Netherlands organization for applied scientific research

FEL

TNO Physics and Electronics Laboratory

89-3866

DTIC COPY

report no. FEL-89-B260

copy no. 18

Message handling in a military environment

AD-A217 929

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

DTIC
ELECTE
FEB 12 1990
S D
E

90 02 09 096

Netherlands
organization for
applied scientific
research

TNO-report

TNO Physics and Electronics
Laboratory

P.O. Box 96864
2509 JG The Hague
Oude Waalsdorperweg 63
The Hague, The Netherlands

Phone +31 70 26 42 21

report no. FEL-89-B260

copy no. 18

title

Message handling in a military environment

author(s):

Ir. W.A. Levenbach

classification

title	: unclassified
abstract	: unclassified
report	: unclassified

no. of copies	: 33
no. of pages	: 44
appendices	: 2

date : September 18, 1989

report no.	:	FEL-89-B260
title	:	Message handling in a military environment
author(s)	:	Ir. W.A. Levenbach
institute	:	TNO Physics and Electronics Laboratory
date	:	September 18, 1989
NDRO no.	:	-
no. in pow '89	:	704.1

ABSTRACT

This report deals with the use of Message Handling Systems (MHS) in a military C^3I environment. The main elements of MHS, as they are defined in the X.400 series of recommendations of CCITT/ISO, are briefly discussed.

A slight difference between the military and a commercial environment causes special requirements for military message handling. These military demands are discussed along with the now used standard for military message handling (ACP 127) in telex based systems.

The most recent version of X.400/MOTIS (1988), defining the standard for commercial MHSs, seems also to define a good standard for use in a military environment (with some extensions and modifications). The use of commercial available X.400/MOTIS systems is therefore a good choice for creation, submission and delivery of messages in a military environment.

rapport no. : FEL-89-B260
titel : Message handling in a military environment

auteur(s) : Ir. W.A. Levenbach
instituut : Fysisch en Elektronisch Laboratorium TNO

datum : 18 september 1989
hdo-opdr.no. : -
no. in iwp '89 : 704.1

==========

SAMENVATTING

Dit rapport behandelt de mogelijkheden van Message Handling Systems (MHS) in een militaire C3I omgeving. Kort worden de belangrijkste elementen van het MHS beschreven, zoals deze gedefinieerd zijn in de X.400/MOTIS standaarden van CCITT/ISO.
Een militaire omgeving wijkt enigszins af van een civiele omgeving, en stelt een aantal specifieke eisen aan het berichtenverkeer. Aan de hand van de nu gebruikte standaard in het militaire telex-berichtenverkeer (ACP 127) worden deze eigenschappen nader belicht. De meest recente versie van X.400/MOTIS (1988) blijkt met enige uitbreidingen en modificaties goede mogelijkheden te bieden om ook in een militaire omgeving als standaard te worden aangehouden. Het lijkt daarom een logische keus te streven naar de inzet van commercieel verkrijgbare X.400/MOTIS systemen voor het opstellen, verzenden en ontvangen van berichten binnen een militaire omgeving.

1 INTRODUCTION

With the increasing number of C3I (Command, Control, Communication and Intelligence) systems in military environments within both NATO and nations of NATO a need for reliable standardized communication systems has shown up. An interface must be developed that assists in the exchange of information between the different C3I architectures in national and NATO command centres, and that guarantees interoperability between them. Exchange of information will be message oriented and will be both top-down (e.g. tasking orders) and bottom-up (e.g. status reports).

The basis of this document is formed by the existing commercial standards for message handling (X.400). Unique military requirements will be discussed along with military message formats (ACP 127, ADatP-3) and will be based on the military specifications for 'Standard Automated Message Interface for NATO Allied command and control information systems' (STAMINA). Military requirements should be supported as specified extensions on the commercial standards (super-set concept).

The aim of Message Handling System (MHS) standards is to provide an international service for the exchange of electronic messages. Two organizations are involved in the production of standards for MHS: CCITT (Consultative Committee for International Telephone and Telegraph) and ISO (International Standards Organization). In 1984 CCITT published a standard set of recommendations on electronic message handling, known as X.400 (1984). Since then CCITT and ISO have been working together on new parallel standards with identical text respectively known as X.400 and MOTIS (Message Oriented Text Interchange System).
X.400 specifies the overall system and service description of Message Handling Systems (MHS) and is one of a set of recommendations (X.400, X.401, etc.). The corresponding ISO recommendations are numbered ISO 10021-1, ISO 10021-2, etc.

This report describes the use of a store and forward computer-based message handling system for the exchange of electronic messages between computer systems of different sizes and from different vendors. Only the application profiles (upper layers of OSI) will

be discussed here. End-user services and local functions and protocols will not be discussed.

The document contains 7 chapters, the first chapter being this introduction. The next four chapters will successively give a description of the abstract models of the MHS, the naming and addressing conventions, the elements of service that are specified in X.400 recommendations for message handling and the military enhancements, needed for use in a military environment.

