)	i	i	
4.8	nationally defined (16-30)	i	i	
5	ORName			

Ref	Element	Profile		References
		Orig	Rec	
5.1	mnemonic O/R address	m	m	
5.2	numeric O/R address	m	m	
5.3	terminal O/R address	o	o	
5.4	formatted postal O/R address	o	o	
5.5	unformatted postal O/R address	o	o	
5.6	directory-name	m	m	

Note:

1 These elements are for support of EoS that are only needed to support the ACP127 FG.

B.2 Optional functional groups

The following requirements are additional to those specified in B.1 if support of the functional groups is claimed.

B.2.1 ACP 127 Interworking (ACP127)

B.2.1.1 ACP 127 Interworking (ACP127) MM heading fields

Ref	Element	Profile	
		Orig.	Rec.
17.11	codress-message		m
17.14	handling-instructions		m
17.15	pilot-forwarded		m
17.16	acp127-message-identifier		m
17.18	originator-plad		m

B.2.1.2 ACP 127 Interworking (ACP127) MM body

Ref	Element	Profile	
		Orig.	Rec.
16	correction-body-part		m
19	acp127Data-body-part		m

B.3 Additional information

B.3.1 MM Elements of Service support

The table in ACP 123, annex B, appendix A, clause 8.1.1, shall be completed to indicate, for each MM Element of Service, whether it is available to the MHS user and, if so, how this is achieved. For each EoS for which support is claimed, the implementor will check the column which indicates how the EoS is supported in a

given instance. If appropriate the Comments column can be filled in to provide additional information as to how the EoS is selected.

ACP 123 goes beyond X.400 by stating which MM Elements of Service are to be supported as user options and which have requirements for display at the user interface. If support for these are claimed, the EoS must be selectable at the user interface for a given message. These requirements are indicated with the following codes in the Profile column in the following table:

s the user must be able to select the service and its associated information on origination

D this information must be displayed to the user, if it is present

Ref	Element of Service	Profile
1	ACP 127 Message Identifier	D
2	ACP 127 Notification Request	
3	ACP 127 Notification Response	D
4	Authorizing Users Indication	sD
5	Auto-forwarded Indication	D
6	Blind Copy Recipient Indication	sD[1]
7	Body Part Encryption Indication	D
8	Clear Service	D[2]
9	Codress Message indicator	D
10	Copy Precedence	sD[3]
11	Corrections	D
12	Cross-referencing Indication	sD
13	Distribution Code	sD
14	Exempted Addresses	sD
15	Expiry Date Indication	sD
16	Extended Authorization Info	sD
17	Forwarded Message Indication	sD
18	Handling Instructions	D
19	Importance Indication	
20	Incomplete Copy Indication	s[10]D
21	Language Indication	sD
22	Message Instructions	sD
23	Message Type	sD[4]
24	IPM-message Identification	D
25	Multi-part Body	sD
26	Non-receipt Notification Request Indication	sD[5]
27	Obsoleting Indication	sD
28	Originator Indication	D
29	Originator Reference	sD
30	Originator PLAD	
31	Other Recipient Indicator	sD

Ref	Element of Service	Profile
32	Pilot Forwarded	D
33	Primary and Copy Recipients Indication	sD[6]
34	Primary Precedence	sD[7]
35	Receipt Notification Request Indication	sD[8]
36	Reply Request Indication	sD[9]
37	Replying Message Indication	sD
38	Security Information Labels	
39	Sensitivity Indication	
40	Subject Indication	sD
41	Typed Body	
42	Use of Address List	sD

Notes:

1 If this recipient is a BCC recipient the indication must be immediately displayed to the user without explicit user command when the message is read.

2 If the Clear Service Indication is present, the phrase "RECEIVED IN THE CLEAR, TREAT AS CONFIDENTIAL" must be immediately displayed to the user when the message is read.

3 If a recipient is a Copy recipient, the Copy Precedence must be immediately displayed without explicit user command when the message is read.

4 If Message Type is present, the associated information must be immediately displayed to the user without requiring explicit user command when the message is read.

5 If a non-receipt notification is received, the information associated with it must be displayable to the user.

6 A recipient must immediately see an indication of whether he/she is specified as a Primary or Copy recipient for the message without requiring explicit user command when the message is read. Additional action may be required to display other Primary and Copy recipients.

7 If a recipient is a Primary recipient, the Primary Precedence must be immediately displayed without explicit user command when the message is read.

8 If Receipt Notification was requested, this must be displayed to the user without explicit user command when the message is read.

9 If Reply was requested, this must be displayed to the user without explicit user command when the message is read.

10 Must make available to user if forwarding of incomplete messages is supported.

B.3.2 Encoded information type conversion requests supported

It shall be stated in the IO-ICS, which encoded information type conversion request the implementation supports.

B.3.3 Non-standard integer body part types supported

It shall be stated in the IO-ICS, which non-standard integer body part types the implementation supports.

B.3.4 Extended body part types supported

It shall be stated in the IO-ICS, which extended body part types implementation supports.

B.3.5 General text body part repertoire support

It shall be stated in the IO-ICS, which general text body part repertiore the implementation supports.

ANNEX E

TACTICAL DOMAIN PROTOCOL

This annex defines additional MMHS protocols that are suited to support of tactical domains, and a profile of implementation requirements to ensure interoperability. This annex is the same as Annex E of STANAG 4406.

ANNEX E: MMHS TACTICAL PROTOCOL AND PROFILE

[This annex is provided for information.]

1. INTRODUCTION

This annex describes a tactical MMHS protocol/profile solution that is to be used for interconnection of MMHS systems over links/networks with reduced throughput capacity (lower than 20 Kbps).

Based on the requirements for Military Message Handling over low thoughput channels in tactical scenarios [ref 10], this annex identifies a set of interoperability protocols that cover all of the identified tactical MMHS interfaces. This includes application level messaging protocols and related lower layer protocols that need to be taken into account.

This annex further describes the use of data compression, encoding techniques, and addressing. The protocols defined include the STANAG 4406/X.400 protocols, the ACP 142 (P_Mul) protocol and the WAP transport protocol WDP (Wireless Datagram Protocol). For compression a new compression wrapper is defined called the “Compressed Data Type” with the mandated ZLIB [ref. 18] [ref.19] algorithm.

2. FUNCTIONAL COMPONENTS AND INTERFACES

This Annex defines the interfaces to be used for exchanging messages in tactical scenarios together with the protocols to be used over those interfaces. Figure 2.1 shows the generic conceptual tactical MMHS architecture including the agreed tactical interfaces. The figure shows one possible composition of the functional components that may be required in some tactical scenarios. In other scenarios, only a sub-set of the functional components and interfaces may be required. E.g. two nations may be interconnected using only the Light MTAs with the TMI-1 interface over a tactical gateway.

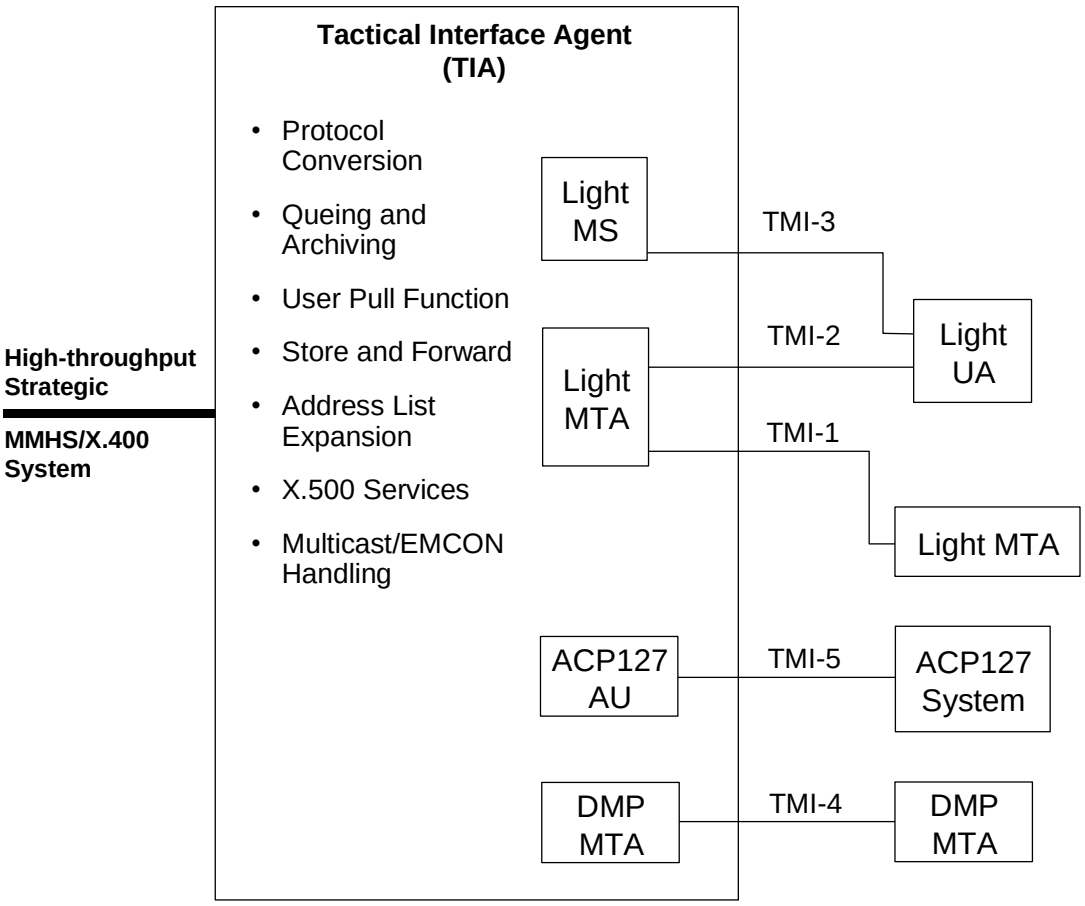


Figure 2.1 – The Generic Conceptual Tactical MMHS Architecture

2.1 Functional Components

Functional Components defines a set of functions required in a tactical message handling system. One of the Functional Components (the TIA) is defined by the inclusion of other Functional Components. The composition of functional components required for tactical MMHS, may vary with the scenario.

2.1.1 Tactical Interface Agent (TIA)

A TIA defines the interface point between the strategic and tactical MMHS systems. Different scenarios may require different services and functionality of the TIA and a TIA may therefore consist of different sets of functional components. The TIA performs functions like Protocol Conversion, Queueing

and Archiving, Storing and Forwarding, Storing for later Retrieval, X.500 services, Multicasting, EMCON procedure handling, etc. The TIA may be integrated with one of the strategic-tactical gateways.

2.1.2 Light User Agent (LUA)

A Light User Agent (LUA) is a STANAG 4406 UA that communicates with LMTAs and LMSs using a low throughput profile and protocol stack defined by the TMI-2 and TMI-3 interfaces respectively.

The LUA may operate in different modes. One is to retrieve the incoming messages using a "user-pull" function. This makes it possible for the LUA user to view the size, subject importance, etc of the messages in order to decide on which incoming messages to retrieve. The second mode is to get the messages delivered directly from the LMTA.

2.1.3 Light Message Transfer Agent (LMTA)

A Light Message Transfer Agent (LMTA) is an X.400 MTA that communicates with the LUAs and other LMTAs using a low throughput profile and protocol stack defined by the TMI-2 and TMI-1 interfaces respectively.

2.1.4 Light Message Store (LMS)

A Light Message Store (LMS) is an STANAG 4406 MS that communicates with LUAs using a low throughput profile and protocol stack defined by the TMI-3 interface.

2.1.5 ACP 127 Access Unit (or ACP 127 GW)

As defined in STANAG 4406 Edition 1, Annex D.

2.1.6 The Direct Messaging Profile (DMP-MTA)

A Direct Messaging Profile - Message Transfer Agent (DMP-MTA) is the MTA functionality that makes it possible to communicate with other DMP-MTAs using a bandwidth-efficient profile and protocol stack defined by the TMI-4 interface.

2.1.7 Other Functional Components

The Tactical Interface Agent may in addition to the functional components described in the previous sections contain:

- a Multicast/EMCON Functional Component

  The Multicast/EMCON Functional Component handles multicast of Messages, and procedures regarding recipients in EMCON conditions. This functional component will also handle circumstances when the communication path exists in only one

direction (Unidirectional Communications). The Multicast/EMCON Functional Component may be used together with other Functional Components such as LMTA, LMS and LUA.

- an Address List Expansion Functional Component
- Archiving Functional Components
- a Protocol/Profile Conversion Functional Component for conversion between the strategic protocols/profiles and the tactical protocol/profiles

2.2 Tactical Messaging Interfaces (TMI) and Conformance Requirements

This section describes the different tactical MMHS interfaces defined in the generic conceptual architecture. The section also indicates which interfaces that have to be implemented in order to state conformance with this Annex.

2.2.1 TMI-1

The support of this interface is **mandatory** in order to state conformance to this Annex.

TMI-1 is the tactical interface between two LMTAs. This interface defines the use of the X.400 P1 protocol with a slim profile/protocol stack, to increase the throughput.

Table 2.2 shows the protocols used for this interface. The different layers and protocols referred to in the table are described in the chapters 4 and 6.

Table 2.2

Layer	Protocol	Clause
Messaging Sub-Layer	**ITU-T X.400 | ISO/IEC DIS 10021 - MTS Transfer Protocol (P1)**	4.1
Tactical Adaptation Sub-Layer	Compressed Data Type	4.2.6
P_Mul Sub-Layer	ACP 142	4.3
Transport Layer	WAP WDP	6

2.2.2 TMI-2

The support of this interface is **optional**.

TMI-2 is the tactical interface between an LMTA and an LUA. This interface defines the use the X.400 P3 protocol with a slim profile over a slim protocol stack to increase the throughput.

Table 2.3 shows the protocols used for this interface. The different layers and protocols referred to in the table are described in the chapters 4 and 6.

Table 2.3

Layer	Protocol	Clause
Messaging Sub-Layer	**ITU-T X.400 | ISO/IEC DIS 10021 - MTS Access Protocol (P3)**	4.1
Tactical Adaptation Sub-Layer	Compressed Data Type	4.2.6
P_Mul Sub-Layer	ACP 142	4.3
Transport Layer	WAP WDP	6

2.2.3 TMI-3

The support of this interface is **optional**.

TMI-3 is the tactical interface between a STANAG 4406 MS and a STANAG 4406 LUA. This interface defines the use the X.400 P7 protocol with a slim profile over a slim protocol stack to increase the throughput.

Table 2.4 shows the protocols used for this interface. The different layers and protocols referred to in the table are described in the chapters 4 and 6.

Table 2.4

Layer	Protocol	Clause
Messaging Sub-Layer	**ITU-T X.400 | ISO/IEC DIS 10021 - MS Access Protocol (P7)**	4.1
Tactical Adaptation Sub-Layer	Compressed Data Type	4.2.6
P_Mul Sub-Layer	ACP 142	4.3
Transport Layer	WAP WDP	6

2.2.4 TMI-4

The support of this interface is **mandatory**.

TMI-4 defines the Direct Messaging Protocol (DMP) to be used for time critical tactical messages between two DMP MTAs.

Table 2.5 shows the protocols used for this interface. The layers and protocols referred to in the table are described in the chapters 5 and 6.

Table 2.5

Layer	Protocol	Clause
Direct Messaging Sub-Layer	DMP	5
Transport Layer	WAP WDP	6

2.2.5 TMI-5

The support of this interface is **optional**.

The ACP 127 Access Unit (Gateway) makes it possible to send Military Messages between STANAG 4406 and ACP 127 systems. The TMI-5 interface is defined by STANAG 4406 Annex D.

Table 2.6 shows the protocols used for this interface. The protocols referred to in the table are described in STANAG 4406 Ed.1 Annex D.

Table 2.6

Layer	Protocol	Clause
Messaging Sub-Layer	STANAG 4406 Edition 1, Annex D	–

3. PROTOCOL ARCHITECTURE OVERVIEW

Figure 3.1 shows the tactical MMHS protocol architecture. This protocol solution covers the interfaces TMI-1, TMI-2, TMI-3 and TMI-4 described in chapter 2. TMI-5 that defines the ACP 127 interface is not included in the figure, but is needed if interoperability with ACP 127 systems is required. The ACP 127 gateway specification is given in annex D of STANAG 4406 Edition 1.

This protocol architecture reuses the messaging applications from the strategic STANAG 4406 environment to the greatest extent possible in a tactical environment, while increasing the throughput substantially over reduced capacity tactical links. The protocol architecture is simple, flexible

and the same protocol architecture may be used for simplex, half-duplex and full-duplex connections. The same protocol solution may also be used for EMCON recipients, multicasting and single recipient scenarios. Each of the layers shown in the figure is described in the following sections.

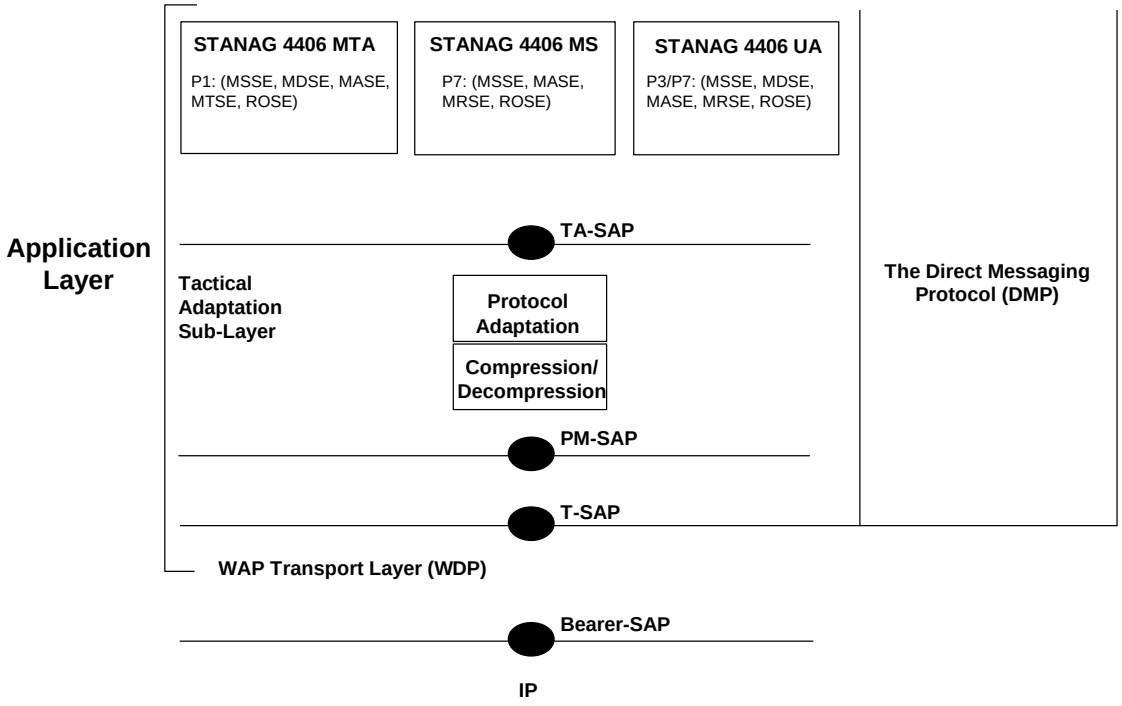


Figure 3.1 – The Tactical MMHS Protocol Architecture

The architecture shows how the protocols and the corresponding service interfaces are related. In the Messaging Sub-Layer the MS and UA use the services of the Tactical Adaptation Sub-Layer, wheras the MTA may use the services of both the Tactical Adaptation Sub-Layer and the Direct Messaging Protocol.

3.1 Document Conventions

This specification uses the same keywords as specified in [ref. 22] for defining the significance of each particular requirement. These words are:

MUST

This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

MUST NOT

This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

SHOULD

This word, or the adjective “RECOMMENDED”, means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT

This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

MAY

This word, or the adjective “OPTIONAL”, means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

3.2 Elements For Layer-to-Layer Communication

3.2.1 Definition of Service Primitives and Parameters

Communication between layers is accomplished by means of service primitives. Service primitives represent, in an abstract way, the logical exchange of information and control between the adjacent layers. Service primitives consist of commands and their respective responses associated with the services requested of another layer. The general syntax of a primitive is:

X-Service.type (Parameters)

where X designates the layer providing the service. Service primitives are not the same as an application programming interface (API) and are not meant to imply any specific method of implementing an API. Service primitives are an

abstract means of illustrating the services provided by the protocol layer to the layer above. The mapping of these concepts to a real API and the semantics associated with a real API are an implementation issue and are beyond the scope of this specification.

3.2.2 Time Sequence Charts

The behaviour of service primitives is illustrated using time sequence charts, which are described in [ref. 21].

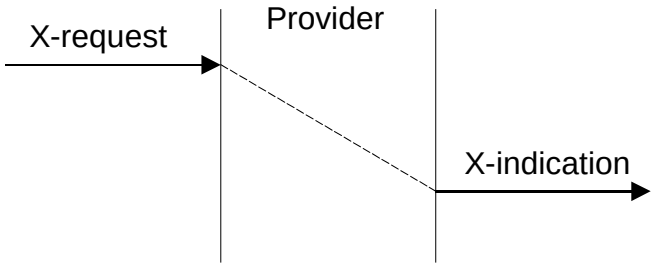


Figure 3.2 – A Non-confirmed Service

Figure 3.2 illustrates a simple non-confirmed service, which is invoked using a request primitive and results in an indication primitive in the peer. The dashed line represents propagation through the provider over a period of time indicated by the vertical difference between the two arrows representing the primitives.

3.2.3 Primitive Types

The primitives types defined in this specification are:

Table 3.3

Type	Abbreviation	Description
request	req	Used when a higher layer is requesting a service from the next lower layer
indication	ind	A layer providing a service uses this primitive type to notify the next higher layer of activities related to the request primitive type of the peer (such as the invocation of the request primitive) or to the provider of the service (such as a protocol generated event)
response	res	A layer uses the response primitive type to acknowledge receipt of the indication primitive type from the next lower layer

Type	Abbreviation	Description
confirm	cnf	The layer providing the requested service uses the confirm primitive type to report that the activity has been completed successfully

3.2.4 Service Parameter Tables

The service primitives are defined using tables indicating which parameters are possible and how they are used with the different primitive types. For example, a simple confirmed primitive might be defined using the following:

Table 3.4

Primitive Parameter	X-primitive			
	req	***ind***	***res***	***cnf***
Parameter 1	M	M(=)		
Parameter 2			O	C(=)

If some primitive type is not possible, the column for it will be omitted. The entries used in the primitive type columns are defined in the following table:

Table 3.5

M	Presence of the parameter is mandatory – it MUST be present
C	Presence of the parameter is conditional depending on values of other parameters
O	Presence of the parameter is a user option – it MAY be omitted
P	Presence of the parameter is a service provider option – an implementation MAY not provide it
–	The parameter is absent
*	Presence of the parameter is determined by the lower layer protocol
(=)	The value of the parameter is identical to the value of the corresponding parameter of the preceding service primitive

In the example table above, *Parameter 1* is always present in *X-primitive.request* and corresponding *X-primitive. indicatio*n. *Parameter 2* MAY be specified in *X-primitive.response* and in that case it MUST be present and have the equivalent value also in the corresponding *X-primitive.confir*m; otherwise, it MUST NOT be present.

4. THE APPLICATION LAYER

4.1 STANAG 4406/X.400 (P1, P3 and P7) (Messaging Sub-Layer)

4.1.1 Use of Application Service Elements and Underlying Services

The X.400 protocols P1, P3 and P7 are used for interconnection between the LMTA, LUA and LMS. The protocols are described in STANAG 4406 Annex A and the X.400 specifications. The following Application Service Elements (ASEs) define the P1, P3 and P7 protocols:

- Message Submission Service Element (MSSE),
- Message Delivery Service Element (MDSE),
- Message Administration Service Element (MASE),
- Message Retrieval Service Element (MRSE),
- Message Transfer Service Element (MTSE),
- Remote Operation Service Element (ROSE).

All of these service elements, which define the messaging functionality of the UA, MTA and MS, are kept unchanged.

These Application Service Elements expect to see the services provided by the connection-oriented Application Layer protocols Reliable Transmission Service Element (RTSE) and Association Control Service Element (ACSE), and the Presentation and Session Layer protocols. None of these connection-oriented protocols are used in this protocol solution in order to reduce the overhead and to be able to use the same system in all tactical MMHS scenarios. Thus one system may be used in all; high latency, simplex, half-duplex, full-duplex, multicast, unicast and EMCON scenarios. The omitted protocols are replaced by the Tactical Adaptation Sub-Layer and the connection-less P_Mul Sub-Layer (see Figure 3.1).

In order to transparently replace the service interface provided by the RTSE , ACSE and the Presentation Layer, the Tactical Adaptation Sub-Layer (described in section 4.2) will provide the protocols in the Messaging Sub-Layer with a service interface similar to the one of the RTSE, and map these connection-oriented services to the actual connection-less services provided by the P_Mul Sub-Layer. This means that the MTAs, UAs, and MSs functionality that are described in STANAG 4406 Annex A and implemented for the strategic MMHS, may be reused. However when used in this tactical profile, we call them LMTAs, LUAs and LMSs respectively to indicate the difference of the use of underlying services from the STANAG 4406 Annex A. The services of the Tactical Adaptaion Sub-Layer is described in section 4.2.

The reliability functionality of the RTSE to handle retransmission and synchronisation is replaced by the P_MUL protocol (for details see section 4.3).

4.1.2 Use of the Responsibility Argument in P1

Since the acknowledgment of the transfer of a message from one LMTA to another is based on the P_Mul functionality, the responsibility argument in P1 must be set to TRUE for all of the recipient addresses. This argument indicates whether the receiving-LMTA shall have the responsibility to either deliver the message to a recipient or to transfer it to another LMTA for subsequent delivery to the recipient. The responsibility flag SHALL be set by the originator's LMTA. (See section 4.3.4 and X.411 section 12.2.1.1.1.6 for details).

4.1.3 Multiple Virtual Associations

Even though the ACSE and the RTSE are omitted, this protocol architecture imposes no limitations on maintaining multiple virtual associations for handling multiple Grade of Delivery queues in the MTA. This functionality is handled above the RTSE level in the MTA and is not affected by the omission of the ACSE and the RTSE. The information about the grade of delivery (or priority) of the virtual association may be further conveyed to the P_Mul APDUs through the Adaptation Sub-Layer (see section 4.2.3.3 for details).

4.1.4 Use of Terminal O/R Address Form

The P1 and P772/P22 address mapping are done independently of each other. Note that this requires equivalent address registers on both sides if the addresses needs to be converted.

4.1.4.1 Use of Terminal O/R Address Form in P1

For tactical receipients the Terminal O/R address form MAY be used instead of Mnemonic address form, with only the network address (IP address) attribute present (as described in section 4.1.4.3).

The IP addresses of the recipients have to be made available to the P_Mul Sub-Layer. If the APDU is encoded before it is delivered to the Tactical Adaptation Sub-Layer, the address information will not be available and must therefore be delivered to this sub layer as a parameter together with the APDU. This is done by the introduction of a new parameter in the TA-TRANSFER.request primitive (see section 4.2.3.3).

4.1.4.2 Use of Terminal O/R Addresses in P772/P22

On origination when sending messages to tactical recipients, the Terminal O/R address form MAY be used instead of Mnemonic address form, with only the network address (IP address) attribute and a terminal-identifier attribute

present (as described in section 4.1.4.3). On origination it is optional which of the Mnemonic or Terminal address forms to use.

4.1.4.3 The X.402 Terminal O/R Address and modifications

LMTAs and LUAs MUST be able to process and understand both Terminal O/R Address Form (*) and Mnemonic O/R Address Form on reception. One of these two forms MUST be used on origination.

A terminal O/R address is one that identifies a user by means of the network address and, if required, the type of his terminal. It may also identify the Management Domain (MD) through which that terminal is accessed. In the case of a Telematic terminal, it gives the terminal's network address and possibly its terminal identifier and terminal type.

A terminal O/R address comprises the following attributes:

1. One network-address (Mandatory on reception) (see (*) below).

2. One terminal-identifier (Mandatory on reception)

3. One terminal-type (Optional).

4. Both one country-name and one administration-domain-name and conditionally one private-domain-name which together identify a MD. (Mandatory on reception)

5. One or more attributes chosen from organization-name, organizational-unit-names, personal-name, unformatted-postal-address and common-name, and conditionally one or more domain-defined attributes, all of which provide additional information to identify the user. (Mandatory on reception)

The private-domain-name and the domain-defined attributes shall be present only if the country-name and administration-domain-name attributes are present.

If used, the Terminal O/R-addresses in this profile MUST contain a network-address (IP-address) and a terminal-identifier (see (*) below).

(*) The recent increase in the use of IP and Internet technology implicate the use of IP network addresses instead of X.121. All data terminals will or should have an IP address, even if there may be a firewall with address mapping to a private addressing scheme. Therefore we mandate the use of the IP address (according to [ref. 20]) as the network address in the terminal O/R address form, even though this is a deviation from the X.402 standard. Note that a Numeric String is not allowed to contain a '.' character. Without

modification, existing X.400 and X.500 products will therefore not allow an IP address to be entered in the network address field of an O/R address. An alternative way of specifying a network address on IP address form is required. This specification therefore mandates that the IP address shall be defined as a domain-defined attribute with Type “IPADDR”.

4.2 The Tactical Adaptation Sub-Layer

The Tactical Adaptation Sub-Layer is needed to provide the expected connection oriented service interface to the protocols at the Messaging sub-layer, and to perform the mapping of these services to the connection less P_Mul protocol. In addition this sub-layer performs operations to increase the throughput, like compression/decompression.

The main concern of this layer is to make it possible to use STANAG 4406 Message Transfer Agents (MTAs), User Agents (UAs) and Message Stores (MSs) over tactical connections while increasing the throughput to a maximum.

Originally the X.400 protocols P1, P3 and P7 use the following ISO/IEC OSI Application Service Elements:

- Remote Operations Service Element (ROSE),
- Message Transfer Service Element (MTSE),
- Message Submission Service Element (MSSE),
- Message Delivery Service Element (MDSE),
- Message Retrieval Service Element (MRSE),
- Message Administration Service Element (MASE).

(See the CCITT X.229 and the ITU-T X.400 standards for details).

All of these service elements make use of the connection oriented Application Service Elements RTSE (Reliable Transfer Service Element) and the ACSE (Association Control Service Element), which further make use of the connection oriented Presentation and Session Layer services.

The RTSE provides a mechanism to recover from communication and end-system failure minimising the amount of retransmissions. However, RTSE and ACSE introduce a lot of overhead that should be avoided in a tactical network. Also they cannot be used in high latency, simplex and EMCON scenarios. We have therefore chosen to use a connectionless protocol stack that includes ACP 142 (P_Mul). ACP 142 will replace the reliability functionality of RTSE, in

that it divides the message into smaller PDUs and ensures retransmission of lost PDUs.

To make this protocol solution transparent for the applications, we need an adaptation layer that maps the connection-oriented service interface to the actual connection-less services provided by ACP 142.

4.2.1 Functionality to Increase the Throughput

The data throughput, over low capacity tactical links, is increased through 3 different means:

1. Use of the short X.402 Terminal O/R Address form in P772/P22 and in P1, instead of the long Mnemonic O/R Address form (see section 4.1.4).

2. Use of compression: The whole APDU (both the content and the envelope) is compressed (see section 4.2.6).

3. Removal of the communication overhead caused by the Reliable Transfer Service Element (RTSE), Association Control Service Element (ACSE) and the OSI Presentation and Session layers. The connection oriented services of the Messaging Sub-Layer (see Figure 2.1) are mapped to the connection less services of the P_Mul Sub Layer.

4.2.2 The Tactical Adaptation Sub-Layer Service Interface

The service interface provided by the Tactical Adaptation Sub-Layer is identical to the one provided by RTSE. The service primitives and parameters are the same as well as the responses the service-user expects to see when invoking a service primitive. One difference is that the primitives have a prefix TA instead of RT. Another is that even though the Tactical Adaptation Sub-Layer provides services similar to the RTSE services, the protocol machine and the functionality are not the same.

Figure 4.1 shows an example of the communication between the Messaging Sub-Layer and the Tactical Adaptation Sub-Layer during the message transmission. When the LMTA with the service element MTSE invokes a TA-OPEN.request, it expects that an APDU is sent to the peer-entity, which issues a TA-OPEN.indication, and that a response/confirmation is returned. What actually happens is that when the MTSE issues a TA-OPEN.request, the Tactical Adaptation Sub-Layer immediately issues a TA-OPEN.confirmation to the MTSE and waits for a TA-TRANSFER.request from the MTSE containing the actual message. The message is transferred using P_Mul and delivered to the Tactical Adaptation Sub-Layer at the peer side. The peer Tactical Adaptation Sub-Layer then issues a TA-OPEN.indication to the MTSE and waits for a TA-OPEN.response before the TA-

TRANSFER.indication is issued. When the P_Mul Data_PDU have been sent to the recipients and a PM_DATA.confirmation is received from the P_Mul Sub-Layer, a TA-TRANSFER.confirmation is issued to the MTSE. Thus the connection establishment services are “faked” and the service-user protocols need not be changed.

It is important to be aware of that TA-TRANSFER.confirmation only acknowledges that the message was sent to the next LMTA (one hop) and is not to be regarded as an end-to-end acknowledgment. A delivery-report from the receiving LMTA (except for LMTAs in EMCON) will confirm that the APDU has been completely transferred and safely stored.

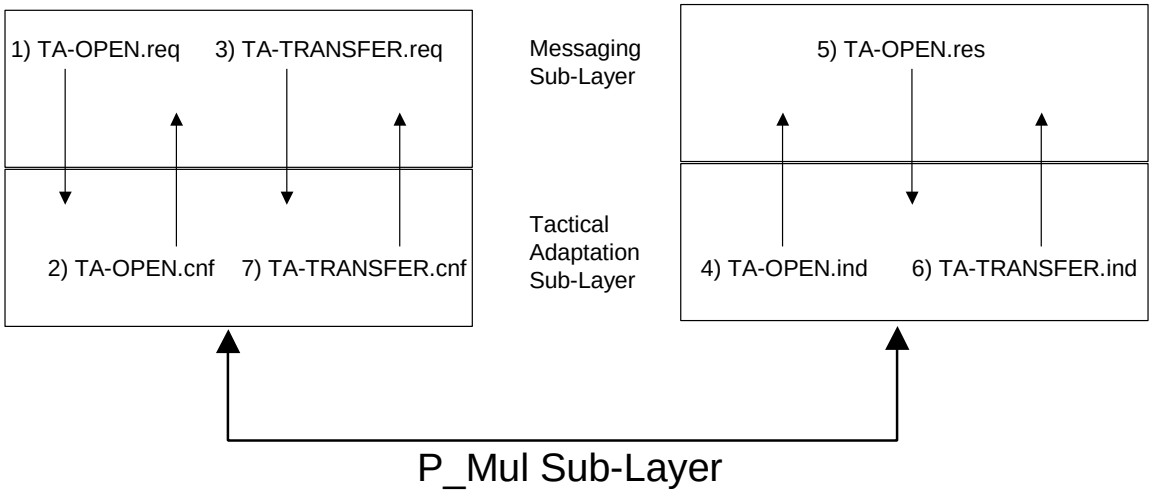


Figure 4.1 – Example of the “Faked” Association Establishment

The services provided by the Tactical Adaptation Sub-Layer are:

- TA-OPEN.request/indication/response/confirmation
- TA-CLOSE.request/indication/response/confirmation
- TA-TRANSFER.request/indication/ confirmation
- TA-TURN-PLEASE.request/indication
- TA-TURN-GIVE.request/indication
- TA-P-ABORT.indication
- TA-U-ABORT.request/indication

4.2.3 The Tactical Adaptation Sub-Layer Service Primitives and Parameters

This service interface may be used to replace the service interface defined by the ITU-T RTSE (X.218) service definitions. The RTSE services mapping specification in X.419 and X.219/X.229 SHALL be followed.

For each of the service primitives, we have only included the parameters of the corresponding RTSE primitives that are Mandatory in X.218 or which are required by the X.419 RTSE services mapping specification for P1, P3 and P7, or by ROSE X.219/X.229.

If these primitives are used to replace the CCITT RTSE (X.218) service interface, the parameter values SHALL be according to the X.419 specification for the use of RTSE (normal mode) or according to the ROSE (CCITT X.219/X.229) specification for the use of RTSE (normal mode).

The primitive sequences are described in section 4.2.5.

4.2.3.1 TA-OPEN

This service replaces the RT-OPEN service defined in the CCITT X.218 specification. The parameters are defined in the X.218 specification.

Table 4.2

Primitive Parameter	**TA-OPEN**			
	req	***ind***	***res***	***cnf***
Dialogue-mode	–	M	–	–
Initial-turn	–	M	–	–
User-data	–	M[1]	–	C(=)
Mode	–	M	–	–
Application context name	–	M	–	C(=)
Presentation context definition list	–	M	–	–
Result	–	–	M	M(=)

1. This parameter is usually used to transfer the arguments of a bind-operation. For this service primitive arguments are NOT allowed because they will not be transferred. The presence of the parameter in the primitive is only to provide the same interface as the CCITT X.218 standard.

4.2.3.1.1 Procedure

When the service-user invokes a TA-OPEN.request primitive, it expects the service to cause an APDU to be sent to the peer-entity to issue a TA-OPEN.indication, and a response/confirmation to be returned. What actually happens is that when the service-user issues a TA-OPEN.request, the Tactical Adaptation Sub-Layer immediately issues a TA-OPEN.confirmation with the Result parameter set to “accepted”, and waits for a TA-TRANSFER.request from the MTSE containing the actual message.

The message is transferred to the Tactical Adaptation Sub-Layer at the peer side. The peer Tactical Adaptation Sub-Layer then issues a TA-OPEN.indication to the service-user with the following parameter default values:

- Mode: “normal mode”
- Application context name: “mts-transfer” for P1, “mts-reliable-access” for P3 and “ms-reliable-access” for P7.
- User-Data: NULL
- Presentation context definition list: The default values are given in X.419 section 7 (P3), section 8 (P7) and section 12 (P1).
- Dialogue-mode: “monologue”

The peer Tactical Adaptation Sub-Layer then waits for a TA-OPEN.response. If the Result parameter in the response primitive is “accepted” the TA-TRANSFER.indication is issued, otherwise a PM-U-ABORT.request is issued. Thus the connection establishment services are “faked” and the service-user protocols do not need to be changed.

4.2.3.2 TA-CLOSE

This service replaces the RT-CLOSE service defined in the CCITT X.218 specification. The parameters are defined in the X.218 specification. No parameters are transferred.

Table 4.3

Primitive Parameter	TA-CLOSE			
	req	***ind***	***res***	***cnf***
User-data	–	M[1]	–	M[1]

Primitive Parameter	TA-CLOSE			
	req	***ind***	***res***	***cnf***
Reason	–	M[2]	–	M[2]

1. This parameter is used by ROSE (see CCITT X.219). The User-data parameter SHALL be set to NULL if ROSE is used. For other ASEs it SHALL not be used.

2. This parameter is used by ROSE (see CCITT X.219) and SHALL be set to “normal” if ROSE is used.

4.2.3.2.1 Procedure

When the Tactical Adaptation Sub-Layer receives a TA-CLOSE.request, it immediately issues a TA-CLOSE.confirmation primitive to the service-user. On the peer side, the TA-CLOSE.response from the service-user SHALL be ignored.

4.2.3.3 TA-TRANSFER

This service replaces the RT- TRANSFER service defined in the CCITT X.218 specification. The parameters are defined in the X.218 specification except for the parameters “List-Of-Destination-Entries”, which is a list of IP addresses of the receiving nodes and the Priority parameter which indicates the grade of Delivery. These parameters are only used to convey this information to the P_Mul Sub-Layer and are therefore not present in the indication primitives.

Table 4.4

Primitive Parameter	TA-TRANSFER		
	req	***ind***	***cnf***
List-Of-Destination-Entries	M	–	
Priority	M	–	
APDU	M	M(=)	–
Transfer-time [1]	M	–	–
Result	–	–	M

1. The transfer-time should be set long enough for the message to be transferred over the low throughput connection.

4.2.3.3.1 Procedure

This service is used to transfer the message to the peer side (next LMTA). It is a confirmed service, but is not symmetric in the sense that there is no TA-TRANSFER.response primitive. It is important to be aware that a TA-TRANSFER.confirmation is issued after a PM_DATA.confirmation primitive is received from the P_Mul Sub-Layer (see section 4.3.3.1), and only acknowledges that the message was sent to the next LMTA (one hop). It is not to be regarded as an end-to-end acknowledgment. A delivery-report from the receiving LMTA (except for LMTAs in EMCON) will confirm that the message has been completely transferred and safely stored.

4.2.3.4 TA-TURN-PLEASE

This service replaces the RT- TURN-PLEASE service defined in the CCITT X.218 specification. The parameters are defined in the X.218 specification.

Table 4.5

Primitive Parameter	TA-TURN-PLEASE	
	req	***ind***
Priority	–	–

4.2.3.4.1 Procedure

This service is used by the service-user to ask for the ”turn” which it must possess before it may use the TA-TRANSFER service. When receiving the TA-TURN-PLEASE.request primitive, the Tactical Adaptation Sub-Layer immediately issues the TA-TURN-GIVE.indication to the service-user. The corresponding APDU is never sent to the peer-entity. This service is included in order not to change the message applications, which expect this service to be present.

4.2.3.5 TA-TURN-GIVE

This service replaces the RT- TURN-GIVE service defined in the CCITT X.218 specification. This service has no parameters.

Table 4.6

Primitive	TA-TURN-GIVE

Parameter	*req*	*ind*
–	–	–

4.2.3.5.1 Procedure

This service is used by the service-user to give the “turn” to the requesting service-user. When receiving the TA-TURN-PLEASE.request primitive, the Tactical Adaptation Sub-Layer immediately issues the TA-TURN-GIVE.indication to the service-user. The TA-TURN-GIVE.request primitive is just ignored. This service is included in order not to change the message applications, which expect this service to be present.

4.2.3.6 TA-P-ABORT

This service replaces the RT-P-ABORT service defined in the CCITT X.218 specification. This service has no parameters.

Table 4.7

Primitive Parameter	TA-P-ABORT
	ind
–	–

4.2.3.6.1 Procedure

This service is used by the Tactical Adaptation Sub-Layer to report to the service-user that a local error has occurred that has caused an abortion of the message delivery process.

4.2.3.7 TA-U-ABORT

This service replaces the RT-P-ABORT service defined in the CCITT X.218 specification. This service has no parameters.

Table 4.8

Primitive Parameter	TA-U-ABORT	
	req	*ind*

Primitive Parameter	TA-U-ABORT	
	req	*ind*
–	–	–

4.2.3.7.1 Procedure

This service is used by the service-user to notify the peer-entity that an error has occurred that has caused the message delivery process to abort.

4.2.4 Use of The P_Mul Sub-Layer Services

The Tactical Adaptation Sub-Layer uses the following service primitives provided by the P_Mul Sub-Layer;

- PM-DATA.request/indication/confirmation,
- PM-P-ABORT.indication,
- PM-U-ABORT.request/indication

See section 4.3.2 for a description of the services.

4.2.5 Service Primitive Sequences

The table below shows the TA-service primitive sequences. The left column shows incoming primitives to the Tactical Adaptation Sub-Layer from the service user or the P_Mul Sub-Layer. The right column shows primitives issued by the Tactical Adaptation Sub-Layer as a response to the incoming primitive.

Table 4.9

Incoming primitive	Issued primitive(s)
TA-OPEN.request	TA-OPEN.confirmation
PM-DATA.indication	TA-OPEN.indication
TA-OPEN.response	TA-TRANSFER.indication, TA-CLOSE indication
TA-CLOSE request	TA-CLOSE.confirmation
TA-CLOSE response	Ignored
TA-TRANSFER request	PM-DATA.request
PM-DATA.confirmation(*)	TA-TRANSFER.confirmation

Incoming primitive	Issued primitive(s)
TA-TURN-PLEASE.request	TA-TURN-GIVE.indication
TA-TURN-GIVE.request	ignored
PM-P-ABORT.indication	TA-P-ABORT.indication
TA-U-ABORT.request	PM-U-ABORT.request
PM-U-ABORT.indication	TA-U-ABORT.indication

(*) This is not a symmetric service in the sense that there is no TA-TRANSFER.response primitive. A PM-DATA.confirmation primitive is issued when the P_Mul Sub-Layer sends the Data_PDU to the recipients.

- The TA-OPEN request primitive is mapped onto the TA-OPEN.confirmation primitive, which fools the service user to believe that an association is established. The Tactical Adaptation Sub-Layer then waits for a TA-TRANSFER.request to be issued.

- The TA-TRANSFER.request primitive is mapped onto the PM-DATA.request primitive.

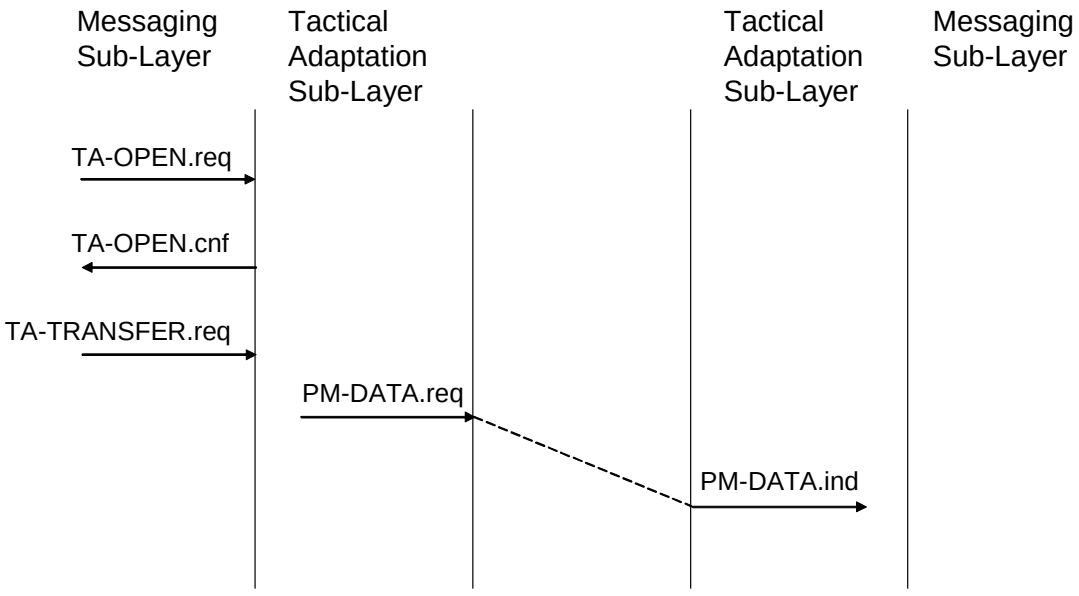


Figure 4.10 – Transfer of a Message

- The TA-CLOSE.request primitive is mapped onto a TA-CLOSE.confirmation primitive to fool the service user to believe that an association is terminated.

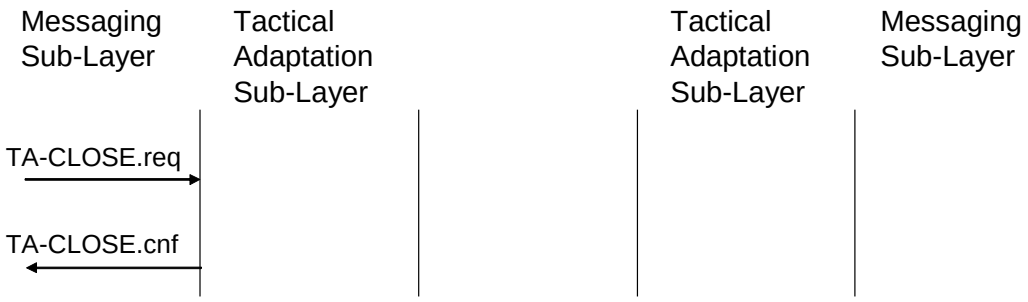


Figure 4.11 – Reception of a TA-CLOSE.req

- The PM-DATA.indication primitive is mapped onto the TA-OPEN.indication to fake an association establishment for the service user. The Tactical Adaptation Sub-Layer then waits for a TA-OPEN.response before it issues the TA-TRANSFER.indication primitive followed by a TA-CLOSE.indication primitive to fool the service user to believe that an association is requested to be terminated (note: There is no TA-TRANSFER.response primitive in order to be conformant to X.218).

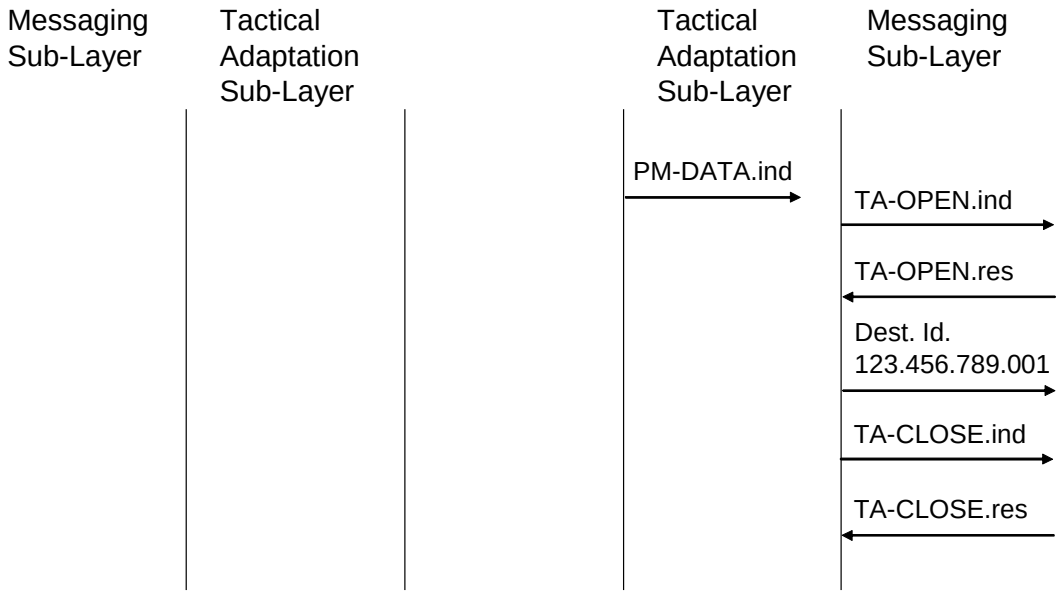


Figure 4.12 – The Reception of a PM-DATA.indication Primitive

- The TA-CLOSE.response primitive is just ignored and causes no action.

- A PM-DATA.confirmation primitive is issued from the P_Mul Sub-Layer when the Data_PDU is sent to the recipients. The primitive is mapped onto a TA-TRANSFER.confirmation primitive. It is important to be aware of that this only acknowledges that the message was sent to the next LMTA (one hop) and is not to be regarded as an end-to-end acknowledgment. For end-to-end acknowledgment, each message SHALL be acknowledged by a delivery-report from the receiving LMTA (except for LMTAs in EMCON), which then confirms that the APDU has been completely transferred and safely stored.

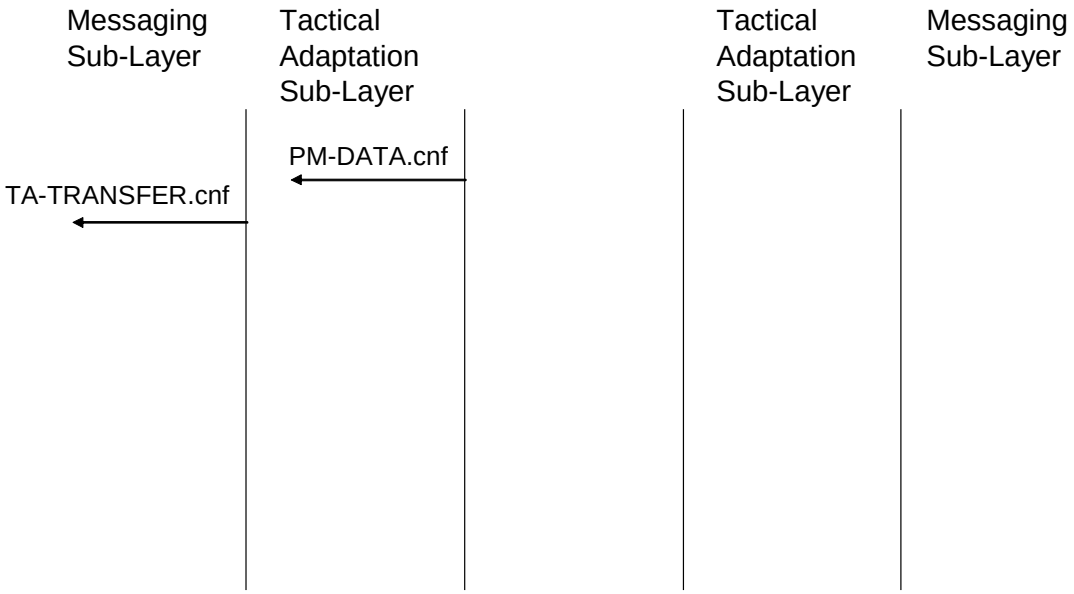


Figure 4.13 – Reception of a PM-DATA.confirmation

- The TA-TURN-PLEASE.request primitive is mapped onto a TA-TURN-GIVE.indication primitive to fool the service user to believe that he has been given the send-token by the peer-entity.

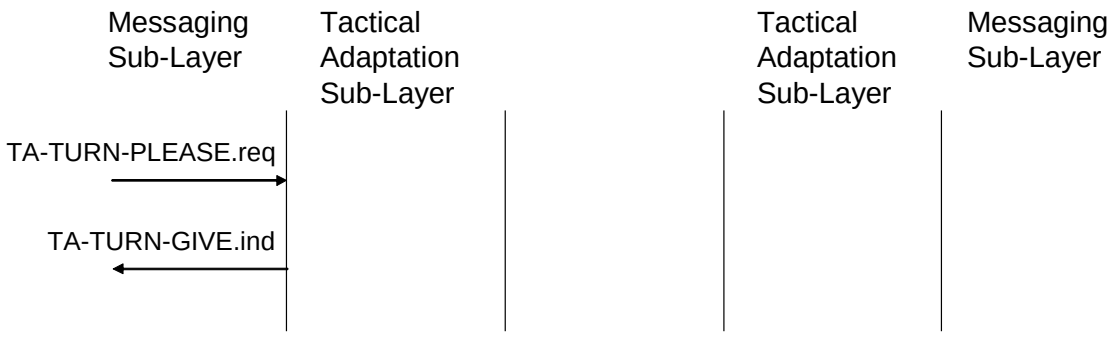


Figure 4.14 – Reception of a TA-TURN-PLEASE.req

- A TA-TURN-GIVE.request is just ignored.

- A PM-P-ABORT.indication primitive indicates an error from the P_Mul Sub-layer and causes a TA-P-ABORT.indication to be issued.

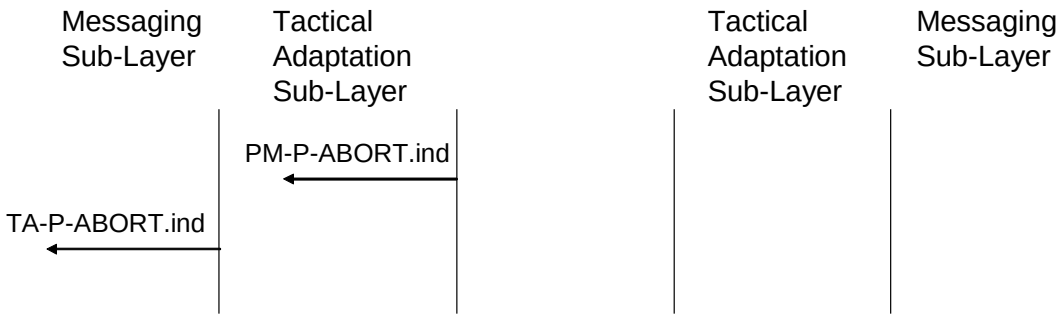


Figure 4.15 – Reception of a PM-P-ABORT.indication Primitive

- A TA-U-ABORT.request primitive is mapped onto a PM-U-ABORT.request primitive. The Tactical Adaptation Sub-Layer may receive the TA-U-ABORT.request primitive at any time.

- A PM-U-ABORT.indication is mapped onto a TA-U-ABORT.indication. The Tactical Adaptation Sub-Layer may issue the TA-U-ABORT.indication primitive at any time.

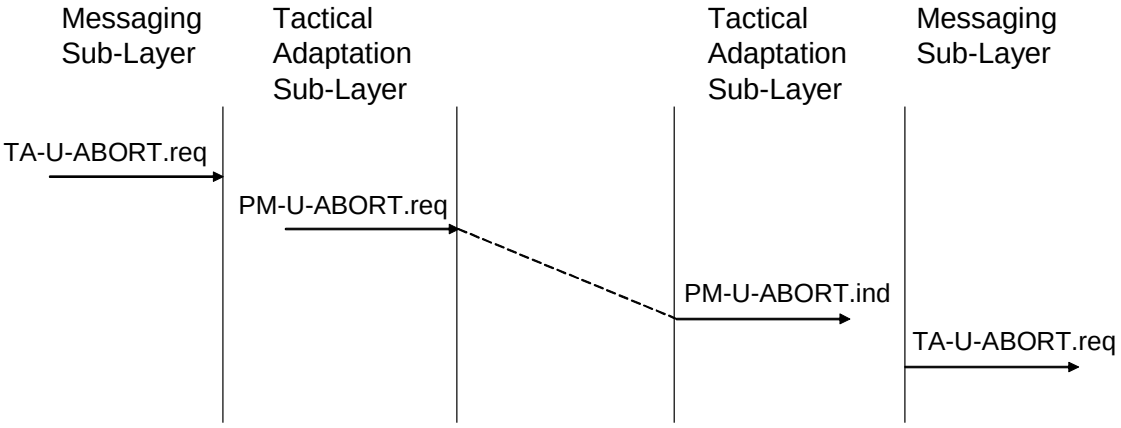


Figure 4.16 – Reception of a TA-U-ABORT.request

- The Tactical Adaptation Sub-Layer may issue the TA-P-ABORT.indication primitive at any time whenever en error occurs in the sub-layer.

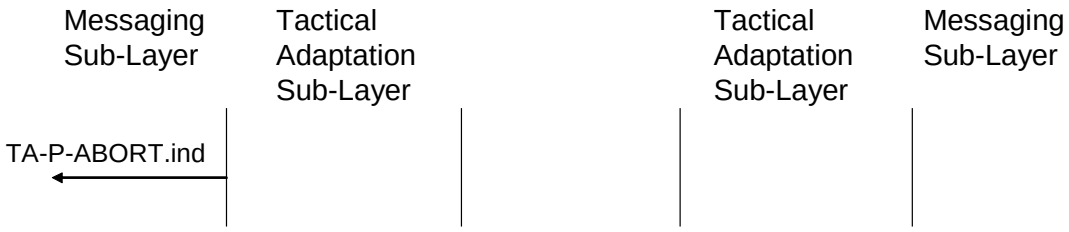


Figure 4.17 – Emission of a TA-P-ABORT.indication

4.2.6 Compression

Compression shall be performed at the Tactical Application Sub-layer in order to compress the whole APDU (both the content and the envelope). In this section we have defined a compression wrapper called “Compressed Data Type”. This Compressed Data Type allows for any OCTET STRING to be compressed, and shall be used to compress the whole APDU and not just the message content. The reason for compressing the whole APDU is that the P1, P3 and P7 envelopes add a substantial overhead to the message.

4.2.6.1 The Compressed Data Type

The Compressed Data Type (CDT) consists of content of any type that is compressed using a specified algorithm. The following object identifier identifies the Compressed Data Type:

```
id-mmhs-CDT ID ::= { iso(1) identified-organization(3) nato(26)
stanags(0)
      mmhs(4406) object-identifiers(0) id-mcont(4) 2 }
```

The Compressed Data Type are defined by the following ASN.1 type:

```
DEFINITIONS ::=
BEGIN

CompressedData ::= SEQUENCE {
      compressionAlgorithm    CompressionAlgorithmIdentifier,
      compressedContentInfo   CompressedContentInfo }

CompressionAlgorithmIdentifier ::= CHOICE {
      algorithmID-ShortForm   [0]   AlgorithmID-ShortForm,
      algorithmID-OID   [1]   OBJECT IDENTIFIER }
```

```
AlgorithmID-ShortForm ::= INTEGER  {
      zlibCompress (0) }

CompressedContentInfo ::= SEQUENCE {
      CHOICE {
            contentType-ShortForm   [0]   ContentType-
ShortForm,
            contentType-OID   [1]   OBJECT IDENTIFIER
      },
      compressedContent [0]   EXPLICIT OCTET STRING }

ContentType-ShortForm ::= INTEGER {
      unidentified (0),
      external (1),     -- identified by the object-identifier
                        -- of the EXTERNAL content
      p1 (2),
      p3 (3),
      p7 (4) }

END
```

The fields of Compressed Data Type have the following meaning:

compressionAlgorithm **(dynamically mandatory)** defines the compression algorithm to be used. The algorithm may be defined using either an INTEGER value (which is **mandatory** to support both on origination and reception) or an OBJECT IDENTIFIER (which is **optional** on origination and **mandatory** on reception).

compressedContentInfo **(dynamically mandatory)** defines the type of content that is compressed. The type of content may be indicated using either an INTEGER value (which is **mandatory** to support both on origination and reception) or an OBJECT IDENTIFIER (which is **optional** on origination and **mandatory** on reception).

compressedContent **(dynamically mandatory)** is the compressed content.

4.2.6.2 Use of the Compressed Data Type

To ensure interoperability, this section defines how the X.400 content and envelope shall be encoded and conveyed within the Compressed Data Type.

The compressed X.400 envelope shall be placed in the *compressedContent* field of the *CompressedContentInfo* element. Note that this X.400 envelope SHALL be ASN.1 and BER encoded. The object identifier for the envelope type of the compressed X.400 envelope SHALL be placed in either the *contentType-ShortForm* or the *contentType-OID* field of the *CompressedContentInfo* element.

An illustration of this required wrapping convention is shown in Figure 4.18.

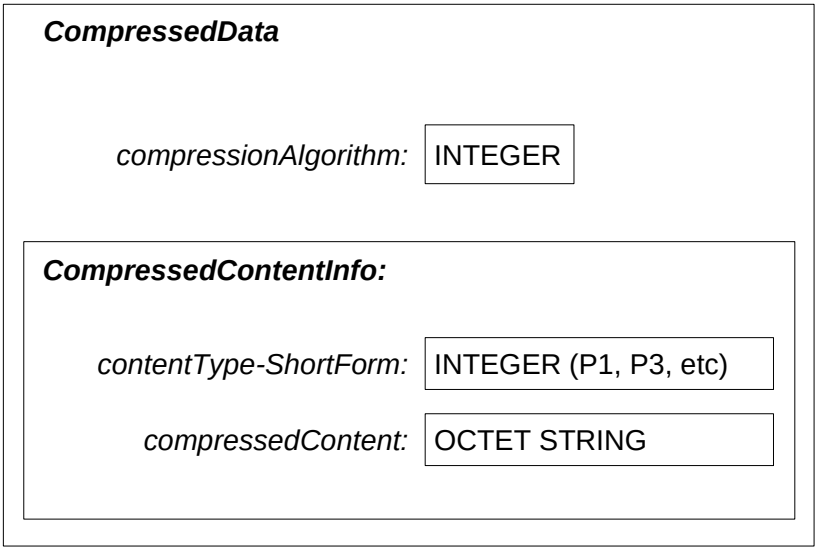


Figure 4.18 – Protocol wrapping

Analysis described in [ref. 2] indicates that full compression of the APDU gives the best result if BER [ref. 3] is used instead of PER [ref. 4] to encode the ASN.1 structures of both P772/P2 and P1. BER encoding SHALL therefore be used before compression.

4.2.6.3 Compression Algorithm

This specification mandates the support of the compression algorithm ZLIB [ref. 18] [ref. 19], which is free of any intellectual property restrictions and has a freely available, portable and efficient reference implementation. The following object identifier identifies ZLIB:

```
id-alg-zlibCompress OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840)
      rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) alg(3) 8 }
```

The INTEGER reference SHOULD however be used and the integer value 0 identifies this algorithm.

4.3 The P_Mul Sub-Layer

P_Mul (ACP 142) [ref. 13] is an application layer protocol that is designed to be used together with other messaging protocols (e.g. STANAG 4406/X.400) to handle EMCON (Emission Control) conditions and multicast communication techniques. It may also be used as a provider of a reliable acknowledged, connectionless application-layer service, even if the multicast of EMCON functionality is not used. It operates directly above a connectionless transport

layer and may operate in simplex, half-duplex or full-duplex mode. P_Mul is thus a flexible protocol that may be used in all of the interfaces shown in Figure 2.1.

The ITU-T X.400 application layer protocols are based on the service support from connection oriented protocols at the top four OSI layers for reliable data transport between application entities. This means that the standard X.400 application cannot be used over simplex connections, or to send messages to users under EMCON conditions, as they are. When EMCON conditions apply, some nodes are only allowed to receive data and are not allowed to acknowledge them.

EMCON conditions are handled in P_Mul by allowing acknowledgments from the receiving nodes to be missing for a rather long time. The sending node has to know which of the receiving nodes that are in EMCON, and retransmissions are performed to increase the probability that the nodes in EMCON receive the message.

P_Mul uses an encapsulation technique where the P_Mul PDU types are wrapped around another Message Transfer Protocol (e.g. x.400 P1). P_Mul replaces layers 5, 6 and parts of layer 7 of the OSI protocol stack, and should be run on top of a connectionless transport-layer protocol.

By making use of the broadcast properties of a connectionless protocol stack, one message may be sent to N recipients instead of sending the message N times. To handle the problem of packet flooding in broadcast networks, a multicast addressing scheme has been invented.

If there are any conflicts between this Annex and ACP 142, this annex takes precedence.

The complete specification of the P_Mul protocol with procedures are given in ACP 142 [ref. 13].

4.3.1 Protocol Data Units

The Tactical Task Force of the Combined Communications and Electronics Board (CCEB) has released P_Mul as ACP 142 [ref. 13].

The ACP 142 specification describes two groups of Protocol Data Units (PDUs). One group consists of those PDUs needed for the transfer of the message. These PDUs are:

- Address_PDU
- Data_PDU
- Ack_PDU

- Discard_PDU

The other group consists of PDUs for dynamic configuration of multicast groups. The concept of multicast groups is introduced to reduce the network load in situations when the sender has exact knowledge about the addresses of the recipients. The objective is that the multicast transmission of a message shall involve as few as possible, by forming groups of transmitting and receiving nodes within a multicast network. The Application Protocol Data Units (APDUs) used to manage multicast groups are:

- **Request_PDU** – for requesting a multicast group
- **Reject_PDU –** for rejecting a multicast group
- **Release_PDU** – for releasing a multicast group
- **Announce_PDU** – announcing a multicast group

These four PDUs will be used by a P_Mul management function and not by the data transfer service user. The specification of the P_Mul management function is out of scope for this Annex. For more details about the P_MUL protocol and the PDUs, see ACP 142 [ref. 13].