Chapter 6 describes the possible architecture of a message handling system in a military C^3I environment. New systems like LOTEX/BERDIS and ABCCIS/INTAL, that are planned to be built for the Royal Netherlands Army (RNLA) and Royal Netherlands Airforce (RNLAF), are discussed briefly, and an X.400 based message handling configuration is pointed out for these systems. In the last chapter (7) the conclusions are presented.

Appendix A contains descriptions and definitions of all elements of service, as they are defined in the CCITT standards of 1988.
Appendix B contains a list of those elements of service that are new in the standards of 1988.

2 ABSTRACT MODELS OF MHS

2.1 Introduction

Message Handling Systems and Services enable users to exchange messages on a store and forward basis. A message submitted by one user, the originator, can be transmitted to one or more other users, the message's recipients. The originator uses its User Agent (UA) to compose the message, and to submit it to the Message Transfer System (MTS), consisting of a number of Message Transfer Agents (MTA). The MTS takes care of conveyance of the message, sending the message from one MTA to another and finally it delivers the message to the recipient's UA.

The basic structure of a message is shown in figure 2.1. A message is made up of an envelope and a content. The envelope carries information that is used by the MTA for conveyance of the message (names, addresses, etc.). The content is the piece of information the originator wishes to be delivered to the recipient.

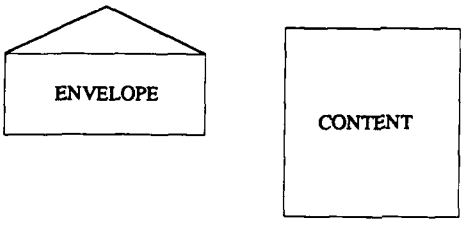

Fig. 2.1: Basic Message Structure.

2.2 FUNCTIONAL MODEL OF MHS

The message handling system, as described in the 1988 specifications of the X.400 [1] standard, consists of four different functional entities:

- Message Transfer Agent (MTA),
- User Agent (UA),
- Message Store (MS),
- Access Unit (AU).

These four entitities are responsible for conveyance, creation and storage of messages and for access to other delivery systems respectively. Figure 2.2 illustrates the entities and their relation. In the following paragraphs the functional entities are described in more detail.

2.2.1 MESSAGE TRANSFER AGENT

Starting at the originator's MTA, each MTA transfers the message to another MTA until the message reaches the recipient's MTA, which then delivers it to the recipient UA or MS using the delivery interaction. The transfer envelope contains information that the MTA requires for conveyance of the message.

2.2.2 USER AGENT

A UA is a functional entity by means of which a single (direct) user engages in message handling, it is the intermedium between the user and the MTS. The UA takes care of construction and manipulation of messages (editors, spelling checkers, document formatters, etc.). UAs are grouped into classes, based on the type of content of messages they can handle. The MTS provides a UA with the ability to identify its class when sending messages to other UAs. UAs within a given class are referred to as cooperating UAs, since they cooperate with each other to enhance the communication amongst their respective users. A UA can support more than one type of message content, and hence belong to several UA classes.

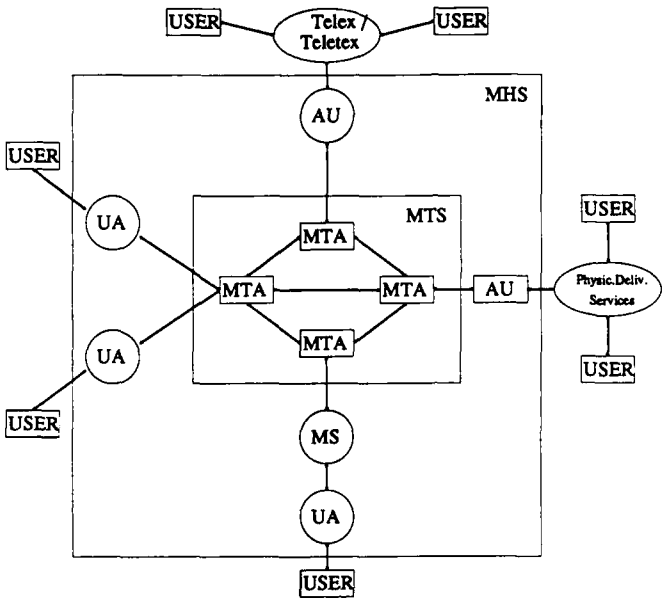

Fig. 2.2: Message Handling System (MHS).

2.2.3 MESSAGE STORE

The message store is a new functional entity in the standards of 1988, and provides facilities for taking delivery of messages from the MTS, storing the messages reliably and allowing the UA to have control over retrieval of the messages. MS works like a mailbox and makes delivery of messages no longer dependent on whether or not the associated UA is active. The introduction of personal computers (PCs) as stand-alone UAs has caused the need for this new entity. Too often messages were declared to be undeliverable when the PC was shut down temporarily. Now the message can be delivered to the MS, which can be located near an MTA in the host computer. A second

reason for the need of this new entity were the problems on PCs in storing capabilities, not only the quantity of storage but also the possibility to make regular backups and to access the messages from a location remote from the office (also when the PC is shut down) affirm this need.