4.3.2 The P_Mul Sub-Layer Service Interface

In order to make P_Mul more independent of the protocols using it and to make P_Mul fit into the layered model described in this STANAG, we have defined a service interface with a set of service primitives to be invoked by the P_Mul user.

We have defined the following services for the P_Mul Sub-Layer:

- PM-DATA.request/indication/confirmation(*)
- PM-P-ABORT.indication
- PM-U-ABORT.request/indication
- PM-REQUEST.request/indication
- PM-REJECT.request/indication
- PM-RELEASE.request/indication
- PM-ANNOUNCE.request/indication

(*) This is not a symmetric service, a PM-DATA.confirmation primitive is issued when the PDU is sent to the receipients.

The PM-DATA, PM-P-ABORT and PM-U-ABORT services are used by the Tactical Adaptation Sub-Layer for data transfer and error handling.

The PM-REQUEST, PM-REJECT, PM-RELEASE and PM-ANNOUNCE services are not used by the Tactical Adaptation sub-layer, but by a P_MUL management function directly in order to set up and organise multicast groups. The reason for defining these four service primitives, is to clearly separate the P_Mul protocol machine from the P_Mul Management function which may be integrated with the user application. How to handle multicast groups is a local implementation matter and some implementations may not include these primitives for handling multicast groups.

Figure 4.19 shows the layered structure of the protocol profile where we see that some of the P_Mul services are used by the Tactical Adaptation Sub-layer and some services are used by the P_Mul Management Function to handle the multicast groups.

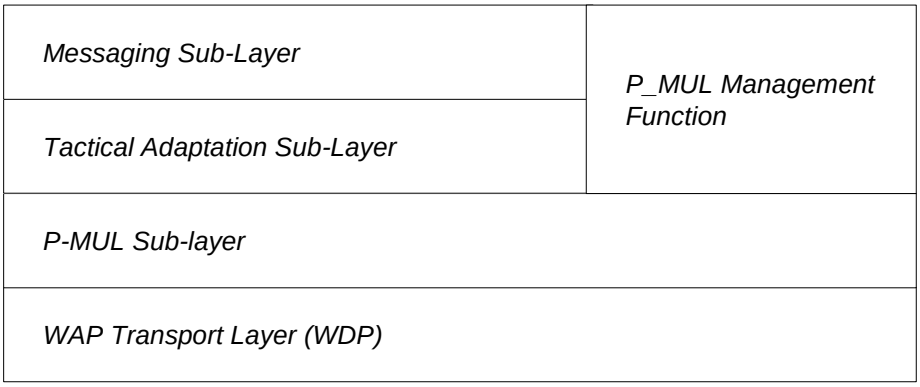


Figure 4.19 – The P_Mul Sub-Layer Interfaces Both the Tactical Adaptation Sub-layer and a P_Mul Management Function

4.3.3 The P_Mul Sub-Layer Service Primitives and Parameters

4.3.3.1 PM-DATA

This service is used to send data from the originator to the receiver.

When the P_Mul Sub-Layer receives a PM-DATA.request primitive, it will contain the message to be sent and the sub-layer SHALL create and send Address_PDUs and Data_PDUs according to the protocol description in ACP 142. See section 4.3.4 for a description on how to map addresses from X.400 to P_Mul.

The PM-DATA.indication primitive is issued by the P_Mul Sub_Layer to the Tactical Adaptation Sub-Layer when all of the Data_PDUs belonging to a

message are received, and an Ack_PDU is sent back indicating no missing Data_PDUs. See ACP 142 for description of the protocol.

A PM-DATA.confirmation primitive, is issued by the P_Mul Sub-Layer to the Tactical Adaptation Sub-Layer when the Data_PDU is sent to the recipients. This is not a symmetric service in that there is no PM-DATA.response primitive. See ACP 142 for description of the protocol. It is important to be aware of that this only acknowledges that the message was sent to the next LMTA (one hop) and is not to be regarded as an acknowledgment for the delivery of the message. For end-to-end acknowledgment, each message SHALL be acknowledged by a delivery-report from the receiving LMTA (except for LMTAs in EMCON), which then confirms that the APDU has been completely transferred and safely stored.

Table 4.20

Primitive Parameter	**PM-DATA**			
	req	***ind***	***res***	***cnf***
Priority	M	M(=)	–	M(=)
MessageID	M	M(=)	–	M(=)
Expiry_Time	O	O(=)	–	–
List_of_Destination_Entries	M	P	–	–

4.3.3.1.1 Priority

This parameter is to be mapped to the priority fields of the Address_PDU and the Data_PDU. See ACP 142 for description of the field and the semantic.

4.3.3.1.2 MessageID

This MMIdentifier is to be derived from the seconds since 00:00:00 1.1.1970 - Unix Time, as defined in ACP 142.

4.3.3.1.3 Expiry_Time

This parameter is to be mapped to the Expiry_Time field of the Address_PDU. See ACP 142 for description of the field and the semantic.

4.3.3.1.4 List_of_Destination_Entries

This parameter is to be mapped to the List_of_Destination_Entries field of the Address_PDU. See ACP 142 for description of the field and the semantic.

4.3.3.2 PM-P-ABORT

The PM-P-ABORT.indication primitive is issued by the P_Mul Sub_Layer to the Tactical Adaptation Sub-Layer if an error occurs in the sub-layer and the processing of the message has to be aborted. This primitive is also issued when the T-Derror.indication primitive is received from the WAP WDP layer.

Table 4.21

Primitive Parameter	PM-P-ABORT	
	req	***ind***
Reason_Code	–	M

4.3.3.2.1 Reason_Code

The Reason_Code is a parameter indicating the reason for the abortion of the message processing caused by the P_Mul Sub-Layer. The Reason_Code may have the following values:

2. Error receiving a message
3. Error sending a message
4. Unknown error

4.3.3.3 PM-U-ABORT

The reception of a PM-U-ABORT.request indicates that an error has occurred in the above sub-layers, which has caused the message processing to be aborted. The P_Mul Sub-Layer shall create and send a Discard_Message_PDU according to the protocol description in ACP 142.

The PM-U-ABORT.indication primitive, is issued by the P_Mul Sub_Layer to the Tactical Adaptation Sub-Layer when a Discard_Message_PDU is received. See ACP 142 for description this PDU.

Table 4.22

Primitive Parameter	PM-U-ABORT	
	req	***ind***
Priority	M	M(=)

Primitive Parameter	PM-U-ABORT	
	req	*ind*
MessageID	M	M(=)

4.3.3.3.1 Priority

This parameter is to be mapped to the priority field of the Discard_Message_PDU. See ACP 142 for description of the field and the semantic.

4.3.3.3.2 MessageID

This MMIdentifier is to be derived from the seconds since 00:00:00 1.1.1970 - Unix Time, as defined in ACP 142.

4.3.3.4 PM-REQUEST

This service is used to notify other transmitting nodes about a selected address to be used to send a message to a multicast-group (see ACP 142 for details).

When the P_Mul Sub-Layer receives a PM-REQUEST.request primitive it shall create and send a REQUEST_PDU according to the protocol description in ACP 142.

The PM-REQUEST.indication primitive, is issued by the P_Mul Sub-Layer to the P_MUL Management Function when a REQUEST_PDU is received. See ACP 142 for description of the protocol.

Table 4.23

Primitive Parameter	PM-REQUEST	
	req	*ind*
SourceID	M	M(=)
MessageID	M	M(=)
Multicast_Group	M	M(=)

4.3.3.4.1 SourceID

This parameter is to be mapped to the SourceID field of the REQUEST_PDU. See ACP 142 for description of the field and the semantic.

4.3.3.4.2 MessageID

This MMIdentifier is to be derived from the seconds since 00:00:00 1.1.1970 - Unix Time, as defined in ACP 142.

4.3.3.4.3 Multicast_Group

This parameter is to be mapped to the Multicast_Group field of the REQUEST_PDU. See ACP 142 for description of the field and the semantic.

4.3.3.5 PM-REJECT

This service is used in response to the PM-REQUEST.request service to notify the sender that the selected address is occupied (see ACP 142 for details).

When the P_Mul Sub-Layer receives a PM-REJECT.request primitive it shall create and send a REJECT_PDU according to the protocol description in ACP 142.

The PM-REJECT.indication primitive is issued by the P_Mul Sub-Layer to the P_MUL Management Function when a REJECT_PDU is received. See ACP 142 for description of the protocol.

Table 4.24

Primitive Parameter	PM-REJECT	
	req	***ind***
SourceID	M	M(=)
MessageID	M	M(=)
Receipient_Address	M	M(=)

4.3.3.5.1 SourceID

This parameter is to be mapped to the SourceID field of the REJECT_PDU. See ACP 142 for description of the field and the semantic.

4.3.3.5.2 MessageID

This MMIdentifier is to be derived from the seconds since 00:00:00 1.1.1970 - Unix Time, as defined in ACP 142.

4.3.3.5.3 Receipient_Address

This parameter is to be mapped to the Multicast_Group field of the REJECT_PDU. See ACP 142 for description of the field and the semantic.

4.3.3.6 PM-RELEASE

This service is used to release a multicast address, which will then be available for others to use (see ACP 142 for details).

When the P_Mul Sub-Layer receives a PM- RELEASE.request primitive it shall create and send a RELEASE_PDU according to the protocol description in ACP 142.

The PM- RELEASE.indication primitive is issued by the P_Mul Sub-Layer to the P_MUL Management Function when a RELEASE_PDU is received. See ACP 142 for description of the protocol.

Table 4.25

Primitive Parameter	PM-RELEASE	
	req	***ind***
SourceID	M	M(=)
MessageID	M	M(=)
Multicast_Group	M	M(=)

4.3.3.6.1 SourceID

This parameter is to be mapped to the SourceID field of the RELEASE_PDU. See ACP 142 for description of the field and the semantic.

4.3.3.6.2 MessageID

This MMIdentifier is to be derived from the seconds since 00:00:00 1.1.1970 - Unix Time, as defined in ACP 142.

4.3.3.6.3 Multicast_Group

This parameter is to be mapped to the Multicast_Group field of the RELEASE_PDU. See ACP 142 for description of the field and the semantic.

4.3.3.7 PM-ANNOUNCE

The PM-ANNOUNCE service is used to announce the allocation of a requested multicast address to the receiving nodes.

When the P_Mul Sub-Layer receives a PM-ANNOUNCE.request primitive it shall create and send one or more ANNOUNCE_PDUs according to the protocol description in ACP 142.

The PM-ANNOUNCE.indication primitive is issued by the P_Mul Sub-Layer to the P_MUL Management Function when a ANNOUNCE_PDU is received. See ACP 142 for description of the protocol.

Table 4.26

Primitive Parameter	PM-ANNOUNCE	
	req	***ind***
SourceID	M	M(=)
MessageID	M	M(=)
Expiry_Time	O	O(=)
Multicast_Group_Address	M	M(=)
List_of_Destination_IDs	M	M(=)

4.3.3.7.1 SourceID

This parameter is to be mapped to the SourceID fields of the ANNOUNCE_PDU. See ACP 142 for description of the field and the semantic.

4.3.3.7.2 MessageID

This MMIdentifier is to be derived from the seconds since 00:00:00 1.1.1970 - Unix Time, as defined in ACP 142.

4.3.3.7.3 Expiry_Time

This parameter is to be mapped to the Expiry_Time field of the ANNOUNCE_PDU. See ACP 142 for description of the field and the semantic.

4.3.3.7.4 Multicast_Group_Address

This parameter is to be mapped to the Multicast_Group_Address field of the ANNOUNCE_PDU. See ACP 142 for description of the field and the semantic.

4.3.3.7.5 List_of_Destination_IDs

This parameter is to be mapped to the List_of_Destination_IDs field of the ANNOUNCE_PDU. See ACP 142 for description of the field and the semantic.

4.3.4 Address Mapping and Routing

In section 4.1.4 we described the use of terminal form O/R addressing using IP addresses as network addresses instead of X.121 addresses. ACP 142 defines the use IP addresses to identify the recipients.

There is a certain overlap concerning routing and addressing functionality in X.400 and P_Mul. This leaves us with several possible options when configuring and implementing an X.400 system on top of a P_Mul network.

If there is only a single recipient of the message, the mapping of the IP address from the terminal O/R address form is straightforward. To make use of the multicasting functionality in P_Mul, the address mapping and routing is a bit more complex.

This section illustrates three different scenarios for how to combine the routing functionality of X.400 with the addressing and multicasting facilities provided by P_Mul.

The illustrations show a sample network consisting of 4 LMTAs, all connected by a P_Mul network. An X.400 message is to be sent from LMTA-A to two recipients Recipient-B and Recipient-C (located on LMTA-B and LMTA-C, respectively). In the discussion below, the concept "System unit" means a logical representation of another LMTA or Access Unit, known in the local LMTA routing information table and used as a basis for routing decisions.

4.3.4.1 Routing Scenario 1

Scenario one (see Figure 4.27) is based on the traditional X.400 routing concept and provides a clear distinction between X.400 and P_Mul functionality. Each LMTA connected to the P_Mul network is represented by a separate System Unit. This means that the routing procedure executed by LMTA-A will conclude that the two recipients are located on different LMTAs and thus create two different copies of the message, one for LMTA-B and one for LMTA-C.

Note that this scenario does not at all exploit the multicasting features of P_Mul because each of the two message copies will in turn be unicasted by the common P_Mul-network. However, we still utilise the other throughput-increasing functions of the Tactical Adaptation Sub-Layer and the P_Mul layers as well as the EMCON functionality. This method SHOULD NOT be used if the message is to be sent to more than one MTA

4.3.4.2 Routing Scenario 2

Scenario two (see Figure 4.28) takes advantage of the P_Mul broadcast functionality by using one common System Unit for the entire P_Mul network. Thus, the LMTA routing procedure will only make one copy of the message, which covers all recipients located on units connected to the P_Mul network.

There are at least two issues concerning the implementation of this scheme as opposed to scenario 1.

The first issue is how to decide the Destination_ID's of the P_Mul Address_PDU's. In scenario 1 it is straightforward to fill in these Destination_ID's since they will simply be the (single) IP-address of each of the system units to which the message will be sent.

In scenario 2 the Destination_ID's must be decided based on the P1 recipients of the message. The LMTA or TIA therefore needs to consult address book information in order to find the Terminal form OR-name (IP-address) of each addressee and a list of Destination_ID's must be built and used to fill in the Address_PDU.

The second issue is that due to the underlying multicast mechanisms, LMTA-B and LMTA-C will receive exactly the same copy of the message. This means that the responsibility flag of the P1 addresses will have the same values upon reception at both LMTAs.

So, unless special precautions are taken, LMTA-C will try to handle both Recipient-B and Recipient-C. Based on its routing table, LMTA-C will find out that Recipient-B is located on LMTA-B and therefore creates a new copy of the message that it sends to LMTA-B over the P_Mul network. Consequently, each LMTA will receive several copies of each message.

To avoid this, the LMTA MUST include a mechanism that turns off the responsibility flag for certain recipients before the incoming messages are passed to the LMTA routing procedure. The LMTA has to check each recipient IP-address against it's own address and turn off the responsibility flag unless they match.

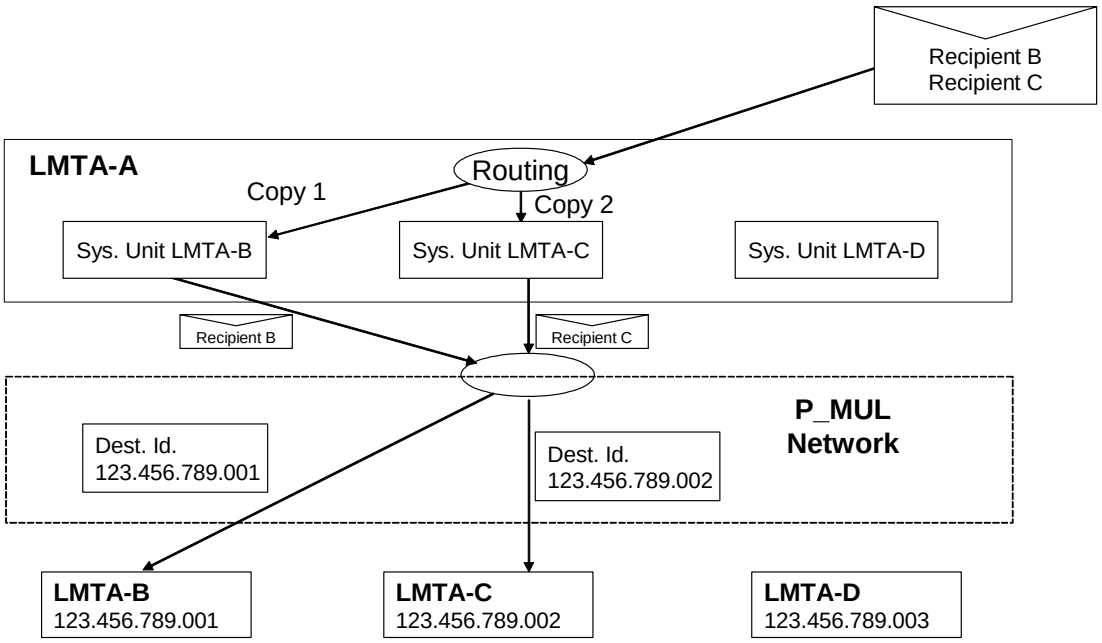


Figure 4.27 – No Utilization of the P_Mul Multicast Functionality

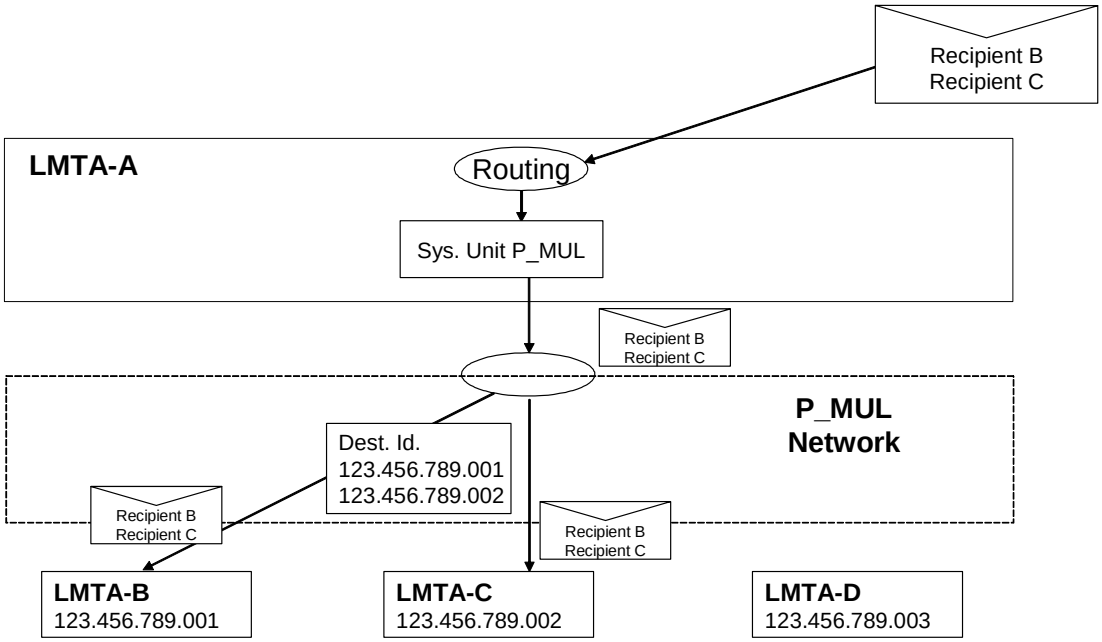


Figure 4.28 – Utilization of the P_Mul Multicast Functionality

4.3.4.3 Routing Scenario 3 (Routing via intermediate LMTAs)

Routing Scenario 2 will not work in a more complex network environment where LMTA-C serves as at gateway towards a P_Mul network for other LMTAs, say LMTA-E and LMTA-F. (i.e. LMTA-C does not only handle messages to local recipients). In this case the IP-address of the recipients will not match the IP-address of LMTA-C.

In this case the message SHALL be sent to the intermediate LMTA with the IP address of the intermediate LMTA as the only destination entry in PM-DATA.req primitive (this address is not included as one of the recipients in the P1 or P772 addresses). The addresses of the real recipients SHALL be given as recipients in the P1 envelope. The intermediate LMTA will then be able to use Routing Scenario 2 to multicast the message to the real recipients based on the address information in P1. If there are several intermediate LMTAs, this routing procedure needs to be repeated for each intermediate LMTA. Only the last intermediate LMTA will use Routing Scenario 2 to multicast to the real recipients.

LMTA-C may also be a gateway into a strategic network where all recipient addresses not necessarily have been assigned a network address. The routing procedure above SHALL therefore be used to reach the intermediate strategic-tactical gateway (or TIA) and the strategic routing mechanism SHALL be used to route further into MTAs in the strategic system based on the O/R addresses in the P1 envelope.

4.3.5 Use of The WAP WDP Services

The WAP WDP (Wireless Application Protocol – Wireless Datagram Protocol) [ref. 16] defines a user service interface consisting of the following service primitives (see section 6.2 for a detailed description):

- T-DUnitdata.request/indication
- T-DError.indication

The T-DUnidata SHALL be used for transmission of all of the PDUs crated by the P_Mul Sub-Layer. The parameters are described in section 6.2.1 and the UDP port numbers to be used are defined in ACP 142 Annex B.

The T-DError.indication primitive SHALL be mapped onto the PM-P-ABORT.indication primitive. The Error Code parameter is of local significance only and SHOULD be mapped to the Reason Code of the PM-P-ABORT.indication primitive.

5. THE DIRECT MESSAGING PROFILE (DMP)

5.1 Introduction

This chapter describes the Direct Message Profile for optimised transfer of time-critical short messages. DMP is optimized for use with a reliable bearer service. Checksum and retransmission mechanisms may be activated when using unreliable bearer services.

5.1.1 Background

The DMP is a response to the need for message-based communbications in tactical scenario using low bandwidth channels, where connectivity may be available irregularly, and where there is a need for interoperation with existing strategic systems.

The current standard (STANAG 4406 Annex E) is designed for this type of environment. The focus of Annex E has been to significantly reduce the transmission overhead, to support multicast media, and to retain complete interoperability with strategic networks. This is in fact very successful, as shown below. However, in some cases the reduction in overhead is still not sufficient.

Several measurements have been performed using various media (HF and VHF radio, wire-based tactical networks). The focus has been to identify the protocol overhead when exchanging short messages (i.e. messages with from 10 to 10000 bytes of user data). This overhead results in a number of additional bytes to transfer (adding to the transmission delay), and a number of protocol handshake operations (resulting in changes of direction, which is expensive on some types of radio links). The following table shows some best-case measurement results.

Table 5.29

Protocol	Overhead (bytes)	Changes of direction
STANAG 4406 Annex C	2700	8
STANAG 4406 Annex E (TMI-1)	700	2
DMP	20	0

5.1.2 Highlights

The DMP provides a very significant reduction in overhead. This is achieved at the cost of functionality – only the required minimum of functions is available, and DMP should thus only be used when bandwidth is the major factor.

DMP is an MTA to MTA protocol, and is interoperable with STANAG 4406. This allows the exchange of messages with the strategic domain. This implies that it is also possible to have multi-hop connections using different protocols on different hops.

DMP is very bandwidth-efficient. This allows DMP to be used for time-critical messages even when using low-bandwidth channels (e.g. HF radio).

The DMP uses existing bearers (such as IP), and only puts moderate demands on processing power. This allows DMP to be implemented on almost any platform, including hand-helds and laptops.

DMP should be seen as a supplement to STANAG 4406 Annex E, for use when bandwidth is more important than full functionality.

5.2 Related Documents

[1] STANAG 4406 Ed 2

5.3 Terminology

5.3.1 Abbreviations and acronyms

Directory Service	A service that provides translation between DMP and STANAG 4406 addressing schemes.
Direct Address	Identifies a specific recipient using a DMP-specific binary number
DMP	Direct Message Profile
DMP Address	An address conveyed by DMP, encoded using Direct or Extended Encoding
IP	Internet Protocol
MTA	Message Transfer Agent
MTU	Maximum Transfer Unit
UDP	User Datagram Protocol
VC	Virtual Cicuit (as used in ITU-T X.25)

5.4 General

With reference to STANAG 4406 Annex E, Figure 2.1, DMP is an alternative tactical interface between two LMTAs. This interface differs from TMI-1 by using a highly optimized and restricted functionality Messaging Sub-Layer, and a simplified Tactical Adaptation Sub-Layer. The table below shows the protocols used for this interface. The different layers and protocols referred to in the table are described in STANAG 4406 Annex E and in this document.

Table 5.30

Layer	Protocol	Reference

Messaging Sub-Layer (P772 and P22)	DMP “Content”	Chapters 5.7.3, 5.7.4, 5.7.6, 5.7.7, and 5.7.8
Message Transfer Layer (P1)	DMP "Envelope"	Chapters 5.7.1, 5.7.2 and 5.7.5
Tactical Adaptation Sub-Layer	Compressed Data Type	Chapter 4.2.6
Transport Layer	WAP WDP	STANAG 4406 Annex E clause 6

DMP is optimized for sending small messages that fits into one network layer packet. The maximum network layer packet size depends on the protocol carrying the message (including heading information, application layer addressing, as well as the user data). At the receiving MTA, sufficient information is available to reconstruct a complete STANAG 4406 message. DMP requires the source message to comply with a set of criteria in order to be able to reconstruct the complete message at the receiving MTA. Non-complying messages must either be sent using other protocols, or rejected at the sending MTA.

DMP can be used in several scenarios, including:

- DATA packet on established X.25 VC (unlimited message size, network handles reassembly)
- CALL packet as part of Fast Select User Data (message size limited to 128 byte)
- UDP packet on IP network (message size limited by UDP datagram size, i.e. (64kb – 8) = 65527)
- UDP/IP over X.25 (message size limited by UDP datagram size, i.e. (64kb – 8) = 65527)
- RFC1006/RFC2126 over TCP/IP (message size limited to (64kb – 4) = 65531)

Optimal message size is determined by the MTU of the network between sender and receiver.

A complete message is sent as a single object, with no need for a return channel. This implies that DMP works best over a reliable communications bearer. DMP supports a checksum and an acknowledgement mechanism to be used when a reliable channel cannot be provided.

5.4.1 Protocol mapping

The mapping supports Message, Delivery Report, Non-Delivery Report, Receipt Notification, Non-Receipt Notification and Other Notification objects, in addition to an Acknowledgement object.

Each object to be sent must be converted to a DMP object. This conversion covers a small subset of available attributes. If the source object contains attributes or attribute values that cannot be converted, then the conversion fails, and the object cannot be sent as a DMP object. Note that some attributes are "converted" by just deleting them, and in some cases including a flag stating that this happened.

On reception, an object must be constructed from the received data. This includes setting default or configurable values for attributes not included in the DMP object.

5.4.2 Addressing

DMP assumes that the underlying network carries sufficient address information to identify the receiving MTA. This allows DMP to include application level addresses only. Each such Direct Address is allocated as a binary number that must be unique within the actual use of DMP, i.e. each valid recipient is identified with a number.

The Direct Address is represented as a 19-bit number, making room for up to 524288 unique addresses. The Directory Service must provide a mapping between the OR-names and the corresponding numbers. How this is done is outside the scope of this document, but one possibility is to use a DomainDefinedAttribute (e.g. DD.Type="dpaddr", DD.Value=number). Extended addressing is used when other addressing forms are required.

Normally, DMP assumes that each P1 addressee corresponds directly to one P22/P772 addressee. Extended addressing is used when the P1 address differs from the P22/P772 address (e.g. Redirection, Address Lists).

Note that the Direct Addresses introduce one or more new addressing domains, where a domain includes a number of originators/recipients each having a domain-specific Direct Address. A given originator/recipient may be part of multiple domains, and may thus have multiple Direct Addresses. A mechanism must exist to ensure that the communicating parties have the same perception of this domain, i.e. to maintain the correspondence between originators/recipients and the Direct Address according to which domain is applicable. The mechanism is outside the scope of this document, but possibilities include relating the DMP domain to a range of IP addresses, and using the Directory Service.

5.4.3 Reports and notifications

DMP is a non-confirmed service. It is still possible to request delivery reports and receipt notifications. These services are requested per recipient as for STANAG 4406.

5.4.4 Error handling

When using a reliable subnet, there is no need for error checking. The following mechanisms are available when an unreliable subnet is used:

- Use the optional checksum and retransmission mechanisms. This allows transmission errors to be detected and recovery to be effected.

- Encapsulate the message within an RFC 1006 TPKT. This provides delimiting the object in cases where the underlying subnet does not preserve PDU boundaries (e.g. TCP).

Any detected errors shall lead to discarding the received data. This should also result in logging the event.

Enabling use of checksum also enables use of Acknowledgement objects (see ch. 5.6.1.3). The receiving MTA shall perform checksum verification. If checksum verification fails, a negative acknowledgement shall be returned to the sender. Otherwise a positive acknowledgement shall be returned.

5.4.5 Time and time synchronization

DMP uses timestamps for several fields. These timestamps are coded in a way that requires fairly well synchronized clocks. The SubmissionTime field is coded into 15 bits as follows:

- Compute (number of seconds since 01 Jan 1970 12:00 UTC divided by two) modulo 32760.

The “divided by 2” term above causes the time resolution to be 2 seconds. The time can be specified within an 18 hour 12 minute window. If a message cannot be transferred to the receiving MTA within the 18 hour 12 minute window, DMP is unable to determine the correct SubmissionTime upon reception. Any Reports, Notifications and DMP Acknowledgements must be received within this 18 hour 12 minute window to ensure correct handling (since this window is also the maximum guaranteed lifetime of message identifiers, see chapter 5.7.9.1). At the receiving MTA, part of this window shall be used to detect (and compensate for) loss of time synchronization between the communicating MTAs as described in chapter 5.7.9.5.1. Other timestamps are coded in such a way that they are dependent on the SubmissionTime field as follows:

- When sending, the current time is compared to the SubmissionTime field. If these times differ by 4 seconds or more, the difference is encoded into the TimeDifference field.

- DTG and ExpiryTime values are calculated as offsets from the submission time.

- When receiving, the transmission delay is calculated as the difference between the current time and the received SubmissionTime value (taking account of the TimeDifference field if present).

- The DTG and ExpiryTime values are converted to actual time.

For this handling to work correctly, the communicating MTAs should have their clocks synchronized to within 30 seconds. If the clock difference exceeds this limit, there may be problems with automatic actions related to time fields (such as time surveillance at the receiver based on the DTG, handling based on expiry time).

5.4.6 Flow control and error recovery

DMP supports two flow controls schemes; local and end-to-end flow control. The former is based on ICMP Source Quench, and the latter is implemented using Acknowledgement objects. Error recovery is based on checksums and retransmissions.

5.4.6.1 Local flow control

Local flow control based on ICMP Source Quench shall be supported. Typically, a router will send a Source Quench message when the buffer capacity is exhausted. A DMP implementation receiving a Source Quench message shall reduce outgoing traffic. As a minimum, outgoing traffic shall be suspended for a configurable delay.

5.4.6.2 End-to-end flow control

Certain applications may require that messages are delivered in sequential order. As an option, DMP supports message transfer with a configurable maximum number of un-acknowledged messages (i.e using a “window” mechanism). This shall be supported using the Acknowledgement mechanism as follows:

- When sending, checksum shall be used. This will activate the Acknowledgment mechanism at the receiving MTA.

- At the receiver, an Acknowledgement shall be returned.

- When the Acknowledgement is received at the sender, the message has been successully sent.

- The sending MTA shall ensure that the “next” message is not sent before the current message has been acknowledged (i.e. “window size” 1), or if too many messages are un-acknowledged (i.e. “window size” N”).

Note that activating checksums also activates the error recovery mechanism described in section 5.4.6.3 below.

5.4.6.3 Error recovery

Error detection is based on the use of checksums, and recovery is based on retransmissions. When activated, the following shall be done at the sending MTA:

- When sending the message for the first time, the ChecksumPresent flag shall be set, the Checksum shall be calculated and inserted, the retransmission timer shall be started, and the retransmission count shall be set to 0. The message shall be stored for later retransmission.

- If receiving a negative acknowledgement, the retransmission timer shall be stopped, and the retransmission counter shall be incremented. If the counter is less than a configurable maximum value, the retransmission timer shall be restarted, and the message shall be retransmitted. If the retransmission counter has reached the maximum value, the message transfer has failed, and the event shall be logged.

- If receiving a positive acknowledgement, the message transfer is successful. The retransmission timer shall be stopped.

- If the retransmission timer expires, the retransmission counter shall be incremented. If the counter is less than the maximum value, the retransmission timer shall be restarted, and the message shall be retransmitted. If the retransmission counter has reached the maximum value, the message transfer has failed, and the event shall be logged.

The following shall be done at the receiving MTA:

- If the message was received with an incorrect checksum, or some other error was detected, a negative

acknowledgement shall be returned. The event may be logged.

- If the message was received with a correct checksum, and no other errors were detected, a positive acknowledgement shall be returned. If this was the first copy of this message (i.e. the DMP MessageIdentifier is not found in the local table described in chapter 5.7.9.1), it shall be regarded as successfully received. Otherwise, a previous acknowledgement was probably lost, and the message is ignored except for returning a positive acknowledgement.

- If receiving a copy of a previously received message, the acknowledgement to return is determined as follows:

    - If the message was previously received correctly, a positive acknowledgement shall be returned (even if errors are detected with the current copy).

    - Otherwise, the akcnowledgement shall reflect the status of the current copy.

5.4.7 Multicast and broadcast

DMP can be used over multicast and broadcast bearers. When used over broadcast media, the acknowledgement mechanism must be disabled. This will also disable the checksum, which requires that the bearer provides a reliable channel (in the sense that data integrity is protected).

With both multicast and broadcast bearers, the receiving MTA must inspect the address field to determine if the message is actually destined for that MTA. This will normally require additional data in the system directory (since an MTA may be responsible for delivery to recipients at other MTAs in addition to any local recipients at the MTA).

5.4.8 Reserved bits and values

The DMP specification includes several bits and values that are marked as “Reserved”. Bits shown as “Reserved” shall always be set to 0 on transmission, and shall be ignored on reception. Values shown as “Reserved” shall not be generated on transmission, and shall result in a decoding failure on reception.

5.5 Address representation

In general, DMP will only transfer addressees for which the receiving MTA is responsible, i.e. each message copy when using DMP will contain a subset of

the initially entered addressees. This is a trade-off between providing complete information, and reducing bandwidth. An optional coding form allows other addressees to be transferred where required.

Each application level address is encoded in one of 2 different ways. Every address in a message must use the same encoding. The encoding is identified in the message header. For best performance, the Direct Encoding should be used. Extended Encoding must be used in the following cases:

- At least one address cannot be represented as a Direct Address
- The P1 address is different from the corresponding P22/P772 address (e.g. for Address Lists)
- Option: Recipients for which the destination MTA is not responsible shall be transported

When converting a message to DMP, any address not convertible to one of the specified encodings shall cause conversion to fail. The encodings are defined in the following sections.

5.5.1 Address encoding

5.5.1.1 Direct Encoding

This encoding requires the P1 address to be the same as the P22/P772 address (i.e. only one address can be encoded for each recipient). Every address must be converted to a Direct Address, and only recipients for which the receiving MTA has delivery responsibility can be transferred.

5.5.1.1.1 Direct Originator Encoding

When using Direct Encoding, the Originator field is coded as follows:

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
OrigExt1	DirectAddress (bits 6-0)						

If OrigExt1 = 1:

OrigExt2	Reserved	DirectAddress (bits 12-7)

If OrigExt2 = 1:

Reserved	DirectAddress (bits 18-13)

Figure 5.31 – Direct Originator Encoding Structure

5.5.1.1.2 Direct Recipient Encoding

When using Direct Encoding, each Recipient field is coded as shown below. If multiple recipients are present, each recipient is encoded using Basic Encoding, and the recipient fields are concatenated.

The encoding of the different fields is specified in section 5.5.2 below.

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
RecipientNumber (bits 3-0)				ReportRequest1		NotificationRequest1	
ActionAddr	DirectAddress (bits 6-0)						
If ReportRequest1 = 11:							
ReportRequest2	RecipientNumber (bits 9-4)						
If ReportRequest2 = 11:							
ReportRequest3	Reserved	RecipientNumber (bits 14-10)					
If NotificationRequest1 = 11:							
NotificationRequest2	DirectAddress (bits 12-7)						
If NotificationRequest2 = 11:							
NotificationRequest3	DirectAddress (bits 18-13)						

Figure 5.32 – Direct Recipient Encoding Structure

5.5.1.2 Extended Encoding

This encoding allows the P1 address to be different from the P22/P772 address (i.e. both P1 and P22/P772 addresses can be encoded for each recipient). Addresses need not be converted to Direct Addresses, and recipients for which the receiving MTA does not have delivery responsibility can optionally be transferred.

Note that in some cases more than 2 addresses may be present for the same recipient (e.g. for a message subjected to both Redirection and DL Expansion). This is not supported by DMP, and information will be lost in such cases.

5.5.1.2.1 Extended Originator Encoding

When using Extended Encoding, the Originator field is coded as follows:

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
AddressForm			Reserved				
If AddressForm = 000, a Direct Address follows.							

Extended Direct Address (see section 5.5.2.7 below)

If AddressForm = 010, an Extended Address follows.

Extended Address (see section 5.5.2.8 below)

Figure 5.33 – Extended Originator Encoding Structure

5.5.1.2.2 Extended Recipient Encoding

The recipient field is coded as follows:

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
AddressForm			ActionAddr	ReportRequest3		NotificationRequest3	
RecNumExt	RecipientNumber (bits 6-0)						

If RecNumExt = 1:

RecipientNumber (bits 14-7)

If AddressForm = x0x, a Direct Address follows. This is the P1 address if AddressForm is 000 or 10x, and the P22/P772 address if AddressForm is 001.

Extended Direct Address (see section 5.5.2.7 below)

If AddressForm = x1x, an Extended Address follows. This is the P1 address if AddressForm is 010 or 11x, and the P22/P772 address if AddresForm is 011.

Extended Address (see section 5.5.2.8 below)

If AddressForm = 1x0, a Direct Address follows. This is the P22/P772 address.

Extended Direct Address (see section 5.5.2.7 below)

If AddressForm = 1x1, an Extended Address follows. This is the P22/P772 address.

Extended Address (see section 5.5.2.8 below)

Figure 5.34 – Extended Recipient Encoding Structure

The encoding of the different fields is specified in section 5.5.2 below.

5.5.2 Address subfields

Each address format defines a number of subfields as shown above. The encoding of these subfields is defined in the following sections.

5.5.2.1 ActionAddr

This bit is set to 1 if the recipient is an Action/To recipient, and set to 0 if the recipient is an Info/Cc recipient.

5.5.2.2 AddrExt1 and AddrExt2

These fields indicate whether the DirectAddress continues into the following byte. See section 5.5.2.7 for details.

5.5.2.3 AddressForm

This field applies to Extended Encoding only, and defines the type and format of an originator or recipient address. The values are:

000	P1 address only, Direct Address
001	P22/P772 address only, Direct Address (see below)
010	P1 address only, Extended Address
011	P22/P772 address only, Extended Address (see below)
100	P1 and P22/P772 addresses, both Direct Addresses
101	P1 and P22/P772 addresses, P1 is Direct Address and P22/P772 is Extended Address
110	P1 and P22/P772 addresses, P1 is Extended Address and P22/P772 is Direct Address
111	P1 and P22/P772 addresses, both Extended Addresses

When used for an originator, only the values 000 and 010 are valid. Other values are reserved.

When used for a recipient, the above values all refer to recipients for which the receiving MTA has delivery responsibility. The values 000 and 010 shall be used if the P1 address is identical to the P22/P772 address. The values 100, 101, 110 and 111 shall only be used if the P1 and P22/P772 addresses are different.

As an option, the values 001 and 011 can be used for conveying recipient addresses for which the receiving MTA does not have delivery responsibility. Note that in this case, no P1 address is constructed by the receiving MTA.

5.5.2.4 AddressLength

This field gives the length of the Extended Address (excluding the bytes containing the length field itself). For AddressType 000, the length can be from 2 to 1023 bytes. For AddressType 001, the length shall always be 6.

The AddressLength shall be encoded in the minimum number of bits (unspecified higher significant bits are assumed to be 0).

5.5.2.5 AddressType and AddressTypeExt

This field defines the type of Extended Address. The defined values are:

000	ASN.1 BER-encoded OR-name
001	ASN.1 PER-encoded OR-name
010-110	Reserved for other address types
111	Extension mark, see below

For AddressType, the value 111 indicates that the AddressLength field contnues into the following byte, and the Address Type is found in the AddressTypeExt field.

For AddressTypeExt, the value 111 is “Reserved”, and shall not be used.

5.5.2.6 DirectAddress

The DirectAddress identifies a specific Originator or Recipient as a binary number. The DirectAddress shall be encoded in the minimum number of bits (unspecified higher significant bits are assumed to be 0). The DirectAddress is encoded as 7, 13 or 19 bits.

5.5.2.7 Extended Direct Address

This field represents a Direct Address using Extended Encoding. The following format is used:

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
AddrExt1	DirectAddress (bits 6-0)						
If AddrExt1 = 1:							
AddrExt2	Reserved	DirectAddress (bits 12-7)					
If AddrExt2 = 1:							
Reserved	DirectAddress (bits 18-13)						

Figure 5.35 – Extended Direct Address Structure

5.5.2.8 Extended Address

This field represents an Extended Address using Extended Encoding. The following format is used:

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
AddressType			AddressLength (bits 4-0)				
If AddressType = 111:							
AddressTypeExt			AddressLength (bits 9-5)				
If AddressType = 000, or AddressType = 111 and AddressTypeExt = 000:							
ASN.1 BER-encoded OR-name (2 to 1023 bytes)							
If AddressType = 001, or AddressType = 111 and AddressTypeExt = 001:							
ASN.1 PER-encoded OR-name (1 to 1023 bytes)							

Figure 5.36 – Extended Address Structure

5.5.2.9 NotificationRequest1, NotificationRequest2 and NotificationRequest3

These fields show the types of notifications requested for this recipient. Values are:

00 None

01 Non-Receipt Notification

10 Receipt Notification (also implies Non-Receipt Notification)

11 Extension mark, see below

For NotificationRequest1 and NotificationRequest2, the value 11 indicates that the DirectAddress field continues into a following byte, and the notification requests are specified in NotificationRequest2 or NotificationRequest3 respectively.

For NotificationRequest3, the value 11 is “Reserved”, and shall not be used.

5.5.2.10 OrigExt1 and OrigExt2

These fields indicate whether the originator DirectAddress continues into the following byte. See section 5.5.1.1.1 for details.

5.5.2.11 RecNumExt

This field indicates whether the RecipientNumber field continues into the following byte. See section 5.5.1.2.2 for details.

5.5.2.12 RecipientNumber

The original P1 recipient number must be transferred in DMP. This is a number with a theoretical range of 1 through 32767. The encoding uses 4, 10 or 15 bits (Direct Encoding) or 7 or 15 bits (Extended Encoding) to represent the recipient number, with the RecipientNumber encoded as an offset from the previous recipient. The first recipient is assumed to follow a recipient with number 0 (noting that the first STANAG 4406 recipient has number 1).

If the P1 address is not present (i.e. AddressForm is set ot 001 or 011), the RecipientNumber shall be set to 0.

The following algorithm can be used for encoding the value. The resulting value shall be encoded in the minimum number of bits (i.e. 4, 10 or 15 bits):

```
prev_rec_num = 0;
for each recipient:
        value = recipient_number – 1 – prev_rec_num;
        prev_rec_num = recipient_number;
```

This algorithm can be used for decoding the value:

```
prev_val = 0;
for each recipient:
        recipient_number = value + 1 + prev_val;
        prev_val = recipient_number;
```

5.5.2.13 ReportRequest1, ReportRequest2 and ReportRequest3

These fields show the types of reports requested for this recipient. Values are:

00	None
01	Non-Delivery Report
10	Delivery Report (also implies Non-Delivery Report)
11	Extension mark, see below

For ReportRequest1 and ReportRequest2, the value 11 indicates that the RecipientNumber field continues into a following byte, and the report request is encoded in ReportRequest2 and ReportRequest3 respectively.

For ReportRequest3, the value 11 is “Reserved”, and shall not be used.

5.5.3 Examples

Some examples of address encodings are given. In a complete example, the address encoding would be specified in the message heading.

Action recipient, number 1, direct address 0x35b, Delivery Report and Receipt Notification requested:

00001011	Recipient offset 0, Delivery Report requested, address needs more than 6 bits
11011101	Action recipient, address bits 6 to 0
10000110	Receipt Notification requested, address bits 12 to 7

Info recipient, number 2, P1 direct address 0x2cf, using Extended Encoding (not all recipients use same format), Delivery Report requested, no notifications requested:

00001000	Address form 0 (P1 DMP Address), info recipient, delivery report requested, no receipt requested
00000001	Recipient offset 1
11001111	Address needs more than 6 bits, address bits 6 to 0
00000101	Address bits 13 to 7

5.6 Message structure

Each message is structured as an envelope (including a variable-size address field), followed by the message content. The content includes a message heading and the message body. The complete message is delimited by the bearer service (see chapter 5.4.4 for bearer services that do not preserve PDU boundaries). Any message that cannot be converted into this format shall cause the conversion to fail. Note that some fields are discarded during conversion (e.g. the P1 content-identifier).

5.6.1 Message envelope encoding

5.6.1.1 Envelope structure

The message envelope provides values for the entire message as follows, with the encoding of the different fields specified in section 5.6.1.2 below:

<table>
<tr><td>bit 7</td><td>bit 6</td><td>bit 5</td><td>bit 4</td><td>bit 3</td><td>bit 2</td><td>bit 1</td><td>bit 0</td></tr>
<tr><td colspan="5">ProtocolIdentifier</td><td colspan="3">ProtocolVersion</td></tr>
<tr><td colspan="3">HopCount</td><td>Address-Encoding</td><td>Checksum-Present</td><td colspan="3">ContentType</td></tr>
</table>

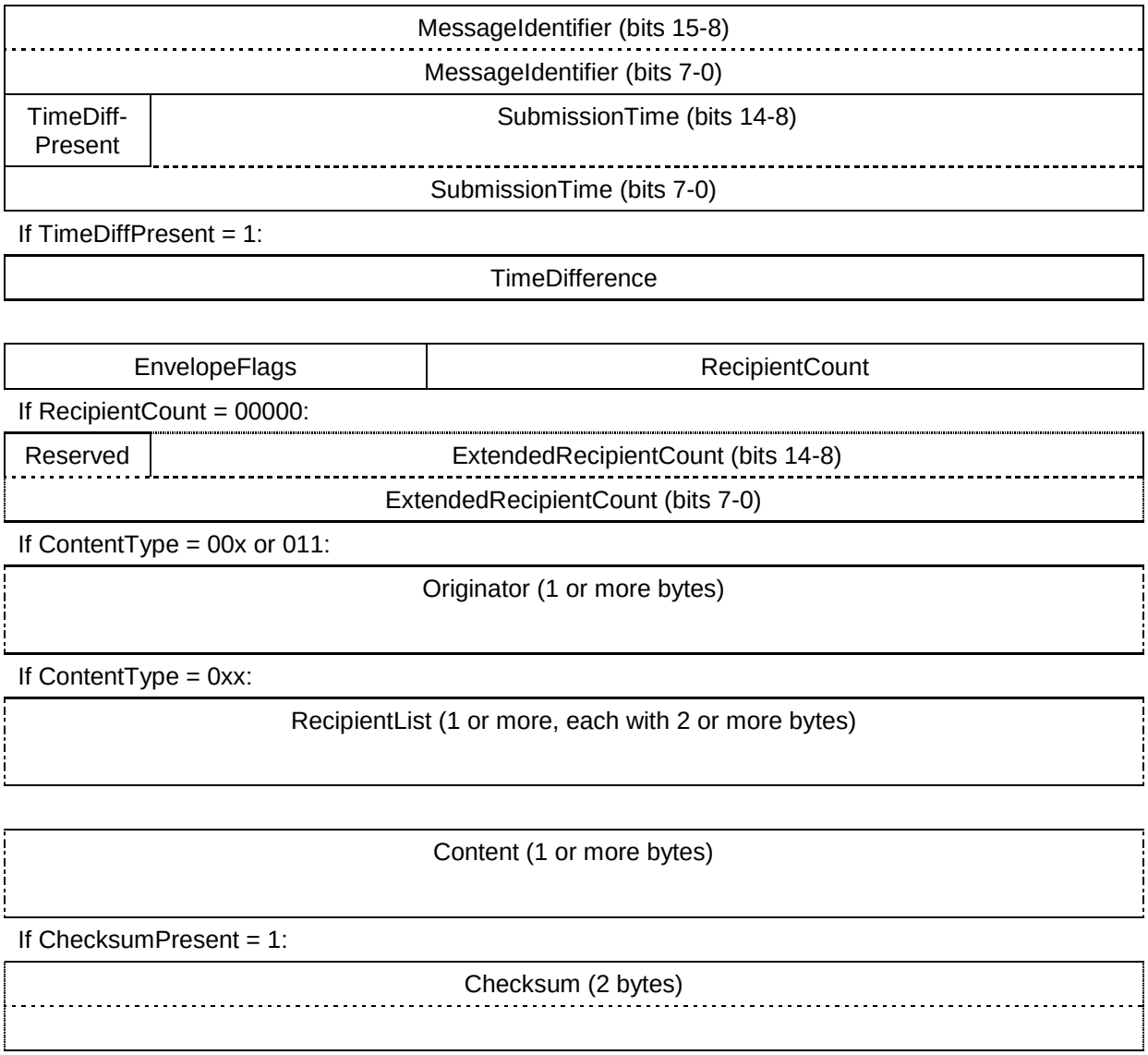


Figure 5.37 – Envelope Structure

5.6.1.2 Envelope fields

5.6.1.2.1 ProtocolIdentifier

This field is used for identifying the object as a DMP object. Values are specified in ITU.T X.263/1998. Values used for DMP are:

01101	Reserved for national versions of DMP
11101	DMP as specified in this document

Other values are either in use or reserved for other protocols.

National versions of DMP can only be used by bilateral agreement between the communicating parties.

5.6.1.2.2 ProtocolVersion

This field is used for identifying the version of DMP as follows:

000	DMP version 1 as specified by this document
001-111	Reserved for future versions of DMP

5.6.1.2.3 HopCount

This field is a 3-bit counter used for loop detection. The value is initialized the first time the message is sent using DMP, and is then decremented for each subsequent DMP link. If zero, a loop is assumed to be present, and the message is trapped. Note that this requires the HopCount to be relayed via any non-DMP links (as a P1 extension). See chapter 5.7.9.6.

5.6.1.2.4 AddressEncoding

This field determines the encoding of all addresses in the message as follows:

0	Use Direct Encoding (see chapter 5.5.1.1)
1	Use Extended Encoding (see chapter 5.5.1.2)

5.6.1.2.5 ChecksumPresent

This field is used for activating the checksum and the acknowledgement mechanisms as follows:

0	No use of checksum
1	Checksum present in this message, acknowledgements used

5.6.1.2.6 ContentType

This field sets the content type of the message as follows:

000	STANAG 4406 Message
001	IPM-88 Message
010	Report
011	Notification
100	Acknowledgement
101-111	Reserved for future content types or different encodings of current content types

5.6.1.2.7 MessageIdentifier

This is a 16-bit value constructed as described in 5.7.9.1.

5.6.1.2.8 TimeDiffPresent

This field indicates the presence of the TimeDifference field as follows:

0	TimeDifference not present
1	TimeDifference field is present

The TimeDifference field shall be included if, and only if, the value is 4 seconds or more.

5.6.1.2.9 SubmissionTime

This is a 15-bit value showing the submission time relative to an 18 hour 12 minute window. The value shall be computed as “(number of seconds since 01 Jan 1970 12:00 UTC divided by 2) modulo 32760”. Values are encoded as shown below. See also chapters 5.4.5 and 5.7.9.5.1.

0x0000-0x7FEF	Number of 2-second units
0x7FF0-0x7FFF	Reserved

5.6.1.2.10 TimeDifference

This field encodes the time difference between the time of sending the DMP message and the message submission time. The time is encoded with decreasing accuracy as the difference increases as follows:

0x00-0x01	Reserved, do not use
0x02-0x1D	Number of 2-second units (4 to 58 seconds)
0x1E-0x91	Number of 15-second units (1 minutes to 29 minutes 45 seconds)
0x92-0xDF	Number of 5-minute units (30 minutes to 6 hours 55 minutes)
0xE0-0xF7	Number of 30-minute units (7 hours to 18 hours 30 minutes)
0xF8-0xFF	Reserved, do not use

5.6.1.2.11 EnvelopeFlags

This field contains flags related to specific message envelope attributes, as follows:

Bit 7 (ContId)	If set, the ContentIdentifier field was present and has been discarded

Bit 6 (ReasgProhib)	If set, the RecipientReassigmentProhibited was present with the value “prohibited”
Bit 5 (DLEProhib)	If set, the DLExpansionProhibited field was present with the value “prohibited”

5.6.1.2.12 RecipientCount

This field specifies the number of P1 and/or P22/P772 recipients transferred with the DMP message. If the number of recipients is more than 31, then this field shall be set to 00000, and the number of recipients shall be encoded into the ExtendedRecipientCount field below. A recipient field including both P1 and P22/P772 addresses counts as 1 recipient.

5.6.1.2.13 ExtendedRecipientCount

This is a 15-bit value showing the number of recipients transferred with the DMP message. If the number of recipients is 31 or less, then the RecipientCount field should be used instead. Note that the values 0x0000 to 0x001F are reserved and shall not be used.

5.6.1.2.14 Originator

This field encodes the message originator. The encoding is determined by the AddressEncoding field (see section 5.6.1.2.4 above).

5.6.1.2.15 RecipientList

This field contains a list of 1 or more recipient items. Each recipient is encoded as determined by the AddressEncoding field (see section 5.6.1.2.4 above).

5.6.1.2.16 Content

The message content is described in section 5.6.2.

5.6.1.2.17 Checksum

This is a 16-bit checksum of the DMP object. The checksum uses the CCITT-16 mechanism described in ITU-T X.25 (i.e. the HDLC 16-bit checksum).

5.6.1.3 Acknowledgement

5.6.1.3.1 Acknowledgement structure

An acknowledgement is encoded as a message envelope only (no content), as follows:

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
ProtocolIdentifier					ProtocolVersion		

Reserved	Recipient-Present	Address-Encoding	Checksum-Present=1	ContentType=100
Reason				
Diagnostic				
SubjectMessageIdentifier (bits 15-8)				
SubjectMessageIdentifier (bits 7-0)				

If RecipientPresent = 1:

RecipientList (0 or more, each with 2 or more bytes)

Checksum (2 bytes)

Figure 5.38 – Acknowledgement Structure

5.6.1.3.2 Acknowledgement fields

The acknowledgement-specific fields are encoded as shown below. Other fields are encoded as described in sections 5.6.2.1 and 5.6.2.3.

5.6.1.3.2.1 RecipientPresent

This field indicates whether the Recipient field is present. This is needed for multicast to identify the original recipient to which this Acknowledgement applies. If multicast is used, then each recipient for which the acknowledging MTA is responsible shall be included in the RecipientList. If multicast is not used, then the RecipientPresent shall be set to 0, and the RecipientList shall be absent.

0 Recipient absent

1 Recipient present

Note that this document does not prescribe a mechanism for determining whether a giving message is sent using multicast. This must be determined from the underlying multicast protocol (e.g. implicit when using P_MUL, based on use of multicast addresses if using some other multicast protocol).

5.6.1.3.2.2 Reason

This field specifies the result of the message to which the acknowledgement refers.

0x00 Successful, positive acknowledgement

0x01 Unspecified error

0x02 Checksum incorrect

0x02-0xff Reserved

5.6.1.3.2.3 Diagnostic

This field provides additional diagnostic information.

0x00-0xff Reserved

5.6.2 Message content encoding

The message content is encoded differently depending on the message type (ContentType field, see section 5.6.1.2.6).

5.6.2.1 STANAG 4406 message

5.6.2.1.1 STANAG 4406 message structure

The message content includes a number of heading fields and the message body. The STANAG 4406 message content is as follows:

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
MessageType		Reserved	Precedence			BodyFormat	
SecurityClassification			SecurityPolicy			HeadingFlags	

If SecurityPolicy = 110:

NationalPolicyIdentifier

If SecurityPolicy = 111:

MissionPolicyIdentifier

SecurityCategories
ExpiryTime
DTG
SIC (1 to 58 bytes)

If BodyFormat = 00:

EIT	CompressionAlgorithm	Reserved
UserData (1 or more bytes)		

If BodyFormat = 01:

Subject (1 or more bytes)

EIT	CompressionAlgorithm	Reserved
UserData (1 or more bytes)		

If BodyFormat = 10:

UserData (1 or more bytes)

Figure 5.39 – STANAG 4406 Message Structure

5.6.2.1.2 STANAG 4406 message fields

The different fields are encoded as follows:

5.6.2.1.2.1 MessageType

This field encodes the STANAG 4406 message type as follows:

00	Operation
01	Project
10	Exercise
11	Drill

5.6.2.1.2.2 Precedence

This field encodes the Action Precedence. The Info Precedence is assumed to be the same as the Action Precedence, except in the specific cases encoded below.

000	Deferred
001	Routine
010	Priority
011	Immediate
100	Flash
101	Override
110	Priority, with Info Precedence set to Routine
111	Immediate, with Info Precedence set to Routine

5.6.2.1.2.3 BodyFormat

This field specifies the encoding of the message body as follows:

00	Free text (used when the subject is not essential)
01	Free text including subject
10	Rerserved for structured body (e.g. tactical formats)
11	Reserved

5.6.2.1.2.4 SecurityClassification

This field specifies the hierarchical part of the message security label. The given encoding applies to the NATO and the National security policies as defined by the SecurityPolicy values 100 and 101. Note that the encoding may be redefined when using other security policies.

000	Unmarked
001	Unclassified
010	Reserved
011	Restricted
100	Reserved
101	Confidential
110	Secret
111	Top secret

5.6.2.1.2.5 SecurityPolicy

This field identifies the security policy that applies to the security label of this message.

000-011	Network defined
100	NATO
101	National (nation of local server)
110	Extended, next byte contains national policy
111	Extended, next byte contains mission-defined policy

Note that the NATO policy does not fully support the ESSSecurityLabel (see chapter 5.7.9.7).

5.6.2.1.2.6 NationalPolicyIdentifier

This field identifies the specific national security policy when using SecurityPolicy value 110.

0x00-0xfe	Country code (allocated according to chapter 8)
0xff	Reserved

5.6.2.1.2.7 MissionPolicyIdentifier

This field identifies the specific mission when using SecurityPolicy value 111.

0x00-0xfe	Allocated on a per-mission basis
0xff	Reserved

5.6.2.1.2.8 SecurityCategories

This field specifies the non-hierarchical part of the message security label. The given encoding applies to the NATO and the National security policies as defined by the SecurityPolicy values 100 and 101. Note that the encoding may be redefined when using other security policies.

bit 7	Clear
bit 6	Crypto Security
bit 5	Exclusive
bit 4	National Eyes Only
bit 3	Reserved
bit 2	Reserved
Bit 1	Reserved
Bit 0	Reserved

5.6.2.1.2.9 HeadingFlags

This field contains flags related to specific heading fields, as follows:

Bit 1 (AuthUsers)	If set, the Authorizing Users field was present and has been discarded
Bit 0 (Subj)	If set, the Subject field was present and has been discarded

5.6.2.1.2.10 ExpiryTime

This field contains the message expiry time encoded as an offset from the message submission time.

0x00	Not present
0x01-0x1D	Number of 2-second units (2-58 seconds)
0x1E-0x91	Number of 15-second units (1 min – 29 min 45 sec)
0x92-0xBB	Number of 5-minute units (30 min – 3 hours 55 min)
0xBC-0xE3	Number of 30-minute units (4 hours – 23 hours 30 min)
0xE4-0xFE	Number of 2-hour units (24-76 hours)

0xFF	Reserved

5.6.2.1.2.11 DTG

This field contains the DTG encoded as an offset from the message submission time.

0x00	Not present
0x01-0x7E	DTG in the past
0x7F	Reserved
0x80	Reserved
0x81-0xFE	DTG in the future
0xFF	Reserved

0x01-0x3C/0x81-0xBC	Number of minutes (0-59 min)
0x3D-0x64/0xBD-0xE4	Number of 15-minute units (1 hour – 10 hours 45 min)
0x65-0x7E/0xE5-0xFE	Number of hours (11-36 hours)

5.6.2.1.2.12 SIC

This field encodes up to 8 SICs. The first byte determines the contents of the SIC field as follows:

0x00-0xb6	2 bytes, single 3-character SIC, characters [A-Z0-9] only
0xb7-0xbd	3 bytes, single 3-character SIC, any valid character (encoded by adding the value B7 00 00 to the calculated SIC)
0xbe-0xbf	Reserved (not used)
0xc0-0xcf	2 or more 3-character SICs

The first byte is encoded as follows:

1100CNNN

C = 0 characters [A-Z0-9] only

C = 1 any valid characters

NNN = number of SICs – 1 (value 000 is reserved)

0xd0-0xdf	1 or more 3 to 8 character SICs

The first byte is encoded as follows:

1101CNNN

C = 0 characters [A-Z0-9] only

C = 1 any valid characters

NNN = number of SICs – 1

The second byte is encoded as a bitmap showing SIC length for each SIC (0 = 3, 1 = 4 to 8)

0xe0-0xfd	Reserved (not used)
0xfe	No SIC
0xff	Reserved (not used)

Each SIC is encoded as a binary number by converting each character to a number, multiplying it by a factor depending on character set and position, and then adding the values. When only [A-Z0-9] are used, the mapping is as follows (the multiplier is 36):

0 to 9	mapped to	0 to 9
A to Z	mapped to	10 to 35

When additional characters are required, the mapping is as follows (the multiplier is 74):

0 to 9	mapped to	0 to 9
A to Z	mapped to	10 to 35
a to z	mapped to	36 to 61
‘()+,-./:=?	mapped to	62 to 72
space	mapped to	73

When encoding a SIC that is longer than 3 characters, the SIC length is encoded into bits 7 to 4 of the first byte. The resulting value ranges, encoded lengths and needed number of bytes for different length SICs is shown in the table below.

Table 5.40

	Characters [A-Z0-9] only			Any valid characters		
length	**bytes**	**Values (00 to …)**	**bit 7-4**	**bytes**	**Values (00 to …)**	**bit 7-4**
3	2	B6 3F		3	06 2E E7	
4	3	19 A0 FF	110x	4	01 C9 8F 0F	1010
5	4	03 9A A3 FF	1010	4	84 43 5A 9F	0xxx or 1000
6	4	81 BF 0F FF	0xxx or 1000	5	26 3B 78 32 3F	11xx
7	5	12 3E DE 3F FF	111x	6	0B 0D 30 BE 86 7F	1011
8	6	02 90 D7 40 FF FF	1011	7	03 31 D0 17 12 E0 FF	1001

5.6.2.1.2.13 EIT

This field specifies the encoded information type contained in the message body.

000	empty
001	ia5-text
010	general text
011	bilaterally-defined (binary data)
100	adatp-3
101	Reserved
110	Reserved
111	Reserved

5.6.2.1.2.14 CompressionAlgorithm

The field identifies the compression used for the message body.

00	No compression
01	Zlib compressed
10	Reserved
11	Reserved

5.6.2.1.2.15 UserData

This field contains the message body. The encoded information type is specified by the EIT field, and the use of compression is specified by the CompressionAlgorithm field. See also chapter 5.7.9.10.

5.6.2.1.2.16 Subject

This field contains the message subject. The subject shall be encoded as an ISO-8859-1 string, and shall be zero-terminated.

5.6.2.2 IPM 88 message

5.6.2.2.1 IPM 88 message structure

The message content includes a number of heading fields and the message body. The IPM 88 message content is as follows:

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
Reserved			Importance			BodyFormat	
SecurityClassification			SecurityPolicy			HeadingFlags	

<table>
<tr><td colspan="3">If SecurityPolicy = 110:</td></tr>
<tr><td colspan="3">NationalPolicyIdentifier</td></tr>
<tr><td colspan="3">If SecurityPolicy = 111:</td></tr>
<tr><td colspan="3">MissionPolicyIdentifier</td></tr>
<tr><td colspan="3">SecurityCategories</td></tr>
<tr><td colspan="3">ExpiryTime</td></tr>
<tr><td colspan="3">If BodyFormat = 00:</td></tr>
<tr><td>EIT</td><td>CompressionAlgorithm</td><td>Reserved</td></tr>
<tr><td colspan="3">UserData (1 or more bytes)</td></tr>
<tr><td colspan="3">If BodyFormat = 01:</td></tr>
<tr><td colspan="3">Subject (1 or more bytes)</td></tr>
<tr><td>EIT</td><td>CompressionAlgorithm</td><td>Reserved</td></tr>
<tr><td colspan="3">UserData (1 or more bytes)</td></tr>
<tr><td colspan="3">If BodyFormat = 10:</td></tr>
<tr><td colspan="3">UserData (1 or more bytes)</td></tr>
</table>

Figure 5.41 – IPM 88 Message Structure

5.6.2.2.2 IPM 88 message fields

The Importance field is encoded as shown below. Other fields are encoded as described in section 5.6.2.1.

5.6.2.2.2.1 Importance

This field encodes the message importance.

000	Low
001	Reserved
010	Normal
011	Reserved
100	High
101->111	Reserved

5.6.2.3 Report

5.6.2.3.1 Report structure

The Report content is encoded in the same way for STANAG 4406 and IPM 88 reports. The report content is encoded as follows:

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
SecurityClassification			SecurityPolicy			Reserved	

If SecurityPolicy = 110:

NationalPolicyIdentifier

If SecurityPolicy = 111:

MissionPolicyIdentifier

SecurityCategories
SubjectMessageIdentifier (bits 15-8)
SubjectMessageIdentifier (bits 7-0)

Figure 5.42 – Report Structure

Report data for one or more recipients follows, each encoded as described below.

A Delivery Report is coded as follows:

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
ReportType=0	InfoPresent	Address-Encoding	Reserved				
DeliveryTime							
ReportingName (1 or more bytes)							

If InfoPresent = 1:

SupplementaryInformation (1 or more bytes)

Figure 5.43 – Delivery Report Structure

A Non-Delivery Report is coded as follows:

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
ReportType=1	Address-Encoding	Reason					
InfoPresent	Diagnostic						
ReportingName (1 or more bytes)							
If InfoPresent = 1:							
SupplementaryInformation (1 or more bytes)							

Figure 5.44 – Non-Delivery Report Structure

5.6.2.3.2 Report fields

The report-specific fields are encoded as shown below. Other fields are encoded as described in sections 5.6.1.2.4 and 5.6.2.1.