In addition to the normal submission facilities the MS also enables the user agent to indicate that some parts of a submitted message are to be taken from the message store directly and inserted into another message being submitted. A UA submits a message through the MS. Sending the invitations for a meeting, for example, the secretary will be able to indicate that the MS adds the agenda to it, as it is received from the chairman and stored in the MS.
The MS will be able to maintain logs of submitted messages.

2.2.4 ACCESS UNIT

The other functional entity that is new in the standards of 1988 is the access unit (AU). It provides a gateway between MHS and an external communications service. Three types of AU have been defined, providing access to physical delivery systems (PDAU), teletex and telex respectively. An example of a physical delivery system is the postal system. An electronic message may be sent to a printing device, here the content is printed on a paper letter and the electronic envelope is replaced by a paper envelope. The postal system will now take care of delivery. Access units for teletex and telex enable users of teletex and telex terminals to participate fully in the InterPersonal Message (IPM) Service.

2.3 INFORMATION MODEL OF MHS

Messages are not the only information objects that can be conveyed by the MHS and MTS. Two other classes are specified: *probes* and *reports*.

2.3.1 MESSAGES

A message is used to exchange information between two or more users, and consists as shown in paragraph 2.1 of two parts: envelope and content. The MTS is solely interested in the information that the envelope contains and neither modifies nor examines the

content, except for conversion (e.g. conversion from facsimile to IA5 (International Alphabet) text or to telex, etc.).

As outlined in paragraph 2.2.2 user agents are grouped into classes of cooperating UAs, according to the common ability to handle messages of a particular content type. So far the only content type that has been standardized is the interpersonal message (IPM), known as P2 content-type. P2 determines the syntax and semantics of a message content for exchange between end-to-end IPM UAs.

The content of an interpersonal message consists of a header and one or more bodyparts. The header contains information needed by the UA to handle the associated body, information about the addressee, sender, subject, etc. The body-parts contain the main piece of information the originator wishes to convey to its recipient(s). Each body-part may contain a different type of encoded information, like IA5 text, facsimile, graphics, voice or even an entire IP message (forwarded IPM). In figure 2.3 an example of an IPM is illustrated.

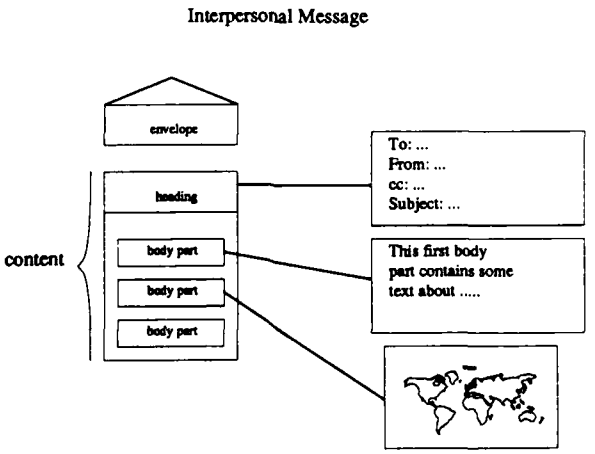

Fig. 2.3: Interpersonal Message (IPM).

2.3.2 PROBES

A probe describes a message, and is used to determine the deliverability of a message. A probe comprises an envelope alone, which contains much the same information as the envelop of a message. Instead of the content the probe's envelope will contain an information type describing the length of the content. A user or computer process that doubts whether a (classified) message can be delivered successfully via the MTS, will first send a probe to the intended recipient. Upon receipt of a delivery notification the real message can be submitted.

2.3.3 REPORTS

Reports are generated by the MTS and contain information about delivery of a message or probe. Reports are divided into:

- delivery reports: delivery, export, or affirmation of the subject message or probe.
- non-delivery reports: non-delivery or non affirmation of the subject message or probe.

2.4 ORGANIZATIONAL CONFIGURATION

The MHS consists of a number of organizational blocks, called management domains. A management domain (MD) is a set of messaging systems (at least one of which contains, or realizes, an MTA) that is managed by a single organization (figure 2.4). Two different types of management domains exist:

- Administration management domain (ADMD),
- Private management domain (PRMD).

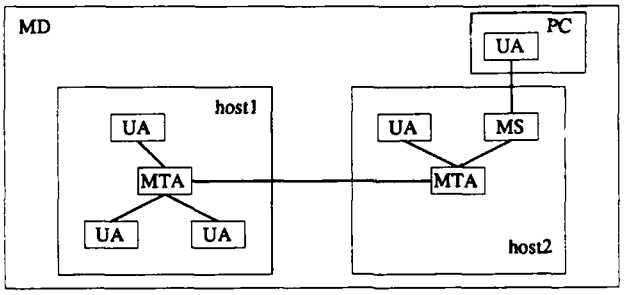

Fig. 2.4: Management domain.

ADMDs are managed by an administration (i.e. a PTT, or national telecommunications company), PRMDs are not (i.e. they are managed by a private organization). The major technical destinction between ADMDs and PRMDs is that ADMDs are positioned above PRMDs in the MHS hierarchical addressing and routing. The possible configurations of ADMDs and PRMDs for intra- and inter-organizational message handling are slightly different in the standards of CCITT and ISO. In general ADMDs serve as an intermediary between PRMDs and other ADMDs (figure 2.5).

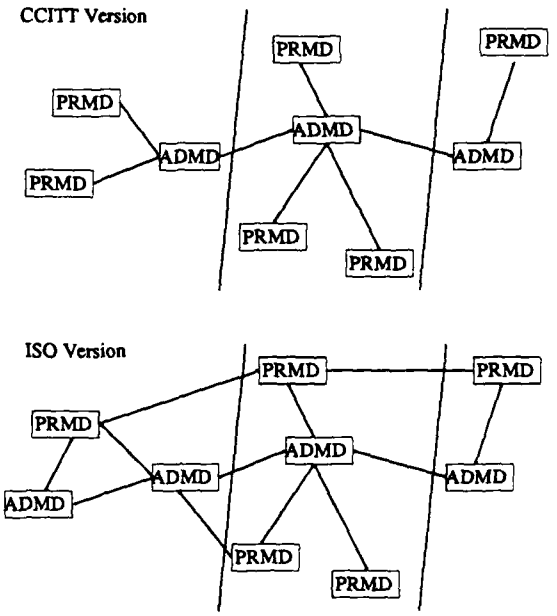

Fig. 2.5: Management Domains (MD).
PRMD = Private Management Domain.
ADMD = Administrative Management Domain.

ISO permits a direct connection of PRMDs, CCITT doesn't.
In the CCITT version ADMDs will always serve as an intermediary between PRMDs. In a military environment ADMDs may probably not be available. If all MTAs and UAs of one military site build up one PRMD, a direct connection to the PRMD of another military site will be desirable, without intervention of high level routing by a PTT (ADMD). If no direct connection between PRMDs is permitted, an alternative solution would be that all airbases together constitute one PRMD.

3 NAMING AND ADDRESSING

3.1 NAMING

Recipients may be addressed individually or by use of a distribution list. A distribution list (DL) is list of recipients. The way of addressing will be exactly the same for individual recipients and for distribution lists. Distribution lists may be nested. This means that one or more elements of a DL may be DLs themselves. Special elements of service (see chapter 5) protect against looping.

Recipients and Distribution Lists are addressed by use of their O/R Name (Originator/Recipient Name). This O/R name comprises an O/R address, a directory name or both.

If a directory name is used, it must be looked up in a directory to find out the O/R address. The structure and components of directory names are described in CCITT X.500 / ISO 9594 [2]. The directory name provides a more user-friendly and more stable way to address a recipient than the use of the O/R address, which may be subject to change, reflecting the changing physical configuration of MHS. In case both the O/R address and a directory name are used, the O/R address is used in first instance and the directory name will only be used if submission fails.

3.2 ADDRESSING

The O/R address is modelled as an ordered list of attributes, each of which consists of a type and a value. The type is an identifier that denotes the class of information and the value is an instance of this class of information. For example, the attribute type *country-name* could in one instance have the value 'Spain':

- type = 'country-name'
- value = 'Spain'

Attributes can either be **standard** or **domain-defined**. Some standard attributes are country-name, administration-domain-name, private-domain-name, organization-name, organizational-unit-name, personal-name, etc.

Domain-defined attributes are used for compatibility with known military domains. For STANAG 5046 for example the attribute-type is *5046* and the value is a string, consisting of a concatenation of a country, command level, organization type, unit, sub-unit, staff section and special role:

- type = '5046'
- value = 'COUNTRY/COMMAND LEVEL/ORG TYPE/UNIT/SUB-UNIT/ STAFF/SECTION/SPECIAL ROLE'

Every user or DL is assigned one or more O/R addresses. An O/R address is an attribute list that distinguishes one user or DL from another and identifies the user's point of access to the MHS or the DL's expansion point (the expansion point of a DL is the MTA where the set of member names of the DL are added to the list of recipients of the message).

The following forms of O/R addresses are distinguished:

Mnemonic O/R address

This is the most important and most user-friendly form of O/R address (*the use of the* directory name instead of the O/R address is of course even more user-friendly). The mnemonic O/R address comprises some mandatory attributes that identify the ADMD, and some conditional attributes that identify a user or DL relative to this ADMD and that depend on the naming policy of that ADMD.

Mandatory Attributes: one country-name,
one administration-domain_name.

Conditional Attributes: one private-domain name,
one organization-name,
one or more organizational unit-names,
one personal-name,
one or more domain-defined attributes.

Numeric O/R address

This is the address that numerically identifies a user, like the mnemonic O/R address it identifies an ADMD and the user relative to it.

Postal O/R address

A user can also be identified by means of its postal address. The postal address identifies the PDS (Physical Delivery System) through which the user is to be accessed.