5.6.2.3.2.1 SubjectMessageId

This is a 16-bit value referring to the subject message, and constructed according to ch 5.7.9.1.

5.6.2.3.2.2 ReportType

This field identifies the type of report.

0	Delivery Report (DR)
1	Non-Delivery Report (NDR)

5.6.2.3.2.3 DeliveryTime

This field specifies the message delivery time, encoded as an offset from the original message submission time.

0x00-0x1D	Number of 2-second units (0 – 58 seconds)
0x1E-0x91	Number of 15-second units (1 min – 29 min 45 sec)
0x92-0xBB	Number of 5-minute units (30 min – 3 hours 55 min)
0xBC-0xE3	Number of 30-minute units (4 hours – 23 hours 30 min)
0xE4-0xFE	Number of 2-hour units (24-76 hours)
0xFF	Reserved

5.6.2.3.2.4 Reason

This field specifies the non-delivery reason code as follows:

0x00-0x3c	Standard reason according to X.411
0x3d	Unknown reason
0x3e	Reason code greater than 0x3c (60)
0x3f	Reserved

5.6.2.3.2.5 InfoPresent

This field specifies whether the SupplementaryInformation field is present.

0	SupplementaryInformation not present
1	SupplementaryInformation present

5.6.2.3.2.6 Diagnostic

This field specifies the non-delivery diagnostic code as follows:

0x00-0x7b	Standard diagnostic according to X.411
0x7c	Diagnostic not specified
0x7d	Unknown diagnostic
0x7e	Diagnostic code greater than 0x7b (123)
0x7f	Reserved

5.6.2.3.2.7 ReportingName

This field encodes the report originator (which corresponds to a recipient of the original message). The ReportingName shall be encoded as a Recipient as specified in chapter 5.5.

5.6.2.3.2.8 SupplementaryInformation

This field includes any supplementary information provided by the report originator. It is encoded as a zero-terminated text string, truncated to ensure that the total report does not exceed 128 bytes.

5.6.2.4 Notification

5.6.2.4.1 Notification structure

Notifications are encoded in the same way for STANAG 4406 and IPM 88 notifications. Notifications are encoded as follows:

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0

SecurityClassification	SecurityPolicy	NotificationType

If SecurityPolicy = 110:

NationalPolicyIdentifier

If SecurityPolicy = 111:

MissionPolicyIdentifier

SecurityCategories
SubjectMessageIdentifier (bits 15-8)
SubjectMessageIdentifier (bits 7-0)

If NotificationType = 00:

ReceiptTime
SupplInfo (1 or more bytes)

If NotificationType = 01:

NonRecReason
DiscardReason

If NotificationType = 10:

ReceiptTime
ONType
SupplInfo (1 or more bytes)

If ONType = 0x00, 0x01 or 0x10:

ACP127Recip (1 or more bytes)

Figure 5.45 – Notification Structure

5.6.2.4.2 Notification fields

The notification-specific fields are encoded as shown below. Other fields are encoded as described in sections 5.6.2.1 and 5.6.2.3.

5.6.2.4.2.1 NotificationType

This field specifies the type of notification.

00	Receipt Notification (RN)
01	Non-Receipt Notification (NRN)

10	Other Notification (ON)
11	Reserved

5.6.2.4.2.2 ReceiptTime

This field contains the message receipt time. It is encoded in the same way as ExpiryTime (see ch 5.6.2.1).

5.6.2.4.2.3 SupplInfo

This field contains any supplementary information. It is encoded as a zero-terminated text string, truncated to ensure the total message does not exceed 128 bytes.

5.6.2.4.2.4 NonRecReason

This field encodes the non-receipt reason code.

0x00-0x0f	Standard non-receipt-reason according to X.420
0x10-0xff	Reserved

5.6.2.4.2.5 DiscardReason

This field encodes the discard reason code as follows:

0x00-0x0f	Standard discard-reason according to X.420
0x10-0xfd	Reserved
0xfe	DiscardReason absent
0xff	Reserved

5.6.2.4.2.6 ONType

This field specifies the type of other notification as follows:

0x00	acp127-nn
0x01	acp127-pn
0x02	acp127-tn
0x03-0xff	Reserved

5.6.2.4.2.7 ACP127Recip

This field identifies the ACP 127 recipient to which the other notification applies. It is encoded as a zero-terminated text string, with a maximum length of 64 characters.

5.6.3 Examples

Example message, 2 recipients, from address 0x009 to 0x049 and 0x033, IMMEDIATE, k,cs,_no_, message identifier 0x0588:

Byte 0	11010000	Direct Message Profile, version 1
Byte 1	00000000	Hop 0, Direct Encoding, no checksum,STANAG 4406 message
Byte 2	00000101	MessageIdentifier (0x05..)
Byte 3	10001000	..0x88
Byte 4	00000000	Submission time
Byte 5	00000000	Submission time
Byte 6	00000010	No flags, 2 recipient addresses
Byte 7	00001001	Originator, address 0x009
Byte 8	00000000	Recipient 1, no reports, no notifications
Byte 9	11001001	Action, address 0x049
Byte 10	00000000	Recipient 2, no reports, no notifications
Byte 11	10110011	Action, address 0x033
Byte 12	00001100	Operation, IMMEDIATE, free text
Byte 13	10110100	Confidential, national policy, no flags
Byte 14	01000000	Crypto Security
Byte 15	00000000	No expiry time
Byte 16	00000000	No DTG
Byte 17	11111110	No SIC
Byte 18	0010100	IA5-text, ZLIB compression
Byte 19→	User data	

5.7 Detailed protocol mapping

The following sections specify the mapping between the Direct Message Profile and the mandatory and optional P1/P22/P772 protocol fields.

5.7.1 Bind and unbind

The Bind and Unbind operations are not explicitly signalled using DMP. An outgoing Bind is mapping to the establishment of an underlying connection. No Bind argument values are used. An incoming Bind is implicit by the reception of a DMP object. Argument values (if needed) must be retrieved from internal data related to the sending MTA (the sending MTA being identified by the source address carried by the DMP bearer service).

5.7.2 P1 Message

Table 5.46

P1 attribute	DMP attribute	Mapping to DMP	Mapping to P1
Message			
- envelope			
- - per-message-fields			
- - - message-identifier	MessageIdentifier	See MTSIdentifier mapping in ch 5.7.9.1	See MTSIdentifier mapping in ch 5.7.9.1
- - - originator-name	Originator	See ORName mapping in ch 5.7.9.2	See ORName mapping in ch 5.7.9.2
- - - original-encoded-information-types	EIT	See EIT mapping in ch 5.7.9.10.	See EIT mapping in ch 5.7.9.10.
- - - content-type	ContentType	See ContentType mapping in ch 5.7.9.3	See ContentType mapping in ch 5.7.9.3
- - - content-identifier	EnvelopeFlags	Discard and set ContId (bit 7) if present	Build from IPM identifier if ContId (bit 7) is set
- - - priority	Precedence, Importance	See Priority mapping in ch 5.7.9.4	See Priority mapping in ch 5.7.9.4
- - - per-message-indicators			
- - - - disclosure-of-other-recipients	(none)	Conversion shall fail if not set	Set
- - - - implicit-conversion-prohibited	(none)	Conversion shall fail if set	Not set
- - - - alternate-recipient-allowed	(none)	Conversion shall fail if not set	Set
- - - - content-return-request	(none)	Conversion shall fail if set	Not set
- - - - bit-5	(none)	Discard	Not set
- - - - bit-6	(none)	Discard	Not set
- - - - service-message	(none)	Conversion shall fail if set	Not set
- - - deferred-delivery-time	(none)	Discard	Not set
- - - per-domain-bilateral-information	(none)	Conversion shall fail if present	Not set
- - - trace-information	SubmissionTime, TimeDifference	See TraceInformation mapping in ch 5.7.9.5	See TraceInformation mapping in ch 5.7.9.5
- - - extensions		If any unsupported extension is marked as critical for transfer or critical for delivery, conversion shall fail. Non-critical unsupported	For supported extensions, criticality shall be set to their respective default values

P1 attribute	DMP attribute	Mapping to DMP	Mapping to P1
		extensions are discarded	
- - - - recipient-reassignment-prohibited	EnvelopeFlags	Set ReasgProhib (bit 6) if prohibited	Set to prohibited if ReasgProhib (bit 6) set
- - - - dl-expansion-prohibited	EnvelopeFlags	Set DLEProhib (bit 5) if prohibited	Set to prohibited if DLEProhib (bit 5) set
- - - - conversion-with-loss-prohibited	(none)	Conversion shall fail if set to prohibited	Set to allowed
- - - - latest-delivery-time	(none)	Discard if non-critical, or if >= expiry-time. Otherwise conversion shall fail	Not set
- - - - originator-return-address	(none)	Discard if non-critical	Not set
- - - - originator-certificate	(none)	Discard if non-critical	Not set
- - - - content-confidentiality-algorithm-identifier	(none)	Discard if non-critical	Not set
- - - - message-origin-authentication-check	(none)	Discard if non-critical	Not set
- - - - message-security-label	SecurityLabel	See MessageSecurityLabel mapping in ch 5.7.9.7	See MessageSecurityLabel mapping in ch 5.7.9.7
- - - - content-correlator	(none)	Discard if non-critical	Not set
- - - - dl-exempted-recipients	(none)	Discard if non-critical	Not set
- - - - certificate-selectors	(none)	Discard if non-critical	Not set
- - - - multiple-originator-certificates	(none)	Discard if non-critical	Not set
- - - - dl-expansion-history	(none)	Discard if non-critical	Not set
- - - - internal-trace-information	(none)	Discard	See TraceInformation mapping in ch 5.7.9.5
- - - - priority-level-qualifier (STANAG 4406 only)	Precedence	See Priority mapping in ch 5.7.9.4	See Priority mapping in ch 5.7.9.4
- - - - hop-counter (DMP specific)	HopCount	See Loop detected mapping in ch 5.7.9.6	See Loop detected mapping in ch 5.7.9.6
- - per-recipient-fields		Normally, only recipients to be reached via DMP and with responsibility set shall be included. As an OPTION, other recipients can be included.	
- - - recipient-name	Recipient	See ORName mapping	See ORName mapping

P1 attribute	DMP attribute	Mapping to DMP	Mapping to P1
		in ch 5.7.9.2	in ch 5.7.9.2
- - - originally-specified-recipient-number	RecipientNumber	Encode as described in ch 5.5.2.12	Decode as described in ch 5.5.2.12
- - - per-recipient-indicators	ReportRequest	Encode as described in ch 5.5.2.13	Decode as described in ch 5.5.2.13
- - - explicit-conversion	(none)	Conversion shall fail if present	Not set
- - - extensions		If any unsupported extension is marked as critical for transfer or critical for delivery, conversion shall fail. Non-critical unsupported extensions are discarded	For supported extensions, criticality shall be set to their respective default values
- - - - originator-requested-alternate-recipient	(none)	Discard if non-critical	Not set
- - - - requested-delivery-method	(none)	Discard if non-critical	Not set
- - - - physical-forwarding-prohibited	(none)	Discard if non-critical	Not set
- - - - physical-forwarding-address-request	(none)	Discard if non-critical	Not set
- - - - physical-delivery-modes	(none)	Discard if non-critical	Not set
- - - - registered-mail-type	(none)	Discard if non-critical	Not set
- - - - recipient-number-for-advice	(none)	Discard if non-critical	Not set
- - - - physical-rendition-attribute	(none)	Discard if non-critical	Not set
- - - - physical-delivery-report-request	(none)	Discard if non-critical	Not set
- - - - message-token	(none)	Discard if non-critical	Not set
- - - - content-integrity-check	(none)	Discard if non-critical	Not set
- - - - proof-of-delivery-request	(none)	Discard if non-critical	Not set
- - - - certificate-selectors-override	(none)	Discard if non-critical	Not set
- - - - recipient-certificate	(none)	Discard if non-critical	Not set
- - - - redirection-history	(none)	Discard if non-critical	Not set
- - - - blind-copy-recipients	(none)	Discard if non-critical	Not set

P1 attribute	DMP attribute	Mapping to DMP	Mapping to P1
- - - - body-part-encryption-token	(none)	Discard if non-critical	Not set
- - - - forwarded-content-token	(none)	Discard if non-critical	Not set
- content		See ch 5.7.3 (IPM), 5.7.4 (MM), 5.7.6 (RN), 5.7.7 (NRN) and 5.7.8 (ON)	See ch 5.7.3 (IPM), 5.7.4 (MM), 5.7.6 (RN), 5.7.7 (NRN) and 5.7.8 (ON)

5.7.3 P22 IPM (X.400/88)

Table 5.47

P22 attribute	DMP attribute	Mapping to DMP	Mapping to P22
IPM			
- heading			
- - this-IPM	(none)	See IPMIdentifier mapping in ch 5.7.9.8	See IPMIdentifier mapping in ch 5.7.9.8
- - originator			
- - - formal-name	Originator	See ORName mapping in ch 5.7.9.2	See ORName mapping in ch 5.7.9.2
- - - free-form-name	(none)	Discard	Not set
- - - telephone-number	(none)	Discard	Not set
- - authorizing-users	HeadingFlags	Discard and set AuthUsers (bit 1) if present	Not set
- - primary-recipients		For each primary recipient, the ActionAddr indicator is set to 1	
- - - recipient			
- - - - formal-name	Recipient	See ORName mapping in ch 5.7.9.2	See ORName mapping in ch 5.7.9.2
- - - - free-form-name	(none)	Discard	Not set
- - - - telephone-number	(none)	Discard	Not set
- - - notification-requests			
- - - - rn	NotificationRequest	Encode as described in ch 5.5.2.9	Decode as described in ch 5.5.2.9
- - - - nrn	NotificationRequest	Encode as described in ch 5.5.2.9	Decode as described in ch 5.5.2.9

P22 attribute	DMP attribute	Mapping to DMP	Mapping to P22
- - - - ipm-return	(none)	Conversion shall fail if set	Not set
- - - - an-supported	(none)	Discard	Not set
- - - - suppress-an	(none)	Discard	Not set
- - - reply-requested	(none)	Discard	Not set
- - - recipient-extensions			
- - - - circulation-list-indicator	(none)	Discard	Not set
- - - - precedence	(none)	Discard	Not set
- - - - recipient-security-request	(none)	Discard	Not set
- - copy-recipients		For each copy recipient, the ActionAddr indicator is set to 0	
- - - recipient			
- - - - formal-name	Recipient	See ORName mapping in ch 5.7.9.2	See ORName mapping in ch 5.7.9.2
- - - - free-form-name	(none)	Discard	Not set
- - - - telephone-number	(none)	Discard	Not set
- - - notification-requests			
- - - - rn	NotificationRequest	Encode as described in ch 5.5.2.9	Decode as described in ch 5.5.2.9
- - - - nrn	NotificationRequest	Encode as described in ch 5.5.2.9	Decode as described in ch 5.5.2.9
- - - - ipm-return	(none)	Conversion shall fail if set	Not set
- - - - an-supported	(none)	Discard	Not set
- - - - suppress-an	(none)	Discard	Not set
- - - reply-requested	(none)	Discard	Not set
- - - recipient-extensions			
- - - - circulation-list-indicator	(none)	Discard	Not set
- - - - precedence	(none)	Discard	Not set
- - - - recipient-security-request	(none)	Discard	Not set
- - blind-copy-recipients	(none)	Conversion shall fail if present	Not set
- - replied-to-IPMs	(none)	Discard	Not set

P22 attribute	DMP attribute	Mapping to DMP	Mapping to P22
- - obsoleted-IPMs	(none)	Discard	Not set
- - related-IPMs	(none)	Discard	Not set
- - subject	MessageFormat, HeadingFlags, UserData	See Subject mapping in ch 5.7.9.9.	See Subject mapping in ch 5.7.9.9.
- - expiry-time	ExpiryTime	Encode as described in ch 5.6.2.1.2.10	Decode as described in ch 5.6.2.1.2.10
- - reply-time	(none)	Discard	Not set
- - reply-recipients	(none)	Conversion shall fail if present	Not set
- - importance	Importance	Encode as described in ch 5.6.2.2.2.1	Decode as described in ch 5.6.2.2.2.1
- - sensitivity	(none)	Conversion shall fail if present	Not set
- - auto-forwarded	(none)	Discard	Not set
- - extensions			
- - - incomplete-copy	(none)	Conversion shall fail if present	Not set
- - - languages	(none)	Discard	Not set
- - - auto-submitted	(none)	Discard	Not set
- - - body-part-signatures	(none)	Discard	Not set
- - - ipm-security-label	(none)	Discard	Not set
- - - authorization-time	(none)	Discard	Not set
- - - circulation-list-recipients	(none)	Discard	Not set
- - - distribution-codes	(none)	Discard	Not set
- - - extended-subject	(none)	Discard	Not set
- - - information-category	(none)	Discard	Not set
- - - manual-handling-instructions	(none)	Discard	Not set
- - - originators-reference	(none)	Discard	Not set
- - - precedence-policy-identifier	(none)	Discard	Not set
- body		Conversion shall fail if more than 1 body is present	
- - body-part			
- - - basic			
- - - - ia5-text	UserData, EIT	See EIT and Body mapping in ch.	See EIT and Body mapping in ch.

P22 attribute	DMP attribute	Mapping to DMP	Mapping to P22
		5.7.9.10	5.7.9.10
- - - - voice	(none)	Conversion shall fail if present	Not set
- - - - g3-facsimile	(none)	Conversion shall fail if present	Not set
- - - - g4-class1	(none)	Conversion shall fail if present	Not set
- - - - teletex	(none)	Conversion shall fail if present	Not set
- - - - videotex	(none)	Conversion shall fail if present	Not set
- - - - encrypted	(none)	Conversion shall fail if present	Not set
- - - - message	(none)	Conversion shall fail if present	Not set
- - - - mixed-mode	(none)	Conversion shall fail if present	Not set
- - - - bilaterally-defined	UserData, EIT	See EIT and Body mapping in ch. 5.7.9.10	See EIT and Body mapping in ch. 5.7.9.10
- - - - nationally-defined	(none)	Conversion shall fail if present	Not set
- - - extended			
- - - - ia5-text-body-part	UserData, EIT	See EIT and Body mapping in ch. 5.7.9.10	See EIT and Body mapping in ch. 5.7.9.10
- - - - g3-facsimile-body-part	(none)	Conversion shall fail if present	Not set
- - - - g4-class1-body-part	(none)	Conversion shall fail if present	Not set
- - - - teletex-body-part	(none)	Conversion shall fail if present	Not set
- - - - videotext-body-part	(none)	Conversion shall fail if present	Not set
- - - - encrypted-body-part	(none)	Conversion shall fail if present	Not set
- - - - message-body-part	(none)	Conversion shall fail if present	Not set
- - - - mixed-mode-body-part	(none)	Conversion shall fail if present	Not set
- - - - bilaterally-defined-body-part	UserData, EIT	See EIT and Body mapping in ch. 5.7.9.10	See EIT and Body mapping in ch. 5.7.9.10

P22 attribute	DMP attribute	Mapping to DMP	Mapping to P22
- - - - nationally-defined-body-part	(none)	Conversion shall fail if present	Not set
- - - - general-text-body-part	UserData, EIT	See EIT and Body mapping in ch. 5.7.9.10	See EIT and Body mapping in ch. 5.7.9.10
- - - - file-transfer-body-part	UserData, EIT	See EIT and Body mapping in ch. 5.7.9.10	See EIT and Body mapping in ch. 5.7.9.10
- - - - voice-body-part	(none)	Conversion shall fail if present	Not set
- - - - report-body-part	(none)	Conversion shall fail if present	Not set
- - - - notification-body-part	(none)	Conversion shall fail if present	Not set
- - - - content-body-part	(none)	Conversion shall fail if present	Not set
- - - - pkcs7-body-part	(none)	Conversion shall fail if present	Not set

5.7.4 P772 MM (STANAG 4406)

STANAG 4406 messages (MMs) use the same mapping as for P22 IPM, supplemented with the following fields:

Table 5.48

P772 attribute	DMP attribute	Mapping to DMP	Mapping to P772
MM			
- heading			
- - extensions			
- - - exempted-address	(none)	Discard	Not set
- - - extended-authorisation-info	DTG	Encode as described in ch 5.6.2.1.2.11	Decode as described in ch 5.6.2.1.2.11
- - - distribution-codes			
- - - - sics	SIC	Encode as described in ch 5.6.2.1.2.12	Decode as described in ch 5.6.2.1.2.12
- - - - dist-extensions	(none)	Discard	Not set
- - - handling-instructions	(none)	Conversion shall fail if present	Not set
- - - message-instructions	(none)	Conversion shall fail if present	Not set
- - - codress-message	(none)	Conversion shall fail if present	Not set

P772 attribute	DMP attribute	Mapping to DMP	Mapping to P772
- - - originator-reference	(none)	Discard	Not set
- - - primary-precedence	Precedence	See Priority mapping in ch 5.7.9.4	See Priority mapping in ch 5.7.9.4
- - - copy-precedence	Precedence	Encode as described in ch 5.6.2.1.2.2	Decode as described in ch 5.6.2.1.2.2
- - - message-type			
- - - - type	MessageType	Encode as described in ch 5.6.2.1.2.1. Conversion shall fail if an unsupported value is used	Decode as described in ch 5.6.2.1.2.1
- - - - identifer	(none)	Discard	Not set
- - - address-list-indicator	(none)	Conversion shall fail if present	Not set
- - - other-receipients-indicator	(none)	Discard	Not set
- - - pilot-forwarding-info	(none)	Discard	Not set
- - - acp127-message-identifier	(none)	Conversion shall fail if the RI is different from originator RI, or if the JFT is more than 60 minutes away from the DTG	Set RI to originator RI, set SSN to 0000, and set JFT to the DTG time
- - - originator-plad	(none)	Discard	Not set
- - - security-information-labels			
- - - - content-security-label	Security Label	See MessageSecurityLabel mapping in ch 5.7.9.7	See MessageSecurityLabel mapping in ch 5.7.9.7
- - - - heading-security-label	(none)	Conversion shall fail if not dominated by content-security-label	Not set
- - - - body-part-security-labels			
- - - - - body-part-security-label	(none)	Conversion shall fail if not dominated by content-security-label	Not set
- - - - - body-part-sequence-number	(none)	Discard	Not set
- - primary-recipients			
- - - recipient-extensions			
- - - - acp127-notification-request	(none)	Conversion shall fail if present	Not set

P772 attribute	DMP attribute	Mapping to DMP	Mapping to P772
- - copy-recipients			
- - - recipient-extensions			
- - - - acp127-notification-request	(none)	Conversion shall fail if present	Not set
- body		Conversion shall fail if more than 1 body is present	
- - body-part			
- - - basic			
- - - - ia5-text	UserData, EIT	See EIT and Body mapping in ch. 5.7.9.10	See EIT and Body mapping in ch. 5.7.9.10
- - - extended			
- - - - adatp3-body-part	UserData, EIT	See EIT and Body mapping in ch. 5.7.9.10	See EDIT and Body mapping in ch. 5.7.9.10
- - - - corrections-body-part	(none)	Conversion shall fail if present	Not set
- - - - forwarded-encrypted-body-part	(none)	Conversion shall fail if present	Not set
- - - - mm-message-body-part	(none)	Conversion shall fail if present	Not set
- - - - acp127data-body-part	(none)	Conversion shall fail if present	Not set

5.7.5 P1 Report

Table 5.49

P1 attribute	DMP attribute	Mapping to DMP	Mapping to P1
Report			
- envelope			
- - report-identifier	MessageIdentifier	See MTSIdentifier mapping in ch 5.7.9.1	See MTSIdentifier mapping in ch 5.7.9.1
- - report-destination-name	Recipient	See ORName mapping in ch 5.7.9.2. The recipient number is set to 0, and the ActionAddr indicator is set to 1	See ORName mapping in ch 5.7.9.2
- - trace-information	SubmissionTime, TimeDifference	See TraceInformation mapping in ch 5.7.9.5	See TraceInformation mapping in ch 5.7.9.5
- - extensions		If any unsupported extension is marked as	For supported extensions, criticality

P1 attribute	DMP attribute	Mapping to DMP	Mapping to P1
		critical for transfer or critical for delivery, conversion shall fail. Non-critical unsupported extensions are discarded	shall be set to their respective default values
- - - message-security-label	SecurityLabel	See MessageSecurityLabel mapping in ch 5.7.9.7	See MessageSecurityLabel mapping in ch 5.7.9.7
- - - redirection-history	(none)	Discard if non-critical	Not set
- - - originator-and-DL-expansion-history	(none)	Discard if non-critical	Not set
- - - reporting-DL-name	(none)	Discard if non-critical	Not set
- - - reporting-MTA-certificate	(none)	Discard if non-critical	Not set
- - - report-origin-authentication-check	(none)	Discard if non-critical	Not set
- - - internal-trace-information	(none)	Discard	See TraceInformation mapping in ch 5.7.9.5
- - - reporting-MTA-name	(none)	Discard if non-critical	Not set
- - - hop-counter (DMP specific)	HopCount	See Loop detection mapping in ch 5.7.9.6	See Loop detection mapping in ch 5.7.9.6
- content			
- - per-report-fields			
- - - subject-identifier	SubjectMessage-Identifier	See MTSIdentifier mapping in ch 5.7.9.1	See MTSIdentifier mapping in ch 5.7.9.1
- - - subject-intermediate-trace-information	(none)	Discard	Not set
- - - original-encoded-information-types	(none)	Discard	Not set
- - - content-type	(none)	See ContentType mapping in ch 5.7.9.3	See ContentType mapping in ch 5.7.9.3
- - - content-identifier	EnvelopeFlags	Discard and set ContId (bit 7) if present	Build from IPM identifier if ContId (bit 7) set
- - - returned-content	(none)	Conversion shall fail if present	Not set
- - - additional-information	(none)	Conversion shall fail if present	Not set
- - - extensions		If any unsupported extension is marked as critical for transfer or critical for delivery, conversion shall fail.	For supported extensions, criticality shall be set to their respective default

P1 attribute	DMP attribute	Mapping to DMP	Mapping to P1
		Non-critical unsupported extensions are discarded	values
- - - - content-correlator	(none)	Discard if non-critical	Not set
- - per-recipient-fields			
- - - actual-recipient-name	Reporting	See ORName mapping in ch 5.7.9.2. The ActionAddr indicator is set to 1	See ORName mapping in ch 5.7.9.2
- - - originally-specified-recipient-number	RecipientNumber	Encode as described in ch 5.5.2.12	Decode as described in ch 5.5.2.12
- - - per-recipient-indicators	(none)	Discard	Not set
- - - last-trace-information			
- - - - arrival-time	(none)	Discard	Set to same value as SubmissionTime
- - - - converted-encoded-information-type	(none)	Discard	Not set
- - - - report-type	ReportType	Set to 0 if delivery-report, set to 1 if non-delivery-report	If set to 0, a delivery-report is built. If set to 1, a non-delivery-report is built.
- - - - - delivery			
- - - - - - message-delivery-time	DeliveryTime	Encode as described in ch 5.6.2.3.2.3	Decode as described in ch 5.6.2.3.2.3
- - - - - - type-of-MTS-user	(none)	Discard	Set to ‘public’
- - - - - non-delivery			
- - - - - - non-delivery-reason-code	Reason	Encode as described in ch 5.6.2.3.2.4	Decode as described in ch 5.6.2.3.2.4
- - - - - - non-delivery-diagnostic-code	Diagnostic	Encode as described in ch 5.6.2.3.2.6	Decode as described in ch 5.6.2.3.2.6
- - - originally-intended-recipient-name	(none)	Discard	Not set
- - - supplementary-information	Supplementary-Information	Encode as described in ch 5.6.2.3.2.8	Decode as described in ch 5.6.2.3.2.8
- - - extensions		If any unsupported extension is marked as critical for transfer or critical for delivery, conversion shall fail. Non-critical unsupported extensions are discarded	For supported extensions, criticality shall be set to their respective default values

P1 attribute	DMP attribute	Mapping to DMP	Mapping to P1
- - - - redirection-history	(none)	Discard if non-critical	Not set
- - - - physical-forwarding-address	(none)	Discard if non-critical	Not set
- - - - recipient-certificate	(none)	Discard if non-critical	Not set
- - - - proof-of-delivery	(none)	Discard if non-critical	Not set

5.7.6 P22/P772 Receipt Notification (RN)

Table 5.50

P22 attribute	DMP attribute	Mapping to DMP	Mapping to P22
RN			
- common-fields			
- - subject-ipm	SubjectMessage-Identifier	See IPMIdentifier mapping in ch 5.7.9.8	See IPMIdentifier mapping in ch 5.7.9.8
- - ipn-originator			
- - - formal-name	Originator	See ORName mapping in ch 5.7.9.2	See ORName mapping in ch 5.7.9.2
- - - free-form-name	(none)	Discard	Not set
- - - telephone-number	(none)	Discard	Not set
- - ipm-intended-recipient	(none)	Discard	Not set
- - conversion-eits	(none)	Discard	Not set
- - notification-extensions			
- - - ipn-security-response	(none)	Discard	Not set
- receipt-fields			
- - receipt-time	ReceiptTime	Encode as described in ch 5.6.2.4.2.2	Decode as described in ch 5.6.2.4.2.2
- - acknowledgement-mode	(none)	Discard	Not set
- - suppl-receipt-info	SupplInfo	Encode as described in ch 5.6.2.4.2.3	Decode as described in ch 5.6.2.4.2.3
- - rn-extensions	(none)	Discard	Not set

5.7.7 P22/P772 Non-receipt Notification (NRN)

Table 5.51

P22 attribute	DMP attribute	Mapping to DMP	Mapping to P22

P22 attribute	DMP attribute	Mapping to DMP	Mapping to P22
NRN			
- common-fields			
- - subject-ipm	SubjectMessage-Identifier	See IPMIdentifier mapping in ch 5.7.9.8	See IPMIdentifier mapping in ch 5.7.9.8
- - ipn-originator			
- - - formal-name	Originator	See ORName mapping in ch 5.7.9.2	See ORName mapping in ch 5.7.9.2
- - - free-form-name	(none)	Discard	Not set
- - - telephone-number	(none)	Discard	Not set
- - ipm-intended-recipient	(none)	Discard	Not set
- - conversion-eits	(none)	Discard	Not set
- - notification-extensions			
- - - ipn-security-response	(none)	Discard	Not set
- non-receipt-fields			
- - non-receipt-reason	NonRecReason	Encode as described in ch 5.6.2.4.2.4	Decode as described in ch 5.6.2.4.2.4
- - discard-reason	DiscardReason	Encode as described in ch 5.6.2.4.2.5	Decode as described in ch 5.6.2.4.2.5
- - auto-forward-comment	(none)	Discard	Not set
- - returned-ipm	(none)	Conversion shall fail if present	Not set
- - nrn-extensions	(none)	Discard	Not set

5.7.8 P22/P772 Other Notification (ON)

Table 5.52

P22 attribute	DMP attribute	Mapping to DMP	Mapping to P22
ON			
- common-fields			
- - subject-ipm	SubjectMessage-Identifier	See IPMIdentifier mapping in ch 5.7.9.8	See IPMIdentifier mapping in ch 5.7.9.8
- - ipn-originator			
- - - formal-name	Originator	See ORName mapping in ch 5.7.9.2	See ORName mapping in ch 5.7.9.2

P22 attribute	DMP attribute	Mapping to DMP	Mapping to P22
- - - free-form-name	(none)	Discard	Not set
- - - telephone-number	(none)	Discard	Not set
- - ipm-intended-recipient	(none)	Discard	Not set
- - conversion-eits	(none)	Discard	Not set
- - notification-extensions			
- - - ipn-security-response	(none)	Discard	Not set
- other-notification-type-fields			
- - on-extensions			
- - - absence-advice	(none)	Discard	Not set
- - - change-of-address-advice	(none)	Discard	Not set
- - - acp127-notification-response			
- - - - acp127-notification-type	ONType	Encode as described in ch 5.6.2.4.2.6	Decode as described in ch 5.6.2.4.2.6
- - - - receipt-time	ReceiptTime	Encode as described in ch 5.6.2.4.2.2	Decode as described in ch 5.6.2.4.2.2
- - - - address-list-indicator	(none)	Discard	Not set
- - - - acp127-recipient	ACP127Recip	Encode as described in ch 5.6.2.4.2.7	Decode as described in ch 5.6.2.4.2.7
- - - - acp127-supp-info	SupplInfo	Encode as described in ch 5.6.2.4.2.3	Decode as described in ch 5.6.2.4.2.3

5.7.9 Common attribute mapping

5.7.9.1 MTSIdentifier

DMP needs to compress the MTSIdentifier to avoid overhead. The MTSIdentifier in the X.400 domain is mapped to a DMP MTSIdentifier upon sending of a message. Upon reception the DMP MTSIdentifier is restored to its original value.

When mapping a Message or a Notification to DMP, conversion shall fail if the GlobalDomainIdentifier part of the MTSIdentifier does not match the corresponding attributes of the originator-name. A unique 16-bit identifier is created, stored in a local table along with the LocalIdentifier part of the MTSIdentifier, and transmitted as the DMP MessageIdentifier. The algorithm for creating the unique identifier shall ensure uniqueness within a period of at

least 18 hours, e.g. by allocating numbers sequentially. This allows transmitting 1 message per second continously.

When mapping a Report to DMP, the MTSIdentifier of the Report itself shall be converted as for a Message (except that since the Report may include multiple “originators” in the form of actual-recipient-name, the originator check cannot be performed). The MTSIdentifier referring to the original Message (i.e. the subject-identifier) shall be handled as follows: Conversion shall fail if the GlobalDomainIdentifier part does not match that of the original originator (i.e. the report-destination-name), or if the LocalIdentifier part cannot be found in the local table. The DMP MessageIdentifier is fetched from the table, and transmitted as the DMP SubjectMessageId.