Terminal O/R address

This is the address that identifies a user by means of the network address and, if required, the type of his terminal. It may also identify the ADMD through which that terminal is accessed. In case of a computer terminal, it gives the terminal's network address and possibly its terminal identifier and terminal type. In the case of a telex terminal, it gives its telex number.

4 ELEMENTS OF SERVICE OF MHS

The elements of service of the MHS can be divided into basic elements and optional elements. Basic elements are those elements which are always available for each message, for all users. Optional elements can be chosen by the subscriber or user to be available on a per-message base or for a contractual period of time. The optional elements can be divided into those which are available for all users (essential) and those which are made available for national or international use on the basis of bilateral agreement (additional).
In this chapter all basic and optional elements of service are listed, that are associated with the different services provided in MHS. The services are divided into:

- MESSAGE TRANSFER SERVICE (MTS),
- MESSAGE STORE SERVICE (MS),
- PHYSICAL DELIVERY SERVICE (PD),
- INTERPERSONAL MESSAGING SERVICE (IPM).

Elements of service belonging to the MTS enable UAs to send and receive messages. The elements of service that belong to MS enable messages to be stored and the elements of service that belong to PD enable users to send messages and have them delivered in a physical medium to non-MHS users. The elements of service of IPM include those available for MT, MS and PD service plus some additional elements which are especially designed for sending and receipt of IP Messages between the class of IPM UAs.
Appendix A contains a definition of all different elements of service.

4.1 Basic message transfer elements of service

The basic MT elements of service enable a UA to submit messages and to have messages delivered to it:

- message identification,
- non-delivery notification,
- original encoded information types indication,
- converted indication,
- submission time stamp indication,
- delivery time stamp indication,

- access management,
- content type indication,
- user / UA capabilities registration.

4.2 Optional message transfer elements of service

The optional message transfer elements of service are divided into four different groups concerning:

1 security,
2 submission and delivery,
3 conversion,
4 query.

The classification behind each element of service indicates whether that specific element is (E)ssential or (A)dditional and whether it is available Per Message (PM) or for a Contractual Period of time (CP).

Security

• message origin authentication	A	PM
• probe origin authentication	A	PM
• report origin authentication	A	PM
• proof of delivery	A	PM
• proof of submission	A	PM
• message flow confidentiality	A	PM
• content confidentiality	A	PM
• content integrity	A	PM
• message sequence integrity	A	PM
• non-repudiation of delivery	A	PM
• non-repudiation of origin	A	PM
• non-repudiation of submission	A	PM
• message security labelling	A	PM
• secure access management	A	CP

Submission and Delivery

• grade of delivery selection	E	PM
• multi-destination delivery	E	PM
• requested delivery method	E	PM
• restricted delivery	A	CP
• DL expansion history indication	E	PM
• DL expansion prohibited	A	PM
• latest delivery designation	A	PM
• disclosure of other recipients	E	PM
• alternate recipient allowed	E	PM
• deferred delivery	E	PM
• delivery notification	E	PM
• prevention of non-delivery notification	A	PM
• deferred delivery cancellation	E	PM
• return of content	A	PM
• designation of recip. by directory name	A	PM
• originator requested alternate recipient	A	PM
• redirection of incoming messages	A	CP
• redirection disallowed by originator	A	PM
• use of distribution list	A	PM
• alternate recipient assignment	A	CP
• hold for delivery	A	CP

Conversion

The purpose of conversion by the MTS is to improve the possibilities of communication between users with different kinds of equipment. Some conversions will result in loss of information, for example the conversion from IA5 text to Teletex.

• conversion prohibition	E	PM
• conversion prohibited in case of loss of information	A	PM
• implicit conversion	A	CP
• explicit conversion	A	PM

Query

The purpose of the query service is to enable UAs to request information related to the control and operation of the MTS:

- probe E PM

4.3 Basic physical delivery elements of service

- basic physical rendition,
- ordinary mail,
- physical forwarding allowed,
- undeliverable mail with return of physical message.

4.4 Optional physical delivery elements of service

- additional physical rendition,
- counter collection,
- counter collection with advice,
- delivery via bureaufax service,
- EMS (Express Mail Service),
- physical delivery notification by MHS,
- physical delivery notification by PDS,
- physical forwarding prohibited,
- registered mail,
- registered mail to addressee in person,
- request for forwarding address,
- special delivery.

4.5 Basic message store elements of service

- stored message deletion,
- stored message fetching,
- stored message listing,
- stored message summary.

4.6 Optional message store elements of service

- stored message alert,
- stored message auto-forward.

4.7 Basic IPM elements of service

The basic IPM elements of service include all elements of service that belong to the basic MTS plus two additional elements:

- IP Message identification,
- typed body.

4.8 Optional IPM elements of service

The optional IPM elements of service include all elements of service that belong to the optional MTS and to the basic and optional PD and MS service plus some additional elements:

- blind copy recipient indication,
- non-receipt notification request indication,
- receipt notification request indication,
- auto-forwarded indication,
- originator indication,
- authorizing users indication,
- primary and copy recipients indication,
- expiry date indication,
- cross referencing indication,
- importance indication,
- incomplete copy indication,
- language indication,
- obsoleting indication,
- sensitivity indication,
- subject indication,

- replying IP Message indication,
- reply request indication,
- forwarded IP Message indication,
- body part encryption indication,
- multi-part body.

4.9 Differences between the standards of 1984 and 1988

Functional extensions

In the new standard two functional entities are added: Message Store and Physical Delivery.

Extension mechanism

The new standards define a mechanism that enables the creation of extensions to the now defined protocol. Arbitrary new extensions may be defined, using an object identifier or integer to identify the specific extension syntax. The lack of upward compatibility in X.400 (1984) will in future (1992) be avoided.

A variety of new elements of service are defined. In addition to the syntax and the encoded value of the elements of service, a pointer is added that notes whether the element is critical for submission (=transport UA -> MTA), transfer (=transport MTA -> MTA) or delivery (=transport MTA -> UA). This makes a message deliverable by the MTA, while not all elements of service are well understood (as long as these elements are not marked critical for delivery.

The most important extensions on the message transfer service protocol (P1) are:

Additional features

- Use of distribution Lists
  Instead of one recipient a list of recipients can be defined (see section 3.1).

- Use of directory services
  The directory services provide a way to address recipients via their user-friendly directory names (see section 3.1).

- Redirection

  The standards of 1984 define one alternate recipient, that takes care of delivery of all messages in a specific management domain.
  In the standards of 1988 the originator is able to define an alternate recipient for each intended recipient separately and recipients may specify their own alternates.

- Size Constraints

  In CCITT standards of 1988, size constraints are applied to a number of protocol fields. In the ISO standards however the actual values of the constraints are not an integral part of the standard. The difference between the standards is likely to remain. Most of the defined values are unchanged from the 1984 standards. Only a few have been increased (e.g. supplementary information in reports). Upper bounds for various variable length data types are defined in X.411 standards.

- Security

  In the area of security a great number of elements of service have been added for:

  authentication

  A means by which the origin of a message, probe or report can be authenticated (i.e. a signature).

  confidentiality

  Protection of a message/content from disclosure to recipients other than the intended recipients.

  integrity

  A means by which the recipient can verify that the content of the message has not been modified.

  proof of submission/delivery

  A means to authenticate that a message was submitted for delivery/delivered to the intended recipient.

  non-repudiation

  Irrevocable proof that a message was submitted or delivered, or that origin of a message is correct.

  security labelling

  Indication of sensitivity of a message, probe or report. This 'security label' is used to determine the handling of the message, in line with the security policy.

All together about 50 new elements of service are defined in the standards of 1988. Of course the new entities MS and PD require a variety of new elements (sections 4.3, 4.4, 4.5 and 4.6). The other elements are used for security (see above), interpersonal messaging (section 4.7) and for some of the new features like the use of distribution lists, registration of user capabilities, redirection, etc.
In Appendix B all new elements of service are listed in alphanumerical order.

5 MILITARY ENHANCEMENTS

5.1 INTRODUCTION

Unique military message handling requirements are supported as specified extensions to commercial standards. The Standard Automated Message Interface for NATO ACCIS (STAMINA) [5] is a specification of the extended standards (profiles) to be used for interfacing NATO C3I systems. The specifications are drawn up by NACISA, and are divided into telecommunication profiles (T-profiles) and application profiles (A-profiles). The T-profiles deal with the lower layers of OSI (layer one to four), described by T/21 (M), T/22 (M) and T/312 (M). Only the A-profiles, which are based on the layers five through seven (Session layer, Presentation layer, Application layer) will be discussed in this document. The A-profiles are strictly concerned with end-system to end-system communication without regards to the underlying transport and subsequent relay services. The defined A-profiles are:

- A/3211 , based on CCITT X.400 (1984), defines functions and procedures to be used for interconnection among Message Handling Systems (MHSs) belonging to different Private Management Domains (PRMDs).
- A/3211 (M), a military superset of A/3211 defined to fulfil the special military operational requirements.

The first profile describes the commercial X.400 service elements that are useful in a military environment, the second profile describes additional requirements, necessary in military systems, but not part of existing commercial X.400 (1984) applications.

A Standard NATO Agreement (STANAG) on message handling will be written by the AC/302 SG 9 advisory committee, and will be published in the near future (1990 - 1995).

Additional military features as described in STAMINA are all based on the existing ACP 127 telex networks (both within NATO and nations of NATO). In the next section an overview is given of the present telex based ACP 127 network and the ACP 127 message format is discussed.

5.2 MILITARY MESSAGE FORMATS

5.2.1 ACP 127 NATO SUPP-3(A)

For the preparation and handling of messages by the NATO Integrated Communication System (NICS) message relay network, messages must be formatted according to the ACP 127 NATO SUPP-3(A) [3] format. Within nations of NATO the general ACP 127 format is used.