When mapping a received DMP Message or Notification, the GlobalDomainIdentifier part of the MTSIdentifier shall be set to the value of the corresponding attributes of the originator-name. A unique LocalIdentifier part is created, and stored in a local table along with the DMP MessageIdentifier. The algorithm for creating the LocalIdentifier shall ensure that the values do not overlap those created when using other protocols, e.g. by prefixing the MTA-name with “DMP-“.

When mapping a received DMP Report, the DMP MessageIdentifier of the Report shall be converted as for a received DMP Message (using the actual-recipient-name from the first per-recipient-field as the originator). The DMP SubjectMessageId shall be handled as follows: The conversion shall fail if the DMP SubjectMessageId cannot be found in the local table. The GlobalDomainIdentifier part shall be set to the value of the original originator (i.e. the report-destination-name). The LocalIdentifier part is fetched from the local table.

See also sections 5.7.9.3, 5.7.9.4 and 5.7.9.8 for other data that may be saved in the local table.

5.7.9.2 ORName

When mapping to DMP, the ORName is converted to a Direct Address using either the Directory Service, or using any other mechanism agreed within the network (e.g. using the DD.DPAddr attribute value as a Direct Address). If the ORName cannot be converted to a Direct address, it may be encoded as an ASN.1 Extended address.

When mapping from DMP, the Direct address is converted to an ORName using the Directory Service, or using any other mechanism agreed within the network. ASN.1 Extended addresses do not need conversion, and can be used directly.

For the Originator, the P1 originator-name is used when mapping to DMP (i.e. the P22/P772 originator formal-name is discarded). When mapping from

DMP, the P1 originator-name and the P22/P772 originator formal-name are both set to the same ORName.

For Recipients, additional steps are needed:

- Each P1 recipient-name for which the responsibility flag is set is converted as above, and the originally-intended-recipient-number is mapped to the DMP RecipientNumber attribute. If the corresponding P22/P772 recipient is listed as a primary-recipient, the DMP ActionAddr indicator is set. If the corresponding P22/P772 recipient is listed as a copy-recipient, the DMP ActionAddr indicator is reset.

- P22/P772 recipients not listed as P1 recipients, or where the P1 responsibility flag is not set, are normally discarded. As an option, such addresses can be transported (as described in chapter 5.5.2.3, last paragraph).

- For P1 recipients not listed as P22/P772 recipients, the ActionAddr indicator shall be set.

5.7.9.3 ContentType

When mapping to DMP, the P1 content-type is used with the P22/P772 object type to set the DMP ContentType attribute. The mapping is as follows:

Table 5.53

P1 content-type	P22/P772 object	DMP ContentType
any, Report	(absent)	Report
interpersonal-messaging-1984	IPM	Message (IPM 88)
interpersonal-messaging-1988	IPM	Message (IPM 88)
interpersonal-messaging-1984	RN/NRN	Notification
interpersonal-messaging-1988	RN/NRN	Notification
stanag-4406	MM	Message (STANAG 4406)
stanag-4406	RN/NRN	Notification
stanag-4406	PN/TN/NN	Notification

Any other combination shall result in a conversion failure.

When mapping from DMP, the DMP ContentType is used to set the P1 content-type and the P22/P772 object type as follows:

Table 5.54

DMP MessageType	P1 content-type	P22/P772 object
Message (STANAG 4406)	stanag-4406	MM
Message (IPM-88)	interpersonal-messaging-1988	IPM
Report	Set to the saved content type of the message to which the report refers	(absent)
Notification	Set to the saved content type of the message to which the notification refers	RN/NRN/ON depending on the NotificationType value

When mapping to DMP, the P1 content-type must be saved at the sending MTA (e.g. in the local table described in section 5.7.9.1). When mapping from DMP, the saved P1 content-type must be restored as shown above.

5.7.9.4 Priority

When mapping to DMP, the P1 priority and priority-level-qualifier fields must be saved at the sending MTA (e.g. in the local table described in section 5.7.9.1): These fields are not transmitted.

When mapping from DMP, the P1 priority and priority-level-qualifier fields are set from the Precedence (STANAG 4406) or Importance (IPM-88) fields. For a Report and a Notification, these fields are set from stored data. The priority-level-qualifier is only set for STANAG 4406.

The values used are:

Table 5.55

DMP Precedence or Importance	P1 priority	P1 priority-level-qualifier
Deferred, Low	Non-Urgent	Low
Routine	Non-Urgent	High
Priority, Normal	Normal	Low
Immediate	Normal	High
Flash, High	Urgent	Low
Override	Urgent	High

5.7.9.5 TraceInformation

When mapping to DMP, the P1 trace-information and internal-trace-information fields are discarded, except for extracting the message

submission time. The DMP SubmissionTime is set from the arrival-time of the first trace-information-element.

When mapping from DMP, the P1 trace-information and internal-trace-information fields shall be constructed as follows:

- A trace-information-element is constructed containing the originator GlobalDomainIdentifier, arrival-time from the DMP SubmissionTime field, routing-action set to “relayed”, and other fields absent.

- If the originator GlobalDomainIdentifier is different from that of the remote server, another trace-information-element is constructed containing the remote server GlobalDomainIdentifier, arrival-time from the DMP SubmissionTime field updated with the TimeDifference field (if present), routing-action set to “relayed”, and other fields absent.

- If the originator GlobalDomainIdentifier is the same as that of the remote server, an internal-trace-information-element is constructed containing the GlobalDomainIdentifier and the mta-name of the remote server, the arrival-time from the DMP SubmissionTime field updated with the TimeDifference field (if present), routing-action set to “relayed”, and other fields absent.

- Subsequent elements are constructed as part of the normal handling.

Note that Audited Reports are not handled, i.e. the original [internal-]trace-information is not preserved.

5.7.9.5.1 Submission time

The timeline is divided into submission time periods (P), each 18 hours 12 minutes long. Submission time is represented relative to the start of the submission time period that the message was submitted in. The offset is encoded in the message header as described in chapter 5.6.1.2.9.

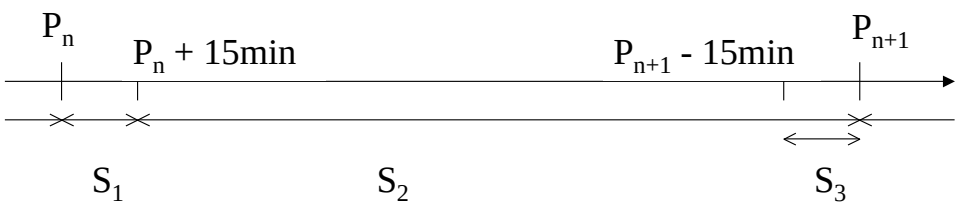


Figure 5.56 – Submission Time

Upon reception, the encoded current time (C) and submission time (E) offsets are used to determine the correct submission time. The following refers to Figure 5.56 above:

- If E is in the interval S_1, C is in the interval S_3, and the cyclic difference between E and C is no more than 15 minutes:
  Assume that the clock is slightly out of sync (must be less than 15 minutes), and compute the submission time as follows: *S = Current time + Length of P + E - C*

- If E is in the interval S_2, and E is more than 15 minutes higher than C:
  Assume that E and C are computed in different submission time periods (either due to a long transfer time or due to clocks out of sync), and compute the submission time as follows: *S = Current time – Length of P) + E - C*

- In all other cases:
  Compute the submission time as follows: *S = Current time + E - C*

5.7.9.6 Loop detection

Loop detection will normally use the P1 trace-information and internal-trace-information fields. When using DMP, this is not possible. Instead, a new P1 extension “hop-counter” is used. When mapping to DMP, if this extension is absent, the HopCount field is set to a configurable maximum value. If the “hop-counter” extension is present, its value is decremented. If equal to zero, the message is assumed to have looped, conversion shall fail, and the event shall be logged. The limit shall be configurable in the range from 1 through 7, with a default value of 4.

When mapping from DMP, the HopCount field is used for constructing a “hop-counter” P1 extension.

At any other location within the MMHS, the “hop-counter” extension shall be relayed if present, but no other processing shall be performed.

The “hop-counter” extension is defined as follows:

```
hop-counter EXTENSION ::= {
      HopCounter,
      RECOMMENDED CRITICALITY { for-transfer },
      IDENTIFIED BY private-extension:
            id-nato-mmhs-mts-extension-hop-counter }

HopCounter ::= INTEGER
```

```
id-nato-mmhs-mts-extension-hop-counter OBJECT IDENTIFIER ::=
      { id-mmts 1 }
```

5.7.9.7 MessageSecurityLabel

The P1 message-security-label (if used) and the P772 information-security-labels are mapped to/from the DMP SecurityLabel attribute. Conversion shall fail if the message-security-label (if present) and the content-security-label do not match, or if any body-part-security-label or the heading-security-label is not dominated by the content-security-label.

When mapping from DMP, the message-security-label (if used) and the content-security-label are set from the DMP SecurityLabel field. The body-part-security-label and heading-security-label fields are not set.

The different fields of the security label are mapped as follows:

Table 5.57

P1/P772 field	DMP field
security-policy-identifier	SecurityPolicy, NationalPolicyIdentifier, MissionPolicyIdentifier
security-classification	SecurityClassification
security-categories	SecurityCategories
privacy-mark	(not used)

Note that the security category encoding described in chapter 5.6.2.1.2.8 does not fully support the ESSSecurityLabel. In particular, permissive (“Releasable to”) and informative categories not supported.

5.7.9.8 IPMIdentifier

When mapping to DMP, the ORName part of the IPMIdentifier is always discarded. When mapping from DMP, the ORName is built from the P22/P772 originator formal-name.

When mapping a Message to DMP, the local-IPM-identifier part is stored in a local table along with the DMP MessageIdentifier (as described in section 5.7.9.1). When mapping a Message from DMP, a unique local-IPM-identifier is created, and stored in a local table along with the DMP MessageIdentifier. The local-IPM-identifier is not transmitted by DMP.

When mapping a Notification to DMP, conversion shall fail if the local-IPM-identifier cannot be found in the local table. The DMP MessageIdentifier is fetched from the table, and transmitted as the DMP SubjectMessageId. When mapping a received DMP Notification, the conversion shall fail if the DMP MessageIdentifier cannot be found in the local table. The local-IPM-identifier is fetched from the local table.

5.7.9.9 Subject

When mapping to DMP, the following algorithm shall be used:

- If the subject indicates that the message is a structured message (determined in an implementation-defined way), set BodyFormat to the value 10, and set HeadingFlags.Subject to 0.
- Otherwise, if the subject length is greater than 0 and less than a configurable limit (default 16 characters), set BodyFormat to the value 01, set HeadingFlags.Subject to 0, and copy the subject to the Subject field as a zero-terminated string.
- Otherwise, set BodyFormat to the value 00. HeadingFlags.Subject is set to 1 if the subject is non-empty (i.e. the subject was longer than the configurable limit above), to 0 otherwise.

When mapping from DMP, the following algorithm shall be used:

Table 5.58

BodyFormat	HeadingFlags. Subject	MM or IPM Subject field
00	0	Empty
00	1	The text “Deleted by gateway <gateway name>”. The <gateway name> shall be a user-friendly name for the sending MTA if such a name exists, otherwise it shall be the MTA name of the sending MTA.
01	0	Copied from the DMP Subject field
01	1	(reserved)
10	0	Set to indicate (in an implementation-defined way) that the message contains a structured body
10	1	(reserved)

5.7.9.10 EITs and body

When mapping to DMP, the original-encoded-information-types is used with the P22/P772 Bodypart type to set the DMP EIT attribute. The mapping is as follows:

Table 5.59

P1 original-encoded-information-types	P22/P772 BodypartType	DMP EIT
ia5-text	ia5-text-body-part	ia5-text
general-text (IA5 and ISO-8859-1 character sets only)	general-text-body-part	general-text
undefined	bilaterally-defined-body-part	bilaterally-defined
file-transfer	file-transfer-body-part (content part extracted and used as bilaterally-defined body part)	bilaterally-defined
ia5-text	adatp-3 (line-oriented data only)	adatp-3

Any other combination shall cause the conversion to fail.

When mapping from DMP, the DMP EIT is used to set the P1 original-encoded-information-types and the P22/P722 Bodypart type as follows:

Table 5.60

DMP EIT	P1 original-encoded-information-types	P2/P772 BodypartType
ia5-text	ia5-text	ia5-text
general-text	general-text (shall set the ISO-8859-1 C0, G0 and G1 character sets, i.e. registration numbers 1, 6 and 100)	general-text
bilaterally-defined	undefined	bilaterally-defined-body-part
adatp-3	ia5-text	adatp-3 (shall set data to be line-oriented)

UserData is handled according to the DMP EIT as follows:

Table 5.61

DMP EIT	To DMP	From DMP
ia5-text	Copy to UserData	Copy from UserData
general-text	Copy to UserData	Copy from UserData
bilaterally-defined	Copy to UserData	Copy from UserData
adatp-3	Copy to UserData	Copy from UserData

5.7.9.11 User data compression

Compression shall be used if the compressed body would result in decreased message size.

5.8 DMP Country Codes

The following table identifies the Country Codes to be used in the DMP version defined by this document. This part of the document may need to be updated from time to time – such an update shall not result in a new version of DMP provided Country Codes are not changed (i.e. additions and deletions are permitted).

NOTE:
No existing Country Code has been found suitable, due to the desirability to use a single byte only. The X.121, ISO-3166-1, E.163 and F.69 codes all require more than 1 byte, although the number of distinct country codes is less than 255. The proposed strategy is to assign codes to NATO member nations only in this version of the document, and then add Country Codes on an as-needed basis.

Table 5.62

Country	Alpha-2 code	Alpha-3 code	Number	DMP code
Belgium	BE	BEL	056	0x01
Bulgaria	BG	BGR	100	0x02
Canada	CA	CAN	124	0x03
Czech Republic	CZ	CZE	203	0x04
Denmark	DK	DNK	208	0x05
Estonia	EE	EST	233	0x06
France	FR	FRA	250	0x07
Germany	DE	DEU	276	0x08
Greece	GR	GRC	300	0x09
Hungary	HU	HUN	348	0x0A

Country	Alpha-2 code	Alpha-3 code	Number	DMP code
Iceland	IS	ISL	352	0x0B
Italy	IT	ITA	380	0x0C
Latvia	LV	LVA	428	0x0D
Lithuania	LT	LTU	440	0x0E
Luxemburg	LU	LUX	442	0x0F
Netherlands	NL	NLD	528	0x10
Norway	NO	NOR	578	0x11
Poland	PL	POL	616	0x12
Portugal	PT	PRT	620	0x13
Romania	RO	ROU	642	0x14
Slovakia	SK	SVK	703	0x15
Slovenia	SI	SVN	705	0x16
Spain	ES	ESP	724	0x17
Turkey	TR	TUR	792	0x18
United Kingdom	GB	GBR	826	0x19
United States	US	USA	840	0x1A

6. THE WAP TRANSPORT LAYER

6.1 Introduction

The WAP (Wireless Application Protocol) connection-less transport protocol WDP (Wireless Datagram Protocol) SHALL be used in this profile as the protocol for the transport layer as specified by the WAP WDP standard [ref. 16]. The WAP architecture and protocols have been developed by the WAP Forum. Parts of the text in this section are taken from the WAP Architecture Specification from the WAP Forum.

According to the WAP WDP specification, the User Datagram Protocol (UDP) [ref. 15] is adopted as the WDP protocol definition for any wireless bearer network where IP is used as a routing protocol. UDP provides port based addressing and IP provides the segmentation and reassembly in a connectionless datagram service. There is no value in defining a new datagram protocol to operate over IP when the ubiquitous User Datagram Protocol (UDP) will provide the same mechanisms and functions, and is already very widely implemented. Therefore in all cases where the IP protocol is available over a bearer service the WDP Datagram service offered for that bearer will be UDP. UDP is fully specified in IETF RFC 768 [ref. 15], while the IP networking layer is defined in the IETF RFC 791[ref. 14].

One reason for adopting WAP WDP in this profile and not only use UDP, is that the WDP protocol in addition to specify the use of UDP over IP, specifies how the mappings to a lot of different available bearer services are to be done. WDP also describes a service interface to the layer above, which allows for applications to operate transparently over the different bearer services. Another reason is that UDP mandates the use of IP, but in some military scenarios IP (or the services from the OSI network layer) is not required and an OSI layer 2 bearer can be used directly.

6.1.1 The Wireless Datagram Protocol (WDP)

The Transport layer protocol in the WAP architecture is referred to as the Wireless Datagram Protocol (WDP). The WDP layer operates above the data capable bearer services supported by the various network types. As a general transport service, WDP offers a consistent service to the upper layer protocols of WAP and communicate transparently over one of the available bearer services. Since the WDP protocols provide a common interface to the upper layer protocols, the layers above are able to function independently of the underlying wireless network. This is accomplished by adapting the transport layer to specific features of the underlying bearer. By keeping the transport layer interface and the basic features consistent, global interoperability can be achieved using mediating gateways.

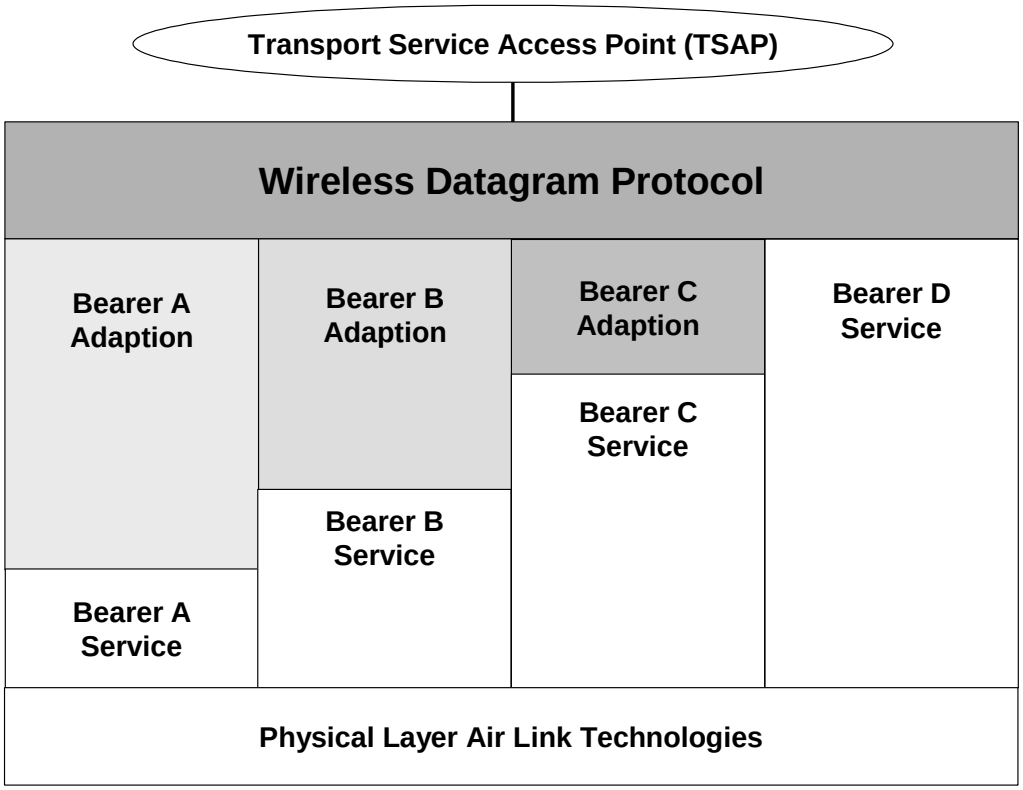


Figure 6.1 – Wireless Datagram Protocol Architecture

The User Datagram Protocol (UDP) is adopted as the WDP protocol definition for any wireless bearer network where IP is used as a routing protocol. When IP is used as the network protocol, the “Robust IP header compression” SHALL be used as defined in the IETF RFC 3095 and RFC 3096.

See [ref. 16] for more information and protocol details.

6.1.2 Bearers

The WAP protocols are designed to operate over a variety of different bearers services, including short message, circuit-switched data, and packet data. The bearers offer differing levels of quality of service with respect to throughput, error rate, and delays. The WAP protocols are designed to compensate for or tolerate these varying levels of service. Since the WDP layer provides the convergence between the bearer service and the rest of the WAP stack, the WDP specification [ref. 16] lists the bearers that are supported and the techniques used to allow WAP protocols to run over each bearer. The list of supported bearers will change over time with new bearers being added as the wireless market evolves.

For the use of WDP over STANAG 5066 (HF), see Appendix A.

6.1.3 Other Services and Applications

The WAP layered architecture enables other services and applications to utilise the features of the WAP stack through a set of well-defined interfaces. This allows the WAP stack to be used for applications and services not currently specified by WAP, for example applications such as MMHS.

6.2 The WDP Service Interface

The WDP protocol uses a single service primitive T-DUnitdata. WDP may also receive a T-DError primitive if the WDP protocol layer cannot execute the requested transmission.

6.2.1 T-DUnitdata

T-DUnitdata is the primitive used to transmit data as a datagram. T-DUnitdata does not require an existing connection to be established. A T-DUnitdata.Req can be sent to the WDP layer at any time.

Table 6.2

Primitive Parameter	T-DUnitdata	
	req	***ind***
Source Address	M	M(=)
Source Port	M	M(=)
Destination Address	M	O(=)
Destination Port	M	O(=)
User Data	M	M(=)

6.2.1.1 Source Address

The source address is the unique address of the device making a request to the WDP layer. The source address may be an MSISDN number, IP address, X.25 address or other identifier. In this profile the use of the IP address is mandatory.

6.2.1.2 Source Port

The application address associated with the source address of the requesting communication instance.

6.2.1.3 Destination Address

The destination address of the user data submitted to the WDP layer. The destination address may be an MSISDN number, IP address, X.25 address or other identifier. In this profile the use of the IP address is mandatory.

6.2.1.4 Destination Port

The application address associated with the destination address for the requested communication instance.

6.2.1.5 User Data

The user data is carried by the WDP protocol. The unit of data submitted to or received from the WDP layer is also referred to as the Service Data Unit. This is the complete unit of data, which the higher layer has submitted to the WDP layer for transmission. The WDP layer will transmit the Service Data Unit and deliver it to its destination without any manipulation of its content.

6.2.2 T-DError

The T-DError primitive is used to provide information to the higher layer when an error occurs which may impact the requested service. A T-DError Indication may be issued by the WDP layer only after the higher layer has made a request to the WDP layer, such as by issuing a T-DUnitdata.request. The T-DError primitive is used when the WDP layer is unable to complete the requested service due to a local problem. It is not used to inform the upper layer of network errors external to the device/server. An example would be if the upper layer issues a T-DUnitdata.request containing an PDU which is larger than the maximum size PDU allowed by the specific WDP implementation. In this case a T-DError Indication would be returned to the upper layer with an error code indicating the PDU size is too large.

Table 6.3

Primitive Parameter	**T-DError**	
	req	***ind***
Source Address	–	O
Source Port	–	O
Destination Address	–	O
Destination Port	–	O
Error Code	–	M

6.2.2.1 Error Code

An error code carried by the D-Error primitive to the higher layer. The error codes are of local significance only and SHOULD match the “Reason Code “ of the PM-P-ABORT.indication service of the P_Mul Sub-Layer.

7. SECURITY

Annex B of this STANAG defines the security protocol for end-to-end integrity and authentication. Annex E systems MUST be able to process (statically Mandatory) the Annex B protocol for end-to-end security between the tactical users and between strategic and tactical users. Transmission of Certificates and CRLs in the message SHOULD be avoided for connections with low data rate. Instead, other means like pre loading the information in the Directories SHOULD be used to the greatest extent.

If the STANAG 4406 Annex B protocol **is not used** e.g. because of data rate limitations, the information of the security marking MUST be placed in the first line of an ia5-text body part. If the message otherwise contains any ia5-text body parts, the security marking MAY be included as the first line of text in any such body part. If no ia5-text body parts would otherwise be present in the message, then a single ia5-text body part SHALL be added containing only the security marking. The security marking used MUST reflect the applicable security policy. The translation between the Annex B S/MIME ESS label and the “first line of text” label, MAY be performed by the Tactical Interface Agent (TIA).

For NATO, security markings SHALL take the form specified in the *NC3B Technical and Implementation Guidance For Consistent Marking of NATO Information in C3 Systems*, see reference 25.

As with strategic MMHS systems, tactical Annex E systems will for the time being have to provide confidentiality at the lower layers.

8. REFERENCES

1. AC/322(SC/5)WG/5 (MMHS),Document AC/322(SC/5)N/101 (1999): Ratification Draft of STANAG 4406 (Edition 3) Military Message Handling System.

2. Data provided by Mr. Chris Bonatti IECA Inc. (1999).

3. (1990): ISO/IEC: IS 8825, Information Technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).

4. (1991): ISO/IEC: DIS 8825-2, Information Technology - Open Systems Interconnection - Specification of ASN.1 Encoding Rules - Part 2: Packet Encoding Rules.

5. (1988): CCITT X.225 Session Protocol Specification for OSI for CCITT Applications.

6. (1988): CCITT X.226 Presentation Protocol Specification for OSI for CCITT Applications.

7. (1988): CCITT X.227 Association Control Protocol Specification for OSI for CCITT Applications.

8. (1988): CCITT X.228 Reliable Transfer: Protocol Specification.

9. (1998): C. Kenneth Miller, CTO: Data Distribution Over IP in High Error Rate Military Environments , IEEE MILCOM 1998.

10. MMHS WG 258 Tactical MMHS Requirements and Scenario Document.

11. MMHS WG 254 Tactical MMHS Protocol Solutions.

12. MMHS WG 168 Tactical MMHS: Sources of overhead

13. ACP 142 version 1

14. IETF RFC 791 Internet Protocol (IP)

15. IETF RFC 768 User Datagram Protocol (UDP)

16. Wireless Application Protocol (WAP), Wireless Datagram Protocol (WDP) Specification, Wireless Application Protocol Forum Ldt. 1999

17. STANAG 5066 (Edition 1), AC/322(SC/6)N/277

18. IETF RFC 1950 ZLIB Compressed Data Format Specification version 3.3

19. IETF RFC 1951 Compressed Data Format Specification version 1.3

20. IETF RFC 1166 Internet Numbers

21. ISO10731 “Information Technology - Open Systems Interconnection - Basic Reference Model - Conventions for the Definition of OSI Services”, ISO/IEC 10731:1994.

22. IETF RFC 2119 “Key words for use in RFCs to Indicate Requirement Levels”

23. IETF RFC 1236 “IP to X.121 Address Mapping for DDN”

24. STANAG 4406 Annex H, “NATO Security Label Guidance for MMHS”.

25. AC/322-WP(2003)022 “NATO Policy for Consistent Marking of NATO Information”

A ADAPTION OF WAP WDP TO STANAG 5066 SERVICES

The STANAG 5066 provides both a reliable (ARQ) data link service and an unreliable broadcast service. As the P_Mul Sub-Layer will take care of the reliability by use of checksums, acknowledgments and retransmissions, this profile may use the Unreliable Datagram Service of STANAG 5066. If the message to be transferred is large it may be considered to use the Reliable Connection-Oriented Service.

A.1 If the IP network protocol is used

If a network protocol is needed for addressing and routing, the IP protocol [ref. 14] SHALL be used together with the “Robust IP header compression” as defined in the IETF RFC 3095 and RFC 3096. The WAP WDP protocol defines the mapping onto IP and the STANAG 5066 defines how IP is to be used over this protocol (See STANAG 5066 Annex F.10). According to Annex F.10, IP may be used over STANAG 5066 with or without the support of the ARQ service that provides a reliable channel. If the multicast functionality of the P_Mul protocol is to be utilised, the non-ARQ mode MUST be used. Since the P_Mul functionality takes care of the reliability, the non-ARQ mode SHOULD also be used for single recipient scenarios. However if the message is large the ARQ-mode MAY be considered as defined in STANAG 5066 F.10.2.

A.2 If no network protocol is used

Some scenarios do not need a network protocol for addressing and/or routing. Such scenarios usually include “one-hop” communication directly between the originator and recipient, and do not involve any intermediate or transit nodes. In such scenarios, the WAP WDP protocol SHOULD be mapped directly onto the STANAG 5066 services.

STANAG 5066 Annex F8 defines a simple Unreliable Datagram-Oriented Protocol (UDOP) using the non-ARQ services of the HF subnetwork, with a minimal header to support multiplexed datagram delivery. Since non-ARQ services are used, the UDOP may support a multicast service through the use of group addresses within the HF Subnetwork. If the multicast functionality of the P_Mul protocol is to be utilised, the non-ARQ mode MUST be used. This service SHOULD also be used for all scenarios whether the multicast functionality of P_Mul is utilised or not. The P_Mul sub-layer will take care of checksums, acknowledgments and retransmissions, and that functionality will not be needed at the STANAG 5066 link-level as well. However if the message is large the Reliable Connection-Oriented Protocol (RCOP) may be considered as defined in STANAG 5066 F.7.

Address mapping between WAP WDP and the STANAG 5066 subnetwork has to be resolved, but this task is not within the scope of this STANAG.

For Broadcast Data Exchange see STANAG 5066 Annex A1.1.3, C.1.1 and F.8.

B ECHO PROFILES SET

B.1 Use of the STANAG 4406 Annex A Profiles

Tactical messaging implementations conforming to STANAG 4406 Annex E shall conform to the MBS requirements of Annex A and any applicable strategic MMHS profile requirements except as amended herein. An exception is the omission of the Application Service Elements ACSE and RTSE, and the omission of the Presentation and Session layers, which are mandated in STANAG 4406 Annex A (Section 2 Part 2). In replacement of these protocols, the protocols defined by the Tactical Adaptation Sub-Layer, the P_Mul Sub-Layer and the WAP Transport Layer SHALL be used as specified in this Annex E.

The support requirements for the different tactical interfaces and the new protocol elements of the Tactical Adaptation Sub-Layer are defined in the text of this Annex E. The support requirements for the elements of service defined ACP 142, are given in Appendix B2 to this Annex E.

It is important to note that in the profile defined in STANAG 4406 Annex A, not very many of the protocol elements are classified as **dynamically mandatory** (mr), which means that they have to be generated for every instance of a message. A protocol element marked as **mandatory (m),** only means that the element or feature has to be supported. It is only required that the implementation shall be able to generate the element, and/or receive the element and perform all associated procedures (i.e., implying the ability to handle both the syntax and semantics of the element). In a tactical environment one should be restrictive with which of these protocol elements that are generated, in order not to overload the tactical communication links.

B.2 Profile for ACP 142

B.2.1 Introduction

This profile describes the classifications of the fields of the Protocol Data Units (PDUs) defined in ACP 142. The substance of the classification scheme is based on conventions developed in the International Standardized Profiles (ISPs). The conventions are also used in both STANAG 4406 and ACP 123. This classification scheme is used to specify the support level of arguments and other protocol features for the ACP 142 protocol.

B.2.2 Referenced documents

[ref.13] ACP 142 Version 1

B.3 Protocol Classification and Conformance

This section describes the profile of the Protocol Data Units (PDUs) defined in the ACP 142 Version 1 specification.

B.3.1 Profile Support Classifications

In order to define a meaningful profile, it is necessary to establish the classification rules for support requirements. The following classification scheme is used as a basis for the profile. The substance of the classification scheme is based on conventions developed in the International Standardized Profiles (ISPs).

This classification scheme is used to specify the support level of arguments, results and other protocol features for the ACP 142 protocol. The classification of information objects and items (elements) is relative to that of the containing information element, if any. Where the constituent elements of a non-primitive element are not individually specified, then each shall be considered to have the classification of that element. Where the range of values to be supported for an element is not specified, then all values defined in the ACP 142 definition and associated procedures shall be supported.

B.3.1.1 Static Capability

The following classifications are used in this profile to specify static conformance requirements – i.e. capability.

mandatory support (m): The element or feature shall be supported. An implementation shall be able to generate the element, and/or receive the element and perform all associated procedures (i.e., implying the ability to handle both the syntax and semantics of the element) as relevant, as specified in ACP 142 definition and associated procedures. Where support for origination (generation) and reception are not distinguished, then both capabilities shall be assumed.

NOTE – Where required by the base standards, mandatory support also implies that the implementation shall be able to pass the element on the origination port/reception port to/from the corresponding element on the submission port/delivery port/retrieval port.

optional support (o): An implementation is not required to support the element or feature. If support is claimed, then the element shall be treated as if it were specified as mandatory support. If support for origination is not claimed, then the element is not generated. If support for reception is not claimed, then an implementation may ignore the element on delivery, but will not treat it as an error.

conditional support (c): The element or feature shall be supported under the specific conditions specified in the profile. If these conditions are met, the element shall be treated as if it were specified as mandatory support. If these conditions are not met, the element shall be treated as if it were specified as optional support (unless otherwise stated).

out of scope (i): The element or feature is outside the scope of this profile – i.e., it will not be the subject of a conformance test.

not applicable (–): The element or feature is not applicable in the particular context in which this classification is used.

B.3.1.2 Dynamic Behavior

The above classifications are used in this profile to specify static conformance requirements (i.e., capability). Default dynamic conformance requirements (i.e., behavior) are as specified in the ACP 142 definition and associated procedures. However, in a few cases it has been necessary to specify additional dynamic conformance requirements in this profile. These are specified using a second classification code for an element as follows.

required (r): The element or feature shall always be present. An implementation shall ensure that the element is always generated or otherwise used, as appropriate. Absence of the element on reception shall result in termination or rejection of the communication with an appropriate error indication as specified in the ACP 142 definition and associated procedures.

prohibited (x): The element or feature shall not be originated by an implementation claiming conformance to this profile. If the element is received it may be treated as a protocol violation unless otherwise stated.