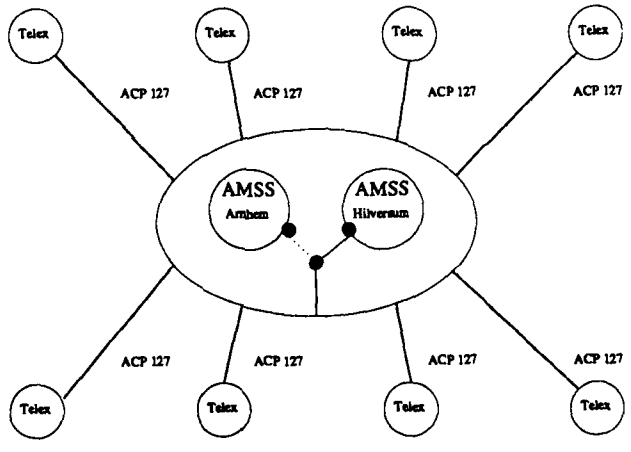

Fig. 5.1: Telex network in the Netherlands.

The telex network in the Netherlands is realized by a star network. The AMSS (=Automated Message Switching System) forms the central node; it is the central computer that connects (PTT, ASCON) all telex machines on the different sites (bases of navy, army and airforce). The AMSS is alternately located in Hilversum and Arnhem.

Only one of the computers will be active at a time, the other one will stay on standby. This national network is connected to the international NATO telex network.

An ACP 127 NATO SUPP-3(A) format based message is composed of four parts:

- Pilot (optional), formatlines (FL) A, B and C, indicating the start of transmission (A), precedence and called stations (B) and a security warning and handling instructions (C).
- Heading (formatlines 1 to 10):
  - 1: start of transmission (= FL A),
  - 2: precedence and called stations (= FL B),
  - 3: calling station,
  - 4: security warning, special handling designator, handling instructions (= FL C),
  - 5: precedence, date time group, message instructions,
  - 6: originator,
  - 7: action addressees,
  - 8: information addressees,
  - 9: exempt addressees,
  - 10: accounting information,
  - 11: separative sign 'BT'.
- Text reservation (formatlines 12a to 12g):
  - 12a: security classification, special handling,
  - 12b: subject indicator,
  - 12c: true date time group, originators reference, exercise/project/operation identification, long message identification,
  - 12d: internal handling instructions,
  - 12e: subject line,
  - 12f: reference line,
  - 12g: narrative text,
  - 13: separative sign 'BT'.
- Ending (formatlines 14 to 16):
  - 14: corrections,
  - 15: validation function,
  - 16: end of transmission function.

It is clear that the formatlines A,B and C may appear twice in a message. First they form the pilot part of the message (optional), readable for the machine, and in formatlines 1, 2 and 4 they are repeated (mandatory). Here they are readable for the recipient user.
For messages that are directed by a national Operating Agency, the general ACP 127 format may be used. The only difference with the ACP 127 NATO SUPP-3(A) format is the loss of two features:

- Message validation check. (formatline 15)
- The special Handling Designator, e.g. LLLLL for 'ATOMAL' (formatline 4).

Within the ACP 127 format four message forms are distinguished :

- Plaindress Message
- Abbreviated Plaindress Message
- Codress Message
- SYS message

Two other types are the Service Message and Abbreviated Service Message. A service message is a message between communication centres pertaining to any phase of traffic handling, communications facilities or circuit conditions. The service messages are composed of one of the above mentioned formats and therefore don't add any new formats. The lines 1, 2, 3, 4, 5, 11, 12g, 13 and 16 are the only lines that are mandatory in all formats (except the SYS-format).

Plaindress Message

A Plaindress message is a message in which originator and recipient are indicated externally of the text. In addition to the mandatory formatlines, a plaindress message will contain formatlines 6, 7 (8 and 9 when used) and 12a.

Abbreviated Plaindress Message

In the abbreviated plaindress message the address components (the additional two or four lines) are omitted for the sake of brevity. In addition to the mandatory formatlines, an abbreviated plaindress message will contain formatline 12a.

Codress Message

In a codress message the entire address (i.e. originator and addressees) is contained only within the encrypted text. The heading of any codress message contains only the minimum of information which will enable a receiving station to deal properly with the transmission. In addition to the mandatory formatlines, a codress message will contain formatline 10.

SYS formats

For direct conveyance of a message to the Message Switching Computer (AMSS) the SYS-format is used. SYS messages are extremely abbreviated messages that deal with functions like:

- opening and closing of connections
- requests for traffic status reports
- requests for the repetition of a message

SYS messages are unclassified. The order in which they are presented determines their precedence.

The format of a SYS message is:

(1) normal line 1 (start of transmission sequence)

(2) SYS-line, the letters 'SYS' followed by a space and the text for a command.

(3) normal line 16 (end of transmission function)

5.2.2 ADatP-3

Lines 12a to 12g contain the text portion of the message. This may be an ASCII text, i.e. readable text plus, depending on the used form, some mandatory additional security and subject information (lines 12a to 12f). Another possibility for these text lines is a text formatted according to ADatP-3 [4] text format.