B.4 Detailed Profile Classifications

This profile defines the detailed support requirements for ACP 142 interoperability. The profile requirements are summarised in Table B-1.

Table B-1 – ACP 142 Interoperability Profile

Ref.	Element	Profile		Comments
		Orig.	Rec.	
	Address_PDU			
1.1	Length_of_PDU	mr	m	
1.2	Priority	m	m	
1.3	MAP	mr	m	

Ref.	Element	Profile		Comments
		Orig.	Rec.	
1.4	PDU_Type	mr	m	
1.5	Total_Number_of_PDUs	mr	m	
1.6	Checksum	mr	m	
1.7	Source_ID	mr	m	
1.8	Message_ID	mr	m	
1.9	Expiry_Time	m	m	
1.10	Count_of_Destination_Entries	mr	m	
1.11	Length_of_Reserved_Field	mr	m	
1.12	List of Destination_Entries	mr	m	See row 2.
2	**List of Destination_Entries**			
2.1	One Destination_Entry			
2.1.1	Destination_ID	mr	m	
2.1.2	Message_Sequence_Number	mr	m	
2.1.3	Reserved Field	o	o	
3	**Data_PDU**			
3.1	Length_of_PDU	mr	m	
3.2	Priority	m	m	
3.3	PDU_Type	mr	m	
3.4	Sequence_Number_of_PDU	mr	m	
3.5	Checksum	mr	m	
3.6	Source_ID	mr	m	
3.7	Message_ID	mr	m	
3.8	Fragment of Data	mr	m	
4	**Discard_Message_PDU**			
4.1	Length_of_PDU	mr	m	
4.2	Priority	m	m	
4.3	PDU_Type	mr	m	
4.4	Checksum	mr	m	
4.5	Source_ID	mr	m	
4.6	Message_ID	mr	m	
5	**Ack_PDU**			
5.1	Length_of_PDU	mr	m	

Ref.	Element	Profile		Comments
		Orig.	Rec.	
5.2	Priority	m	m	
5.3	PDU_Type	mr	m	
5.4	Checksum	mr	m	
5.5	Count_of_Ack_Info_Entries	mr	m	
5.6	List of Ack_Info_Entries	mr	m	See row 6.
6	**List of Ack_Info_Entries**			
6.1	**One Ack_Info_Entry**			
6.1.1	Ack_Info_Entry	mr	m	
6.1.2	Length_of_Ack_Info_Entry	mr	m	
6.1.3	Source_ID	mr	m	
6.1.4	Message_ID	mr	m	
6.1.5	List_of_Missing_Data_PDU_Seq_Numbers	m	m	See row 7.
7	**List_of_Missing_Data_PDU_Seq_ Numbers**			
7.1	**One Missing_Data_PDU_Seq_ Number**			
7.1.1	Missing_Data_PDU_Seq_Number	mr	m	
8	**Request_PDU**			
8.1	Length_of_PDU	mr	m	
8.2	PDU_Type	mr	m	
8.3	Checksum	mr	m	
8.4	Source_ID	mr	m	
8.5	Message_ID	mr	m	
8.6	Multicast_Group_Address	mr	m	
9	**Reject_PDU**			
9.1	Length_of_PDU	mr	m	
9.2	PDU_Type	mr	m	
9.3	Checksum	mr	m	
9.4	Source_ID	mr	m	
9.5	Message_ID	mr	m	
9.6	Multicast_Group_Address	mr	m	
10	**Release_PDU**			
10.1	Length_of_PDU	mr	m	

Ref.	Element	Profile		Comments
		Orig.	Rec.	
10.2	PDU_Type	mr	m	
10.3	Checksum	mr	m	
10.4	Source_ID	mr	m	
10.5	Message_ID	mr	m	
10.6	Multicast_Group_Address	mr	m	
11	**Announce_PDU**			
11.1	Length_of_PDU	mr	m	
11.2	MAP	mr	m	
11.3	PDU_Type	mr	m	
11.4	Count_of_Destination_IDs	mr	m	
11.5	Checksum	mr	m	
11.6	Source_ID	mr	m	
11.7	Message_ID	mr	m	
11.8	Expiry_Time	m	m	
11.9	Multicast_Group_Address	mr	m	
11.10	List of Destination_IDs	mr	m	See row 12
12	**List of Destination_IDs**			
12.1	Destination_ID			
12.1.1	Destination_ID	mr	m	

ANNEX F

STANDARDIZED PROFILE FMH20(D) – GENERAL MS ATTRIBUTES

Standardized Profile

TITLE: Information technology – Standardized Profiles – Military Message Handling Systems – Message Store Attributes FMH20(D) – General MS Attributes

This document is a Standardized Profile (SP) for Military Message Handling System (MMHS) requirements for general Message Store (MS) attributes. It is outside the scope of the current Taxonomy Framework for International Standardized Profiles (ISP). This SP is a content-independent profile for the general MS attributes as defined in CCITT Rec. X.413 (1992) | ISO/IEC 10021-5 (1990).

Introduction

This Standardized Profile (SP) is defined within the context of functional standardization, in accordance with the principles specified by ISO/IEC TR 10000, "Framework and Taxonomy of International Standardized Profiles". The context of functional standardization is one part of the overall field of Information Technology (IT) standardization activities – covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards to promote system interoperability and to provide a basis for the development of uniform, internationally recognized system tests.

One of the most important roles for a SP is to serve as the basis for the development of recognized tests. SPs also guide implementors in developing systems that fit the needs of the MMHS. SPs are produced not simply to 'legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other SPs is crucial to the successful realization of this goal.

FMH20(D) covers information representation by Military Messaging User Agents (MM-UA) and Military Messaging Message Stores (MM-MS). It specifies support of the general MS attributes defined in CCITT Rec. X.413 (1992) | ISO/IEC 10021-5 (1990).

FMH20(D) contains one normative appendix:

Appendix A SPICS Requirements List for FMH20(D)

Information technology – Standardized Profiles – Military Message Handling Systems – Message Store Attributes

FMH20(D) – General MS Attributes

1 Scope

1.1 General

FMH20(D) covers the representation of information, specifically MS attributes, by MM-MSs and MM-UAs.

1.2 Position within the taxonomy

FMH20(D) specifies the profile which states requirements for general MS Attributes.

1.3 Scenario

The model used is one of information representation of MS attributes by the MM-MS and MM-UA (see figure 1).

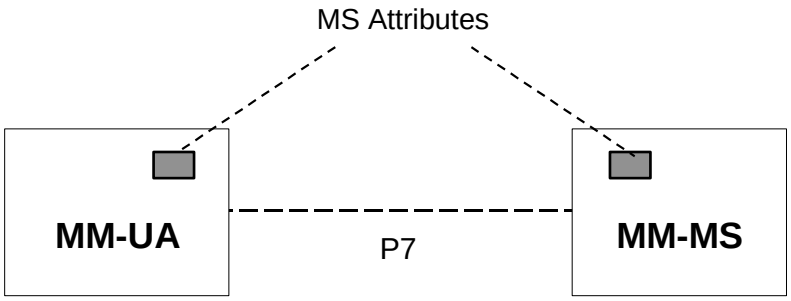


Figure 1 – FMH20(D) Scenario

There are no Open System Interconnection (OSI) upper layer services and protocols within the scope of the FMH20(D) profile.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of FMH20(D). At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on FMH20(D) are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by SPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

Technical corrigenda to the base standards referenced are listed in appendix B of ISO/IEC 10611-5.

NOTE – References in the body of FMH20(D) to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

ACP 123(B): *Common Messaging Strategy and Procedures.*

ISO/IEC 10021-1: 1990, *Information technology – Text Communication – Message-Oriented Text Interchange Systems (MOTIS)* – Part 1: *Service Overview*. *[see also CCITT Recommendation X.400(1992)]*

ISO/IEC 10021-2: 1990, *Information technology – Text Communication – Message-Oriented Text Interchange Systems (MOTIS)* – Part 2: *Overall Architecture. [see also CCITT Recommendation X.402(1992)]*

SO/IEC 10021-5: 1990, *Information technology – Text Communication – Message-Orientated Text Interchange Systems (MOTIS)* – Part 5: *Message Store: Abstract Service Definition. [see also CCITT Recommendation X.413 (1992)]*

CCITT Recommendation X.400(1992), *Message handling system and service overview*.

CCITT Recommendation X.402(1992), *Message handling systems: Overall architecture.*

CCITT Recommendation X.413(1992), *Message handling systems: Message store: Abstract service definition.*

MHS Implementors' Guide, Version 11, July 1994 (ITU-T *Special Rapporteur's Group on Message Handling Systems and ISO/IEC JTC1/SC18/WG4 SWG on Messaging).*

(Application for copies of these documents should be addressed to the American National Standards Institute, 11 West 42nd Street, NY, NY 10036 or to ISO, Van Demonstrate 94, 1013 CN Amsterdam, Netherlands.)

3 Definitions

For the purposes of FMH20(D), the following definitions apply. Terms used in FMH20(D) are defined in the referenced base standard. In addition, the following terms are defined.

3.1 General

Base standard : the base standard referred to in this profile is the X.413 recommendation.

Basic requirement : a general MS attributes specified in the base standard which is required to be supported by all MMHS implementations conforming to this SP.

3.2 Support classification

To specify the support level of features for FMH21(D), the following terminology is defined.

3.2.1 Static capability

The following classification is used in FMH20(D) to specify static conformance requirements – i.e., capability.

mandatory support (m) : the element or feature shall be supported. An implementation shall be able to generate the element, and/or receive the element and perform all associated procedures (i.e., implying the ability to handle both the syntax and semantics of the element) as relevant, as specified in the base standard. Where support for generation and reception are not distinguished, then both capabilities shall be assumed.

optional support (o) : an implementation is not required to support the element. If support is claimed, the element shall be treated as if it were specified as mandatory support. If support for generation is not claimed, then the element is not generated. If support for reception is not claimed, then an implementation may ignore the element on reception, but will not treat it as an error.

4 Abbreviations and Acronyms

ACP	Allied Communication Publication
CCITT	International Telephone and Telegraph Consultative Committee
EoS	Element of Service
IEC	International Electrotechnical Commission
ISO	International Standards Organization
ISP	International Standardized Profile
ISPICS	International Standardized Profiles Implementation Conformance Statement
ITU	International Telecommunications Union
ITU-T	ITU Telecommunications Standardization Sector
MHS	Message Handling System
MM	Military Message
MMHS	Military Message Handling System
MM-	Military Messaging
MM-MS	Military Messaging Message Store
MM-UA	Military Messaging User Agent

MTS	Message Transfer System
MOTIS	Message-Oriented Text Interchange Systems
MS	Message Store
MTS	Message Transfer System
OSI	Open Systems Interconnection
SP	Standardized Profiles
SPICS	Standardized Profiles Implementation Conformance Statement
UA	User Agent

Support level for protocol elements and features (see clause 3.2):

m	mandatory full support
o	optional support

5 Conformance

The scope of conformance to profile FMH20(D) covers MM-MSs and MM-UAs only. Conformance to profile FMH20(D) does not imply the provision of a standard OSI communications protocol for access to the Message Transfer System (MTS).

FMH20(D) states requirements upon implementations to achieve interworking. A claim of conformance to FMH20(D) is a claim that all requirements in the relevant base standard are satisfied, and that all requirement in the following clauses and in appendix A of FMH20(D) are satisfied. Appendix A states the relationship between these requirements and those of the base standard.

5.1 Conformance statement

For each implementation claiming conformance to profile FMH20(D), an International Standard Profiles Implementation Conformance Statement (ISPICS) shall be made available stating support or non-support of each option identified FMH20(D). The ISPICS Proforma in ISO/IEC 10611-5 shall be used to generate the ISPICS.

APPENDIX A

(normative)

SPICS REQUIREMENTS LIST FOR FMH20(D)

In the event of a discrepancy becoming apparent in the body of FMH20(D) and the tables in this appendix, this appendix is to take precedence.

This appendix specifies the support constraints and characteristics of FMH20(D) on what shall or may appear in the implementation columns of a ISPICS.

Clause A.1 specifies the basic requirements for conformance to profile FMH20(D).

In each table, the "Profile" column reflects the level of support required for conformance to this SP (using the classification and notation defined in clause 3.2).

A.1 Basic requirements

A.1.1 General Attributes

Ref	Attribute	UA	MS
1	ms-child-sequence-numbers	o	m
2	ms-content	m	m
3	mt-content-confidentiality-algorithm-identifier	o	o
4	mt-content-correlator	o	m
5	mt-content-identifier	o	m
6	mt-content-integrity-check	o	o
7	ms-content-length	o	m
8	ms-content-returned	o	m
9	content-type	m	m
10	conversion-with-loss-prohibited	o	m
11	ms-converted-eits	o	m
12	ms-creation-time	o	m
13	ms-delivered-eits	o	m
14	delivery-flags	o	m
15	dl-expansion-history	o	m
16	entry-status	m	m
17	entry-type	o	m
18	intended-recipient-name	o	m
19	message-delivery-envelope	m	m
20	message-delivery-identifier	o	m
21	mt-message-delivery-time	o	m

Ref	Attribute	UA	MS
22	message-origin-authentication-check	o	o
23	message-security-label	o	o
24	message-submission-time	o	m
25	message-token	o	o
26	original-eits	o	m
27	originator-certificate	o	o
28	originator-name	m	m
29	other-recipient-names	o	m
30	parent-sequence-number	o	m
31	per-recipient-report-delivery-fields	o	m
32	mt-priority	m	m
33	proof-of-delivery-request	o	o
34	redirection-history	o	m
35	report-delivery-envelope	m	m
36	reporting-dl-name	o	m
37	reporting-mta-certificate	o	o
38	report-origin-authentication-check	o	o
39	security-classification	o	o
40	sequence-number	m	m
41	subject-submission-identifier	o	m
42	this-recipient-name	o	m

ANNEX G

STANDARDIZED PROFILE FMH21(D) – MM-SPECIFIC MS ATTRIBUTES

Standardized Profile

TITLE: Information technology – Standardized Profiles – Military Message Handling Systems – Message Store Attributes FMH21(D) – MM-specific MS Attributes

This document is a Standardized Profile (SP) for Military Message Handling System (MMHS) requirements for Military Message (MM) specific Message Store (MS) attributes. It is outside the scope of the current Taxonomy Framework for International Standardized Profiles (ISP). This SP is a profile of the MM-specific MS attributes as defined in the Allied Communication Publication (ACP) 123.

Introduction

This Standardized Profile (SP) is defined within the context of functional standardization, in accordance with the principles specified by ISO/IEC TR 10000, "Framework and Taxonomy of International Standardized Profiles". The context of functional standardization is one part of the overall field of Information Technology (IT) standardization activities – covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards to promote system interoperability and to provide a basis for the development of uniform, internationally recognized system tests.

One of the most important roles for a SP is to serve as the basis for the development of recognized tests. SPs also guide implementors in developing systems that fit the needs of the MMHS. SPs are produced not simply to 'legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other SPs is crucial to the successful realization of this goal.

FMH21(D) covers information representation by Military Messaging User Agents (MM-UA) and Military Messaging Message Stores (MM-MS). It specifies support of the MM-specific attributes defined in ACP 123.

FMH21(D) contains one normative appendix:

Appendix A SPICS requirements List for FMH21(D)

Information technology – Standardized Profiles – Military Message Handling Systems – Message Store Attributes

FMH21(D) – MM-specific MS Attributes

1 Scope

1.1 General

FMH21(D) covers the representation of information, specifically MS attributes, by MM-MSs and MM-UAs.

1.2 Position within the taxonomy

FMH21(D) specifies the profile which states requirements for MM-specific MS Attributes.

1.3 Scenario

The model used is one of information representation of MM-specific MS attributes by the MM-MS and MM-UA (see figure 1).

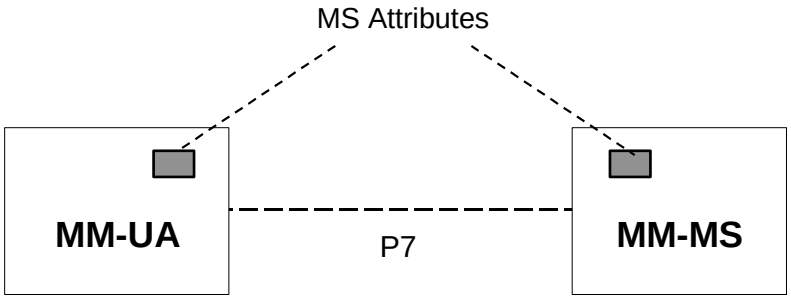


Figure 1 – FMH21(D) Scenario

There are no Open System Interconnection (OSI) upper layer services and protocols within the scope of the FMH21(D) profile.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of FMH21(D). At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on FMH21(D) are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by SPs to such documents is that they may be specific to a particular edition. Members of IEC and

ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

Technical corrigenda to the base standards referenced are listed in annex B, appendix B of ACP 123.

NOTE – References in the body of FMH21(D) to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

ACP 123(B): *Common Messaging Strategy and Procedures.*

ISO/IEC 8859: 1990, *Information processing – 8-bit single-byte coded graphic character sets.*

ISO/IEC 8613-1: 1993, *Information processing – Text and office systems – Open Document Architecture (ODA) and interchange format – Part 1: Introduction and general principles.*

ISO/IEC 10021-1: 1990, *Information technology – Text Communication – Message-Oriented Text Interchange Systems (MOTIS)* – Part 1: *Service Overview. [see also CCITT Recommendation X.400(1992)]*

ISO/IEC 10021-2: 1990, *Information technology – Text Communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 2: Overall Architecture. [see also CCITT Recommendation X.402(1992)]*

ISO/IEC 10021-5: 1990, *Information technology – Text Communication – Message-Orientated Text Interchange Systems (MOTIS) – Part 5: Message Store: Abstract Service Definition. [see also CCITT Recommendation X.413 (1992)]*

CCITT Recommendation X.400(1992), Message handling system and service overview.

CCITT Recommendation X.402(1992), Message handling systems: Overall architecture.

CCITT Recommendation X.413(1992), Message handling systems: Message store: Abstract service definition.

(Application for copies of these documents should be addressed to the American National Standards Institute, 11 West 42nd Street, NY, NY 10036 or to ISO, Van Demonstrate 94, 1013 CN Amsterdam, Netherlands.)

3 Definitions

For the purposes of FMH21(D), the following definitions apply. Terms used in FMH21(D) are defined in the referenced base standards. In addition, the following terms are defined.

3.1 General

MM base standard: the base standard referred to in this profile is ACP 123.

Basic requirement: an MM-specific MS attribute which is required to be supported by all MMHS implementations conforming to this SP.

Functional group: a specification of one or more related MM-specific MS attributes specified in the base standard which together support a significant optional area of functionality.

3.2 Support classification

To specify the support level of features for FMH21(D), the following terminology is defined.

3.2.1 Static capability

The following classifications are used in FMH21(D) to specify static conformance requirements – i.e., capability.

mandatory support (m): the element or feature shall be supported. An implementation shall be able to generate the element, and/or receive the element and perform all associated procedures (i.e., implying the ability to handle both the syntax and semantics of the element) as relevant, as specified in the MM base standard. When support for generation and reception are not distinguished, then both capabilities shall be assumed.

optional support (o): an implementation is not required to support the element. If support is claimed, the element shall be treated as if it were specified as mandatory support. If support for generation is not claimed, then the element is not generated. If support for reception is not claimed, then an implementation may ignore the element on reception, but will not treat it as an error.

out of scope (i): the element is outside the scope of FMH21(D) – i.e., it will not be the subject of a SP conformance test.

4 Abbreviations and Acronyms

ACP	Allied Communication Publication
ACP127	ACP 127 Interworking
CCITT	International Telephone and Telegraph Consultative Committee
FG	Functional group

IEC	International Electrotechnical Commission
IO-ICS	Information Object Implementation Conformance Statement
ISO	International Standards Organization
ISP	International Standardized Profile
ITU	International Telecommunications Union
ITU-T	ITU Telecommunications Standardization Sector
MHS	Message Handling System
MM	Military Message
MMHS	Military Message Handling System
MM-	Military Messaging
MM-MS	Military Messaging Message Store
MM-UA	Military Messaging User Agent
MOTIS	Message-Oriented Text Interchange Systems
MS	Message Store
MTS	Message Transfer System
OSI	Open Systems Interconnection
SP	Standardized Profiles
SPICS	Standardized Profiles Implementation Conformance Statement
UA	User Agent.

Support level for protocol elements and features (see clause 3.2):

m	mandatory full support
o	optional support
i	out of scope

5 Conformance

The scope of conformance to profile FMH21(D) covers MM-MSs and MM-UAs only. Conformance to profile FMH21(D) does not imply the provision of a standard OSI communications protocol for access to the Message Transfer System (MTS).

FMH21(D) states requirements upon implementations to achieve interworking. A claim of conformance to FMH21(D) is a claim that all requirements in the relevant base standard are satisfied, and that all requirements in the following clauses and in appendix A of FMH21(D) are satisfied. Appendix A states the relationship between these requirements and those of the base standard.

5.1 Conformance statement

For each implementation claiming conformance to profile FMH21(D), an Information Object Information Implementation Conformance Statement (IO-ICS) shall be made available stating support or non-support of each option identified FMH21(D). The IO-ICS Proforma in annex B of ACP 123 shall be used to generate the IO-ICS.

Appendix A

(normative)

SPICS REQUIREMENTS LIST FOR FMH21(D)

In the event of a discrepancy becoming apparent in the body of FMH21(D) and the tables in this appendix, this appendix is to take precedence.

This appendix specifies the support constraints and characteristics of FMH21(D) on what shall or may appear in the implementation columns of an IO-ICS.

Clause A.1 specifies the basic requirements for conformance to profile FMH21(D) (reference numbers correspond to items in the IO-ICS). Clause A.2 specifies the additional requirements if support of the ACP 127 FG is claimed.

In each table, the "Profile" column reflects the level of support required for conformance to this SP (using the classification and notation defined in clause 3.2).

A.1 Basic requirements

A.1.1 MM-specific Attributes

Ref	Element	Profile	
		UA	MS
1	acknowledgment-mode	o	m
2	authorizing-users	o	m
3	auto-forward-comment	o	m
4	auto-forwarded	o	m
5	bilaterally-defined-body-parts	o	o
6	blind-copy-recipients	o	m
7	body	m	m
8	conversion-eits	o	m
9	copy-recipients	o	m
10	discard-reason	o	m
11	encrypted-body-parts	o	o
12	encrypted-data	o	o
13	encrypted-parameters	o	o
14	expiry-time	o	m
15	extended-body-part-types[1]	m	m
16	g3-facsimile-body-parts	o	o
17	g3-facsimile-data	o	o
18	g3-facsimile-parameters	o	o

Ref	Element	Profile	
		UA	MS
19	g4-class1-body-parts	o	o
20	heading	m	m
21	ia5-text-body-parts	o	m
22	ia5-text-data	o	o
23	ia5-text-parameters	o	o
24	importance	i	i
25	incomplete-copy	o	m
26	ipm-entry-type	m	m
27	ipm-preferred-recipient	o	m
28	ipm-synopsis	o	m
29	ipn-originator	o	m
30	languages	o	m
31	message-body-parts	o	m
32	message-data	o	o
33	message-parameters	o	o
34	mixed-mode-body-parts	o	o
35	nationally-defined-body-parts	o	o
36	non-receipt-reason	o	m
37	nrn-requestors	o	m
38	obsoleted-mms	o	m
39	originator	o	m
40	primary-recipients	o	m
41	receipt-time	o	m
42	related-mms	o	m
43	replied-to-ipm	o	m
44	reply-recipients	o	m
45	reply-requestors	o	m
46	reply-time	o	m
47	returned-ipm	o	o
48	rn-requestors	o	m
49	sensitivity	i	i
50	subject	o	m
51	subject-ipm	m	m
52	suppl-receipt-info	o	o
53	teletex-body-parts	o	o
54	teletex-data	o	o
55	teletex-parameters	o	o
56	this-ipm	m	m
57	videotex-body-parts	o	o
58	videotex-data	o	o
59	videotex-parameters	o	o
60	voice-body-parts	o	o
61	voice-data	o	o
62	voice-parameters	o	o

Ref	Element	Profile	
		UA	MS
63	acp127-message-identifier	o	o
64	address-list-indicator	o	o
65	codress-message	o	o
66	copy-precedence	m	m
67	distribution-codes	m	m
68	exempted-address	m	m
69	extended-authorisation-info	m	m
70	handling-instructions	o	o
71	message-instructions	m	m
72	message-type	m	m
73	originator-reference	o	m
74	originator-plad	o	o
75	other-recipients-indicator	o	m
76	pilot-forwarding-info	o	o
77	primary-precedence	m	m
78	acp-127-notification-request	o	o
79	acp127-notification-response	o	o
80	sic-codes	m	m
81	distribution-extensions	o	o

Notes:

1 See table A.1.2.1 for extended-body-part-types

A.1.1.1 Extended body part support

Ref	Element	Profile	
		UA	MS
1	ia5-text-body-part	o	m
2	g3-facsimile-body-part	o	o
3	g4-class-1-body-part	o	o
4	teletex-body-part	o	o
5	videotex-body-part	o	o
6	encrypted-body-part	i	i
7	message-body-part	o	m
8	mixed-mode-body-part	o	o
9	bilaterally-defined-body-part	o	o
10	nationally-defined-body-part	o	o
11	general-text-body-part	o	m
12	file-transfer-body-part	o	o
13	voice-body-part	i	i
14	oda-body-part	o	o
15	aDatP3-body-part	m	m
16	corrections-body-part	o	o

Ref	Element	Profile	
		UA	MS
17	forwarded-encrypted-body-part	o	o
18	mm-message-body-part	m	m
19	acp127data-body-part	o	o

A.1.2 MM Auto-Action Registration Parameters

Ref	Element	Profile	
		UA	MS
4	other-parameters		
4.1	auto-forwarding-comment	o	o
4.2	cover-note	o	o
4.3	this-ipm-prefix	o	o

A.2 Optional functional groups

The following requirements are additional to those specified in A.1 support of the optional ACP 127 FG is claimed (references are to the corresponding entries in A.1).

A.2.1 ACP 127 Interworking (ACP127) MM-specific Attributes

Ref	Element	Profile	
		UA	MS
63	acp127-message-identifier		m
65	codress-message		m
74	originator-plad		m
76	pilot-forwarding-info		m
78	acp-127-notification-request		m
79	acp127-notification-response		m

ANNEX H

INFORMATION OBJECT IMPLEMENTATION CONFORMANCE STATEMENT PROFORMA

1 Scope

This annex is an Information Object Implementation Conformance Statement (IO-ICS) Proforma for the MM information object as specified in ACP 123. This IO-ICS Proforma is in compliance with the relevant requirements, and in accordance with the relevant guidance for IO-ICS Proforma given in ISO/IEC 9642-7.

Details of the use of this proforma are provided in Appendix A.

The scope of this annex is the specification of the conformance statements for the content specific functionality for any implementation that supports the MM content type. It has been developed by examining the ASN.1 defined in Annex A of this document. If an ASN.1 element is optional then the corresponding classification applied to the element in this IO-ICS Proforma is optional. If an ASN.1 element is optional then the corresponding classification applied to the element in this IO-ICS Proforma is mandatory. Implementors shall state herein the level of support for all MM EoS and protocol elements.

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this annex of ACP 123. At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this ICS are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by ICSs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

Technical corrigenda to the base standards referenced are listed in annex B.

NOTE - References in the body of this IO-ICS to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

- ISO/IEC 9646-1:1991, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework Part 1: General concepts*.

- ISO/IEC 9646-7:1992, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework Part 7: Implementation Conformance Statements.*

- ISO/IEC 8824:1990, *Information processing systems – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1).*

- ISO/IEC 8859:1992, *Information technology – 8-bit single-byte coded graphic character sets.*

- ISO/IEC 8613-1:1993, *Information technology – Open Document Architecture (ODA) and Interchange Format – Part 1: Introduction and general principles.*

- ISO/IEC 10021-1:1990, *Information technology – Text Communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 1: Service Overview. [see also CCITT Recommendation X.400(1992)]*.

- ISO/IEC 10021-2:1990, *Information technology – Text Communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 2: Overall Architecture. [see also CCITT Recommendation X.402(1992)]*.

- ISO/IEC 10021-7:1990, *Information technology – Text Communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 7: Interpersonal messaging system. [see also CCITT Recommendation X.420(1992)]*.

- CCITT Recommendation X.400(1992), *Message handling system and service overview.*

- CCITT Recommendation X.402(1992), *Message handling systems: Overall architecture.*

- CCITT Recommendation X.420(1992), *Message handling systems: Interpersonal messaging system.*

- ISO/IEC 10021-1:1990/Am.2, *Information technology – Message-Oriented Text Interchange System (MOTIS) – Part 1: System and Service Overview, Amendment 2 Message Store Extensions 1994.*

- ISO/IEC 10021-2:1990/Am.1, *Information technology – Message-Oriented Text Interchange System (MOTIS) – Part 2: Overall*

Architecture; Amendment 1: Representation of O/R Addresses for Human Exchange 1994.

- ISO/IEC 10021-2:1990/Am.2, *Information technology – Message-Oriented Text Interchange System (MOTIS) – Part 2: Overall Architecture; Amendment 2: Minor Enhancements: Multinational Organizations and Terminal-form Addresses 1994.*

- MHS Implementors' Guide, Version 11, July 1994 (*ITU-T Special Rapporteur's Group on Message Handling Systems and ISO/IEC JTC1/SC18/WG4 SWG on Messaging).*

3 Definitions

Terms used in this IO-ICS are defined in ACP 123.

This Specification uses the following terms defined in ISO/IEC 9646-1

Implementation Conformance Statement proforma
Implementation Conformance Statement
Information Object Implementation Conformance Statement proforma
Information Object Implementation Conformance Statement

4 Abbreviations

ACP127	ACP 127 Interworking
AMH	Application Message Handling
ASN.1	Abstract Syntax Notation One
EoS	Element of Service
ICS	Implementation Conformance Statement
IO-ICS	Information Object Implementation Conformance Statement
ISP	International Standardized Profile
MHS	Message Handling Systems
MM	Military Messaging (Message)
MS	Message Store
MT	Message Transfer
MTA	Message Transfer Agent
MTS	Message transfer System
OSI	Open Systems Interconnection
UA	User Agent

5 Conventions

The IO-ICS Proforma is designed as an appendix to this annex (see Appendix A).

6 Conformance

The supplier of an information object implementation that is claimed to conform to MM is required to complete a copy of the IO-ICS Proforma provided in Appendix A and is required to provide the information necessary to identify both the supplier and the implementation.

The scope of conformance to this IO-ICS covers content specific functionality for any implementation that supports the MM content type. Conformance to this IO-ICS does not imply the provision of a standard OSI communications protocol for access to the MTS.

This IO-ICS states requirements upon implementations to achieve interworking. A claim of conformance to this IO-ICS is a claim that all requirements in the relevant base standards are satisfied, and that all requirements in the following clauses and in appendix A of this IO-ICS are satisfied. Appendix A states the relationship between these requirements and those of the base standards.

6.1 Conformance statement

For each implementation claiming conformance to ACP 123 as specified in this IO-ICS, an ICS shall be made available stating support or non-support of each option identified in this IO-ICS.

6.2 MHS conformance

This IO-ICS specifies implementation options or selections such that conformant implementations will satisfy the non-procedural conformance requirements of ACP 123 as well as those of ISO/IEC 10021.

Implementations whose information objects conform to ACP 123 as specified in this IO-ICS shall implement all the mandatory support (m) features identified as base requirements in appendix A of this IO-ICS, and shall state which optional support (o) features are implemented. An implementation of any EoS for which a select (s) classification has been assigned in section A.8.1 must demonstrate the user's ability to invoke all legal values for that EoS. An implementation of any EoS for which a display (D) classification has been assigned in section A.8.1 must display some indication of the received value for that EoS to the user.

6.3 Error handling

Various distinguished integer values may be defined in supplements to ACP 123 that are not defined in the base ACP. These are not expected to cross national boundaries without bilateral agreement. When an unknown distinguished value is encountered, it should, in general, not result in an error. The value should be treated transparently or ignored, wherever possible. When an unknown distinguished value is encountered in connection with an EoS that is classified for display (D) in section A.8.1, the implementation should attempt to convey the unknown value to the user.

Appendix A

(normative)

IO-ICS Proforma for ACP 123

A.1 Identifications

A.1.1 Identification of IO-ICS

Item	Question	Response
1	Date of statement (DD/MM/YY)	
2	IO-ICS serial number	
3	System conformance statement cross reference	

A.1.2 Identification of Implementation and/or system

Item	Question	Response
1	Implementation name	
2	Implementation version	
3	Machine name	
4	Machine version	
5	Operating system name	
6	Operating system version	
7	Special configuration	
8	Other information	

A.1.3 Identification of system supplier and/or test laboratory client

Item	Question	Response
1	Organization name	
2	Contact name(s)	
3	Address	
4	Telephone number	
5	Telex number	
6	Fax number	
7	E-mail address	
8	Other information	

A.2 Identification of information object

Item	Question	Response
1	Title, reference number and date of publication of the information object standard	
2	IO version(s)	
3	Addenda/amendments/ corrigenda implemented	
4	Defect reports implemented	

A.3 Global statement of conformance

Item	Question	Response	Comments
1	Are all mandatory base standards requirements implemented?		

NOTE - Answering "No" to this section indicates non-conformance to the information object specification. Unsupported mandatory capabilities are to be identified in the IO-ICS, with an explanation of why the implementation is non-conformant. Such information shall be provided in A.8, "Other information".

A.4 Instructions for completing the IO-ICS Proforma

A.4.1 Definition of support

A capability is said to be supported if the Implementation Under Test (IUT) is able:

- To generate the corresponding service parameters (either automatically or because the end user explicitly requires the capability);
- To interpret, handle and when required make available to the end user the corresponding service parameter(s).

A capability is referred to as either originator capability (when the MHS end-user is acting as an originator) or a recipient capability (when an MHS end-user is acting as a recipient).

An information object element is said to be supported for origination if the IUT is able to generate it under some circumstances (either automatically or because end-user explicitly requires the related capability).

An information object element is said to be supported for reception if it is correctly interpreted and handled and also when required, made available to the end-user.

A.4.2 Base column

The column indicates the level of support required for conformance to MM.

The values are as follows:

m Mandatory support is required. The element or feature is required to be implemented, and shall be fully supported in conformance with the Specification. An implementation shall be able to generate the element, and/or receive the element and perform all associated procedures (i.e., implying the ability to handle both the syntax and semantics of the element) as relevant, as specified in the MM base standards. Where support for origination (generation) and reception are not distinguished, then both capabilities shall be assumed.

NOTE – Where required by the base standard, mandatory support also implies that the implementation shall be able to pass the element on the origination port/reception port to/from the corresponding element on the submission port/delivery port/retrieval port.

o Optional support is permitted for conformance to ACP 123. The capability may be implemented, and if it is implemented it is required to conform to the Specification. An implementation is not required to support the element. If support is claimed, the element shall be treated as if it were specified as mandatory support. If support for origination is not claimed, then the element is not generated. If support for reception is not claimed, then an implementation may ignore the element on delivery, but will not treat it as an error.

c The item is conditional; the support of this item is subject to a predicate which is referenced in the note column. If these predicate's conditions are met, the element shall be treated as if it were specified as mandatory support. If these conditions are not met, the element shall be treated as if it were specified as optional support (unless otherwise stated).

i The element is outside the scope of this IO-ICS – i.e., it will not be the subject of an ICS conformance test.

- In the given context the base Specification makes it impossible to use this capability.

A.4.3 Support column

This column shall be completed by the supplier or implementor to indicate the level of implementation of each item. The proforma has been designed such that the only entries required in that column are:

Y Yes, the item has been implemented;

N No, the item has not been implemented;

- The item is not applicable.

In the IO-ICS Proforma tables, every leading items marked "m" should be supported by the IUT. Sub-elements marked "m" should be supported if the corresponding leading feature is supported by the IUT.

All entries within the IO-ICS shall be made in ink. Alterations to such entries shall be made by crossing out, not erasing nor making the original entry illegible, and writing the new entry alongside. All such alterations to records shall be initialed by the staff making them.

A.4.4 Note Column

The "Note" column has to read as follows:

see xx(xx) Refers to table xx item xx.

Note xx Refers to Note xx.

pxx Refers to predicate xx.

A.4.5 Item column

Each row within the IO-ICS Proforma which requires implementation details to be entered is numbered in a separate column. This numbering is included as a means of uniquely identifying all possible implementation details within the IO-ICS Proforma.

A.4.6 Predicate definitions

If the classification of an Element of Service (EoS) or a Protocol Element is subject to a predicate, support of the item is mandatory if the related predicate is true. Otherwise support of the item is optional.

Within this appendix, predicates are clearly defined where:

p1 Copy Precedence EoS is supported.

p2 Primary Precedence EoS is supported.

p3 ACP 127 Message Identifier EoS is supported.

p4 ACP 127 Notification Request EoS is supported.

p5 ACP 127 Notifications Response EoS is supported.

p6 Authorizing Users Indication EoS is supported.

p7 Auto-forwarded Indication EoS is supported.

p8 Blind Copy Recipient Indication EoS is supported.

p9 Codress Message Indicator EoS is supported.

p10 Corrections EoS is supported.

p11 Cross-referencing Indication EoS is supported.

p12 Distribution Code EoS is supported.

p13 Exempted Addresses EoS is supported.

p14 Expiry Date Indication EoS is supported.

p15 Extended Authorization Info EoS is supported.

p16 Forwarded Message Indication EoS is supported.

p17 Handling Instructions EoS is supported.

p18 Importance Indication EoS is supported.

p19 Incomplete Copy Indication EoS is supported.

p20 Language Indication EoS is supported.

p21 Message Instructions EoS is supported.

p22 Message Type EoS is supported.

p23 Multi-part Body Indication EoS is supported.

p24 Non-receipt Notification Request Indication EoS is supported.

p25 Obsoleting Indication EoS is supported.

p26 Originator Indication EoS is supported.

p27 Originator Reference EoS is supported.

p28 Originator PLAD EoS is supported.

p29 Other Recipient Indicator EoS is supported.

p30 Pilot Forwarded EoS is supported.

p31 Primary and Copy Recipients Indication EoS is supported.

p32 Receipt Notification Request Indication EoS is supported.

p33 Reply Request Indication EoS is supported.

p34 Replying Message Indication EoS is supported.

p35 Sensitivity Indication EoS is supported.

P36 Use of Address List EoS is supported.

p37 If the implementation can originate a request for Receipt or Non-receipt Notifications, then it is mandatory to support receipt of the MN PDU, else it is optional.

p38 If any of the conditions for Non-receipt can occur, all the related fields need to be generatable.

p39 If auto-forwarding is supported, the related fields in an NRN must be supported.

p40 If any of the subsidiary MM-specific parameters are supported then m, else o.

p41 If any of the heading-extensions are supported then support of this element is m, else support is o.

A.5 Capabilities and Options

The following tables list the detailed requirements for MM implementations.

A.5.1 Supported Options

Item	Question	Base	Support	Comments
1	Are all mandatory requirements of the FMH11(D) profile implemented?	o		
2	Are all mandatory requirements of the FMH20(D) profile implemented?	o		
3	Are all mandatory requirements of the FMH21(D) profile implemented?	o		
4	Are all mandatory requirements of the ACP 127 Interworking (ACP127) FG implemented, as defined in FMH11(D)?	o		

A.5.2 MM EoS

A.5.2.1 Basic MM EoS

Item	Element	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec	
1	Copy Precedence	o	o			
2	MM-message Identification	m	m			
3	Primary Precedence	o	o			
4	Subject Indication	m	m			
5	Typed Body	m	m			

A.5.2.2 Optional MM EoS

Item	Element of Service	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	

Item	Element of Service	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
1	ACP 127 Message Identifier	o	o			
2	ACP 127 Notification Request	o	o			
3	ACP 127 Notification Response	o	o			
4	Authorizing Users Indication	o	o			
5	Auto-forwarded Indication	o	m			
6	Blind Copy Recipient Indication	o	o			
7	Body Part Encryption Indication	o	o			
8	Clear Service	o	o			
9	Codress Message indicator	o	o			
10	Corrections	o	o			
11	Cross-referencing Indication	o	o			
12	Distribution Code	o	o			
13	Exempted Addresses	o	o			
14	Expiry Date Indication	o	o			
15	Extended Authorization Info	o	o			
16	Forwarded Message Indication	o	o			
17	Handling Instructions	o	o			
18	Importance Indication	o	o			
19	Incomplete Copy Indication	o	o			
20	Language Indication	o	o			
21	Message Instructions	o	o			
22	Message Type	o	o			
23	Multi-part Body Indication	o	o			
24	Non-receipt Notification Request Indication	o	o			
25	Obsoleting Indication	o	o			
26	Originator Indication	o	o			
27	Originator Reference	o	o			
28	Originator PLAD	o	o			

Item	Element of Service	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
29	Other Recipient Indicator	o	o			
30	Pilot Forwarded	o	o			
31	Primary and Copy Recipients Indication	m	m			
32	Receipt Notification Request Indication	o	o			
33	Reply Request Indication	o	o			
34	Replying Message Indication	m	m			
35	Security Information Labels	o	o			
36	Sensitivity Indication	o	o			
37	Use of Address List	o	o			

A.5.3 Supported information objects

Item	Element	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
1	Military Message (MM)	m	m			
1.1	heading	m	m			see A.5.3.1
1.2	body	m	m			see A.5.3.2
2	Military Notification (MN)	m	c			p37, Note 1, see A.5.3.3

Note:

1 If the conditions for which a Non-receipt Notification would be generated are not supported, the ability to generate a Non-Receipt Notification is optional.

A.5.3.1 MM heading fields

Item	Element	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
1	this-IPM	m	m			see A.5.3.4(3)
2	originator	m	m			see A.5.3.4(2)
3	authorizing-users	c	m			p6, see A.5.3.4(2)
4	primary-recipients	m	m			see A.5.3.4(1)
5	copy-recipients	m	m			see A.5.3.4(1)
6	blind-copy-recipients	c	m			p8, see A.5.3.4(1)
7	replied-to-IPM	m	m			p34, see A.5.3.4(3)
8	obsoleted-IPMs	c	m			p25, see A.5.3.4(3)

Item	Element	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
9	related-IPMs	c	m			p11, see A.5.3.4(3)
10	subject	m	m			
11	expiry-time	c	m			p14
12	reply-time	c	m			p33
13	reply-recipients	c	m			p33, see A.5.3.4(2)
14	importance	c	m			p18
15	sensitivity	c	m			p35
16	auto-forwarded	c	m			p7, Note 1
17	extensions	c	m			p41
17.1	incomplete-copy	c	c			p19
17.2	languages	c	m			p20
17.3	primary-precedence	c	c			p2, see A.5.3.4(4)
17.4	copy-precedence	c	c			p1, see A.5.3.4(4)
17.5	message-type	c	c			p22
17.5.1	type	m	m			
17.5.2	identifier	o	m			
17.6	address-list-indicator	c	c			p36, see A.5.3.4(2)
17.6.1	type	o	m			
17.6.2	list-name	o	m			
17.6.3	notification-request	o	m			
17.6.4	reply-request	o	m			
17.7	exempted-address	c	c			p13, see A.5.3.4(2)
17.8	extended-authorisation-info	c	c			p15
17.9	distribution-codes	c	c			p12
17.9.1	sics	m	m			
17.9.2	dist-extensions	o	m			
17.10	message-instructions	c	c			p21
17.11	codress-message	o	c			p9
17.12	originator-reference	c	c			p27
17.13	other-recipient-indicator	c	c			p29
17.13.1	type	m	m			
17.13.2	designator	m	m			
17.14	handling-instructions	o	c			p17
17.15	pilot-forwarding-info	o	c			p30
17.15.1	pilot-precedence	o	m			see A.5.3.4(4)
17.15.2	pilot-recipient	o	m			
17.15.3	pilot-security	o	m			
17.15.4	pilot-handling	o	m			
17.16	acp127-message-identifier	o	c			p3
17.17	originator-plad	o	c			p28

Item	Element	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
17.18	security-information-labels	o	o			

Note:

1 Support for Auto-forwarding is dependent on national or local policy and may be influenced by security procedures.

A.5.3.2 MM body

Item	Element	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
1	ia5-text	o	o			see ISO/IEC 10021-7
1.1	parameters	m	m			
1.1.1	repertoire	o	m			
1.2	data	m	m			
2	voice	o	o			see ISO/IEC 10021-7
2.1	parameters	m	m			
2.2	data	m	m			
3	g3-facsimile	o	o			see ISO/IEC 10021-7
3.1	parameters	m	m			
3.1.1	number-of-pages	o	o			
3.1.2	non-basic-parameters	o	o			
3.1.2.1	two-dimensional	o	o			
3.1.2.2	fine-resolution	o	o			
3.1.2.3	unlimited-length	o	o			
3.1.2.4	b4-length	o	o			
3.1.2.5	a3-width	o	o			
3.1.2.6	b4-width	o	o			
3.1.2.7	uncompressed	o	o			
3.2	data	m	m			
4	g4-class-1	o	o			see ISO/IEC 10021-7
5	teletex	o	o			see ISO/IEC 10021-7
5.1	parameters	m	m			
5.1.1	number-of-pages	o	o			
5.1.2	telex-compatible	o	m			
5.1.3	non-basic-parameters	o	o			
5.2	data	m	m			

Item	Element	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
6	videotex	o	o			see ISO/IEC 10021-7
6.1	parameters	m	m			
6.1.1	syntax	o	o			
6.2	data	m	m			
7	encrypted	o	o			see ISO/IEC 10021-7
7.1	parameters	m	m			
7.2	data	m	m			
8	message	o	o			see ISO/IEC 10021-7
8.1	parameters	m	m			
8.1.1	delivery-time	o	o			
8.1.2	delivery-envelope	o	o			
8.2	data	m	m			
8.2.1	IPM	m	m			
9	mixed-mode	o	o			see ISO/IEC 10021-7
10	bilaterally-defined	o	o			see ISO/IEC 10021-7
11	nationally-defined	o	o			see ISO/IEC 10021-7
12	externally-defined	o	o			see A.5.3.2.1

A.5.3.2.1 Extended body part support

Item	Element	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
1	ia5-text-body-part	o	o			see A.5.3.2(1)
2	g3-facsimilie-body-part	o	o			see A.5.3.2(3)
3	g4-class1-body-part	o	o			see A.5.3.2(4)
4	telextex-body-part	o	o			see A.5.3.2(5)
5	videotex-body-part	o	o			see A.5.3.2(6)
6	encrypted-body-part	o	o			
6.1	parameters	o	m			
6.2	data	m	m			
7	message-body-part	c	c			p16, see A.5.3.2(5)
8	mixed-mode-body-part	o	o			
9	bilaterally-defined-body-part	o	o			
10	nationally-defined-body-part	o	o			
11	general-text	o	o			
12	file-transfer-body-part	o	o			see A.5.3.2.2

Item	Element	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
13	voice-body-part	o	o			
13.1	parameters	o	m			
13.2	data	m	m			
14	oda-body-part	o	o			see ISO/IEC 8613-1
15	adatp3-body-part	o	o			
15.1	parameters	o	m			
15.2	data	m	m			
16	corrections-body-part	o	c			p10
16.1	parameters	o	m			
16.2	data	o	m			
17	forwarded-encrypted-body-part	o	o			
17.1	parameters	o	m			
17.1.1	delivery-time	o	m			
17.1.2	delivery-envelope	m	m			
17.2	data	m	m			
18	mm-message-body-part	c	c			p16
18.1	parameters	o	m			
18.1.1	delivery-time	o	m			
18.1.2	delivery-envelope	m	m			
18.2	data	m	m			see A.5.3(1)
19	acp127data-body-part	o	o			
19.1	parameters	o	m			
19.2	data	o	m			
20	forwarded-CSP-Message-Body-Part	o	o			
21	report-body-part	i	i			
22	notification-body-part	i	i			
23	content-body-part	m	m			

A.5.3.2.2 General text repertoire support

Item	Repertoire set description	Repetoire identifier(s)	Profile		Support		Comments
			Orig.	Rec.	Orig.	Rec.	
1	Basic (ISO 646)	{1,6}	o	o			
2	Basic-1 (ISO 8859-1)	{1,6,100}	o	o			
3	Basic + Chinese (1)	{1,6,58}	o	o			
4	Basic + Chinese (2)	{1,6,165}	o	o			
5	Basic + Japanese (1)	{1,6,13,87}	o	o			
6	Basic + Japanese (2)	{1,6,13,168}	o	o			
7	Basic + Korean	{1,6,149}	o	o			

Item	Repertoire set description	Repetoire identifier(s)	Profile		Support		Comments
			Orig.	Rec.	Orig.	Rec.	
8	Basic-1 + Cyrillic (ISO 8859-5)	{1,6,100,144}	o	o			
9	Basic-1 + Arabic (ISO 8859-6)	{1,6,100,127}	o	o			
10	Basic-1 + Greek (ISO 8859-7)	{1,6,100,126}	o	o			
11	Basic-1 + Hebrew (ISO 8859-8)	{1,6,100,138}	o	o			
12	Full Latin (1)	{1,6,100,154}	o	o			
13	Full Latin (2) (ISO 6937	{1,6,156}	o	o			
14	Teletex Basic Latin (T.61)	{102,103,106, 107}	o	o			

A.5.3.3 MN fields

Item	Element	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
1	subject-IPM	m	m			
2	ipn-originator	c	m			p26
3	IPM-preferred-recipient	m	m			
4	conversion-eits	o	m			
5	notification-extensions	o	o			
6	non-receipt-fields	c	c			p38
6.1	non-receipt-reason	m	m			
6.2	discard-reason	m	m			
6.3	auto-forward-comment	c	m			p39
6.4	returned-IPM	o	o			
6.5	nrn-extensions	o	o			
7	receipt-fields	o	o			
7.1	receipt-time	m	m			
7.2	acknowledgment-mode	o	m			
7.2.1	manual	m	m			
7.2.2	automatic	o	m			
7.3	suppl-receipt-info	o	o			
7.4	rn-extensions	o	o			
8	other-notification-type-fields	o	c			p5
8.1	acp127-notification-response	o	c			p5
8.1.1	acp127-notification-type	o	m			
8.1.2	receipt-time	o	m			

Item	Element	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
8.1.3	addressListInicator	o	m			
8.1.4	acp127-recipient	o	m			
8.1.5	acp127-supp-info	o	m			

A.5.3.4 Common data types

Item	Element	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
1	RecipientSpecifier					
1.1	recipient	m	m			see A.5.3.4(2)
1.2	notification-requests	c	m			p32, p34
1.2.1	rn	c	m			p32
1.2.2	nrn	c	m			p24
1.2.3	IPM-return	o	o			
1.3	reply-requested	c	m			p33
1.4	recipient-extensions	c	o			p4
1.4.1	acp127-notification-request	c	o			p4
2	ORDescriptor					
2.1	formal-name	m	m			see A.5.3.4(5)
2.2	free-form-name	c	c			p26
2.3	telephone-number	o	o			
3	MMIdentifier					
3.1	user	m	m			see A.5.3.4(5)
3.2	user-relative-identifier	m	m			
4	MMHSPrecedence					
4.1	deferred (0)	o	m			
4.2	routine (1)	m	m			
4.3	priority (2)	m	m			
4.4	immediate (3)	m	m			
4.5	flash (4)	m	m			
4.6	override (5)	o	m			
4.7	nato-reserved (6-15)	i	i			
4.8	nationally defined (16-30)	i	i			
5	ORName					
5.1	mnemonic O/R address	m	m			
5.2	numeric O/R address	m	m			
5.3	terminal O/R address	o	o			

Item	Element	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
5.4	formatted postal O/R address	o	o			
5.5	unformatted postal O/R address	o	o			
5.6	directory-name	m	m			

A.6 Message Store Attributes

This section classifies MM-specific MS attributes and applies to both the UA an MS.

Item	Attribute	Base	Support	Notes
1	acknowledgment-mode	o		
2	authorizing-users	o		
3	auto-forward-comment	o		
4	auto-forwarded	o		
5	bilaterally-defined-body-parts	o		
6	blind-copy-recipients	o		
7	body	m		
8	conversion-eits	o		
9	copy-recipients	o		
10	discard-reason	o		
11	encrypted-body-parts	o		
12	encrypted-data	o		
13	encrypted-parameters	o		
14	expiry-time	o		
15	extended-body-part-types	o		
16	g3-facsimile-body-parts	o		
17	g3-facsimile-data	o		
18	g3-facsimile-parameters	o		
19	g4-class1-body-parts	o		
20	heading	m		
21	ia5-text-body-parts	o		
22	ia5-text-data	o		
23	ia5-text-parameters	o		
24	importance	o		
25	incomplete-copy	o		
26	ipm-entry-type	m		
27	ipm-preferred-recipient	o		
28	ipm-synopsis	o		
29	ipn-originator	o		
30	languages	o		
31	message-body-parts	o		
32	message-data	o		
33	message-parameters	o		

34	mixed-mode-body-parts	o		
35	nationally-defined-body-parts	o		
36	non-receipt-reason	o		
37	nrn-requestors	o		
38	obsoleted-ipms	o		
39	originator	o		
40	primary-recipients	o		
41	receipt-time	o		
42	related-ipms	o		
43	replied-to-ipm	o		
44	reply-recipients	o		
45	reply-requestors	o		
46	reply-time	o		
47	returned-ipm	o		
48	rn-requestors	o		
49	sensitivity	o		
50	subject	o		
51	subject-ipm	m		
52	supp-receipt-info	o		
53	teletex-body-parts	o		
54	teletex-data	o		
55	teletex-parameters	o		
56	this-ipm	m		
57	videotex-body-parts	o		
58	videotex-data	o		
59	videotex-parameters	o		
60	voice-body-parts	o		
61	voice-data	o		
62	voice-parameters	o		
63	acp127-message-identifier	o		
64	address-list-indicator	o		
65	codress-message	o		
66	copy-precedence	o		
67	distribution-codes	o		
68	exempted-address	o		
69	extended-authorisation-info	o		
70	handling-instructions	o		
71	message-instructions	o		
72	message-type	o		
73	originator-reference	o		
74	originator-plad	o		
75	other-recipients-indicator	o		
76	pilot-forwarding-info	o		
77	primary-precedence	o		
78	acp127-notification-request	o		
79	acp127-receipt-response	o		

A.7 AutoForwardRegistrationParameter

Item	Element	Base		Support		Notes
		Orig.	Rec.	Orig.	Rec.	
4	other-parameters	c	c			p40
4.1	auto-forwarding-comment	o	o			
4.2	cover-note	o	o			
4.3	this-ipm-prefix	o	o			

A.8 Other information

A.8.1 Elements of Service support

The following tables shall be completed to indicate (Y or √), for each MM, MT, MH/PD, and MS Element of Service, whether the EoS is made available to the MHS user and, if so, how this is achieved. For each EoS for which support is claimed, the implementor will check the column which indicates how the EoS is supported in a given instance. Where support for origination and reception cannot be covered by a single indication, then both shall be indicated. If appropriate the Comments column can be filled in to provide additional information as to how the EoS is selected.

The columns have the following meanings:

Service — the EoS can be dynamically selected by the MHS user (i.e., for invocation and/or notification, as appropriate) without requiring reconfiguration of the UA or other intervention in each instance (whether the semantics of the EoS are available at a human user interface, programmatic interface or by other means may be specified in the Comments column)

Auto — the EoS is automatically invoked/actioned by the UA without reference to the MHS user (whether selection is dynamically determined based on some other knowledge or criteria may be specified in the Comments column)

Config — the UA may be configured to select the EoS by the execution of some off-line process

Other — any other means of using the EoS

A.8.1.1 MM Elements of Service support

Ref	Element of Service	Service	Auto	Config	Comments/Other
1	ACP 127 Message Identifier				
2	ACP 127 Notification				

Ref	Element of Service	Service	Auto	Config	Comments/Other
	Request				
3	ACP 127 Notification Response				
4	Authorizing Users Indication				
5	Auto-forwarded Indication				
6	Blind Copy Recipient Indication				
7	Body Part Encryption Indication				
8	Clear Service				
9	Codress Message indicator				
10	Copy Precedence				
11	Corrections				
12	Cross-referencing Indication				
13	Distribution Code				
14	Exempted Addresses				
15	Expiry Date Indication				
16	Extended Authorization info				
17	Forwarded Message Indication				
18	Handling Instructions				
19	Importance Indication				
20	Incomplete Copy Indication				
21	Language Indication				
22	Message Instructions				
23	Message Type				
24	IPM-message Identification				
25	Multi-part Body				
26	Non-receipt Notification Request Indication				
27	Obsoleting Indication				
28	Originator Indication				
29	Originator Reference				
30	Originator PLAD				
31	Other Recipient Indicator				
32	Pilot Forwarded				
33	Primary and Copy Recipients Indication				
34	Primary Precedence				
35	Receipt Notification Request Indication				
36	Reply Request Indication				
37	Replying Message Indication				
38	Security Information Labels				
39	Sensitivity Indication				

Ref	Element of Service	Service	Auto	Config	Comments/Other
40	Subject Indication				
41	Typed Body				
42	Use of Address List				

A.8.1.2 MT Elements of Service support

Ref	Element of Service	Service	Auto	Config	Comments/Other
1	Access Management				
2	Alternate Recipient Allowed				
3	Alternate Recipient Assignment				
4	Content Confidentiality				
5	Content Integrity				
6	Content Type Indication				
7	Conversion Prohibition				
8	Conversion Prohibition in Case of Loss of Information				
9	Converted Indication				
10	Deferred Delivery				
11	Deferred Delivery Cancellation				
12	Delivery Notification				
13	Delivery Time Stamp Indication				
14	Designation of Recipient by Directory Name				
15	Disclosure of Other Recipients				
16	DL Expansion History Indication				
17	DL Expansion Prohibited				
18	Explicit Conversion				
19	Grade of Delivery Selection				
20	Hold for Delivery				
21	Implicit Conversion				
22	Latest Delivery Designation				
23	Message Flow Confidentiality				
24	Message Identification				
25	Message Origin Authentication				
26	Message Security Labelling				
27	Message Sequence Integrity				
28	Multi-Destination Delivery				
29	Non-delivery Notification				
30	Non-repudiation of Delivery				

Ref	Element of Service	Service	Auto	Config	Comments/Other
31	Non-repudiation of Origin				
32	Non-repudiation of Submission				
33	Original Encoded Information Types Indication				
34	Originator Requested Alternate Recipient				
35	Prevention of Non-delivery Notification				
36	Probe				
37	Probe Origin Authentication				
38	Proof of Delivery				
39	Proof of Submission				
40	Redirection Disallowed by Originator				
41	Redirection of Incoming Messages				
42	Report Origin Authentication				
43	Requested Preferred Delivery Method				
44	Restricted Delivery				
45	Return of Content				
46	Secure Access Management				
47	Submission Time Stamp Indication				
48	Use of Distribution List				
49	User/UA Capabilities Registration				

A.8.1.3 MH/PD Elements of Service support

Ref	Element of Service	Service	Auto	Config	Comments/Other
1	Additional Physical Rendition				
2	Basic Physical Rendition				
3	Counter Collection				
4	Counter Collection with Advice				
5	Delivery via Bureaufax Service				
6	EMS (Express Mail Service)				
7	Ordinary Mail				
8	Physical Delivery Notification by MHS				

Ref	Element of Service	Service	Auto	Config	Comments/Other
9	Physical Delivery Notification by PDS				
10	Physical Forwarding Allowed				
11	Physical Forwarding Prohibited				
12	Registered Mail				
13	Registered Mail to Addresses in Person				
14	Request for Forwarding Address				
15	Special Delivery				
16	Undeliverable Mail with Return of Physical Message				

A.8.1.4 MS Elements of Service support

Ref	Element of Service	Service	Auto	Config	Comments/Other
1	MS Register				
2	Stored Message Alert				
3	Stored Message Auto-forward				
4	Stored Message Deletion				
5	Stored Message Fetching				
6	Stored Message Listing				
7	Stored Message Summary				

A.8.2 Encoded information type conversion requests supported

The following table shall be completed if support of the MM Conversion FG is claimed, to indicate (Y or √) which encoded information type conversions the implementation can request (see clause 7.1 of AMH2n(D) Part 1).

Item	Encoded Information Type Conversion	Supported (Y/N)	Comments
1.1	ia5-text-to-teletex (0)		
1.2	ia5-text-to-g3-facsimile (8)		
1.3	ia5-text-to-g4-class-1 (9)		
1.4	ia5-text-to-videotex (10)		
1.5	teletex-to-ia5-text (11)		
1.6	teletex-to-g3-facsimile (12)		
1.7	teletex-to-g4-class-1 (13)		
1.8	teletex-to-videotex (14)		
1.9	videotex-to-ia5-text (16)		

Item	Encoded Information Type Conversion	Supported (Y/N)	Comments
1.10	videotex-to-teletex (17)		

A.8.3 Non-standard integer body part types supported

The following table shall be completed to indicate (Y or √) which (if any) non-standard integer body part types the implementation is capable of originating and/or receiving.

Item	Body Part Type	Orig.	Rec.	Comments
1	ODA (12)			
2	ISO6937Text (13)			
3	USA nationally-defined body part types (310)			
4	JIS-1 (440)			
5	other (specify)			

A.8.4 Extended body part types supported

The following table shall be completed to indicate (Y or √) which (if any) specific extended body part types the implementation is capable of originating and/or receiving (in addition to those specified in A.5.3.2.1), and the object identifier value(s) supported in each case.

Item	Body Part Type	Orig.	Rec.	Comments
1				
2				
3				
4				
5				

It should be indicated below whether the implementation can be configured to allow other externally-defined body part types to be used, and how this is achieved.

A.8.5 General text body part repertoire support

The following table shall be completed to indicate (Y or √) which specific character repertoires the implementation is capable of originating and/or receiving for support

of the general-text body part type. It shall be stated in the Comments column how such capability is implemented.

NOTE – The table identifies some useful repertoire sets as proposed by the three regional workshops, but this should not be seen as a comprehensive list. Repertoire set {1,6} is considered to be the minimum support level. It is expected that the European and North American regional profiles will also require support of repertoire set {1,6,100}.

Item	Repertoire set description	Repertoire identifier(s)	Orig.	Rec.	Comments
1					
2					
3					
4					
5					
6					

Appendix B

(normative)

Technical corrigenda

International Standards are subject to constant review and revision by the ISO/IEC Technical Committees concerned. The following amendments and corrigenda are approved by ISO/IEC JTC1 and are considered as normative references in this part of ACP 123.

NOTE - Corresponding corrigenda to the equivalent CCITT Recommendations are contained in the joint CCITT/ISO MHS Implementor's Guide Version 11.

ISO/IEC 10021-1/Cor.1:1991

ISO/IEC 10021-1/Cor.2:1991

ISO/IEC 10021-1/Cor.3:1992

ISO/IEC 10021-1/Cor.4:1992

ISO/IEC 10021-1/Cor.5:1992

ISO/IEC 10021-1/Cor.6:1994

ISO/IEC 10021-1/Cor.7:1994

ISO/IEC 10021-2/Cor.1:1991

ISO/IEC 10021-2/Cor.2:1991

ISO/IEC 10021-2/Cor.3:1992

ISO/IEC 10021-2/Cor.4:1992

ISO/IEC 10021-2/Cor.5:1993

ISO/IEC 10021-2/Cor.6:1994

ISO/IEC 10021-2/Cor.7:1994

ISO/IEC 10021-7/Cor.1:1991

ISO/IEC 10021-7/Cor.2:1991

ISO/IEC 10021-7/Cor.3:1992

ISO/IEC 10021-7/Cor.4:1992

ISO/IEC 10021-7/Cor.5:1992

ISO/IEC 10021-7/Cor.6:1993

ISO/IEC 10021-7/Cor.7:1994

ISO/IEC 10021-7/Cor.8:1994

ISO/IEC 10021-7/Cor.9:1994

ANNEX I

REFERENCE DOCUMENTS

STANAG 4406: Military Message Handling System, Edition 2, October 2006

The International Telegraph and Telephone Consultative Committee (CCITT)[1], September 1992, Data Communication Networks Message Handling Systems Recommendations X.400-X.420

The International Telegraph and Telephone Consultative Committee (CCITT)[1], February 1993, Data Communication Networks Directory Recommendations X.500-X.525

ITU Special Rapporteur's Group on Message Handling Systems (Q14/VII) and ISO/IEC JTC 1/SC 18/WG 4 SWG on Messaging, July 1994, MHS Implementors' Guide Version 11

ISO/IEC 8613-1: 1993, Information technology – Open Document Architecture (ODA) and Interchange Format – Part 1: Introduction and general principles

ISO/IEC 8824: 1990, Information processing systems – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1)

ISO/IEC 8859: 1992, Information technology – 8-bit single-byte coded graphic character sets

ISO/IEC 9646-1: 1991, Information technology – Open Systems Interconnection – Conformance Testing Methodology and Framework Part 1: General concepts

ISO/IEC 9646-7: 1992 Information Technology – Open Systems Interconnection – Conformance Testing Methodology and Framework Part 7: Implementation Conformance Statements

ISO/IEC 10021 parts 1-7 Information technology – Text Communication – Message-Oriented Text Interchange Systems (MOTIS)

ISO/IEC ISP 10611 parts 1-5 International Standardized Profiles AMH1n – Message Handling Systems – Common Messaging

[1] Note that CCITT is now known as the International Telecommunications Union – Telecommunications Standardization Sector (ITU-T).

ACP 198( ) Instructions for the Preparation of Communications-Electronics Publications

ACP 120( ) Common Security Protocol

ACP 121( ) Communication Instructions General

ACP 126( ) Communication Instructions – Teletypewriter (Teleprinter) Procedures

ACP 127( ) Communication Instructions – Tape Relay Procedures

ACP 128( ) Allied Telecommunications Record System (ALTERS) Operating Procedures

ACP 131( ) Communication Instructions – Operating Signals

ACP 133( ) Common Directory Service and Procedures

Interim Implementation Guide For ACP 123/STANAG 4406 Messaging Services Between Nations, ACP 145, Edition A, September 2008.

LIST OF EFFECTIVE PAGES

Subject Matter	Page Numbers	
Title Page	i	
Foreword	ii	
Letter of Promulgation	iii	
Record of Message Corrections	iv	
Table of Contents	v to ix	
Chapter 1	1-1 to 1-15	
Chapter 2	2-1 to 2-37	
Chapter 3	3-1 to 3-7	
Chapter 4	4-1 to 4-28	
Chapter 5	5-1 to 5-6	
Annex A	A-1 to A-88	
Annex B	B-1 to B-11	
Annex C	C-1 to C-67	
Annex D	D-1 to D-23	
Annex E	E-1 to E-118	
Annex F	F-1 to F-8	
Annex G	G-1 to G-10	
Annex H	H-1 to H-30	
Annex I	I-1 to I-2	
List of Effective Pages	LEP-1	