ADatP-3 (Allied Data Publication) is entitled NATO MESSAGE TEXT FORMATTING SYSTEM (FORMETS).

FORMETS provides the rules, procedures and vocabulary to be used in the construction of character-oriented message text formats for use for information exchange between different national and NATO authorities and systems in both manual and computer-

assisted operational environments. FORMETS is to be used for all formatted character-oriented messages within NATO command and control information systems, unless specifically excluded by multinational agreement. It is concerned solely with the part of the message that the originator really wishes to convey (formatline 12a to 12g in ACP-127). The transmission of formatted messages remains in accordance with the instructions given in the relevant ACPs.

FORMETS is an artificial language and is built up of *characters, fields, sets* and *message text*. In natural language these components are respectively called *letters, words, sentences* and *text.*
Examples of these structural components and their relationship are illustrated in figure 5.2. The different fields that are used in this example are for illustration purposes only and may not correspond to agreed standards. The syntax of the illustrated message text however is correct, according to ADatP-3 standard and is suitable for implementation in an ACP 127 formatted message.

COMPONENT	EXAMPLE
CHARACTER	X
FIELD	/SUBJECT:X.400
SET	MEETING/FEL TNO/SUBJECT:X.400//
MESSAGE TEXT	EXER/OPTIONAL SET// MSGID/MANDATORY SET// REF/OPTIONAL SET/REFERENCE// MEETING/FEL TNO/SUBJECT:X.400// INVITATION/LUCIEN// 31OCT/INCL/LUNCH//

Fig. 5.2: Structural components of FORMETS.

5.3 MILITARY REQUIREMENTS

When adopting civil standards like X.400 in a military environment, there will be some shortcomings; some features will need special attention and some enhancements will be necessary. Particularly important in a military environment are 8 features: multi-homing and support of mobile hosts, multi-endpoint connections, internetworking,

network/system management, security, robustness and quality of service, precedence and preemption, realtime and tactical communications.
Comparing the commercial X.400 (1988) specifications and the military requirements, the following additional requirements on the commercial standard can be defined:

1 Internetworking possibilities with ACP 127 (Allied Communication Publication) networks. In order to be able to communicate with ACP 127 networks, some additional service elements will be needed:

EXTENDED AUTHORIZATION INFO

Element of service enables originating UA to indicate the date and time when the message was officially authorized by the releasing officer.

SUBJECT INDICATOR CODE (SIC)

Element of service enables originating UA to give distribution information to a recipient UA. The distribution information consists of up to eight subject codes as defined in ACP 127.

PRIMARY / COPY PRECEDENCE

Element of service enables originating UA to associate additional grades of delivery with a message in the content header for a primary / copy recipient. It is a military service element in addition to the MT service element 'grade of delivery'. It maps its values to the MT service element as follows:

- FLASH - URGENT (2),
- IMMEDIATE - NORMAL (0),
- PRIORITY - NORMAL (0),
- ROUTINE - NON URGENT (1).

It indicates the precedence of distribution in the recipient organization. Primary precedence takes precedence over copy precedences.

SECURITY CLASSIFICATION

Element of service enables originating UA to indicate the security level of the message. The classification LEVELS are in ascending order marked:

- NATO UNCLASSIFIED,
- NATO RESTRICTED,

- NATO CONFIDENTIAL,
- NATO SECRET,
- COSMIC TOP SECRET.

This service specifies guide-lines to be used by the recipient of the message in regard to the security classification of the message content.

SECURITY CATEGORY

Element of service enables originating UA to indicate the security category of a message. The categories conveyed are:

- ATOMAL,
- CRYPTO SECURITY,
- SPECIAL HANDLING INTEL,
- US-SITOP-ESI,
- EYES ONLY .....
- EXCLUSIVE .....

2 Support of ADatP-3 formatted messages.

3 Provision of an interorganizational message service (IOM).
So far only one class of cooperating UAs has been defined, concerning person-to-person communication. The specified content type is the interpersonal message (IPM) and the used protocol is the P2 protocol. For military environments it is useful to be able to convey messages between independent organizations. The originator should be able to convey a message without having any knowledge about recipient's organization (for example a message is sent to *airforce France*; in France a recipient UA is defined that coordinates further conveyance within the France airforce, depending on the content part of the message). A new content class should be defined: the class of interorganizational messages (IOM).

In order to fulfil the extra military requirements, the existing protocol elements may be changed, or new protocol elements may be added. The more general solution of these two, concerning upward compatibility with future extensions, is the latter: definition of additional protocol elements. Following this approach a new protocol (P77) is defined as

a superset on the existing P2 protocol, which makes the class of IOMs a superset of the class of IPMs.
Following these specifications the P1 protocol is left unchanged, which assures remaining compatibility with the existing civil X.400 networks.

6 MESSAGE HANDLING IN C3I ENVIRONMENTS

6.1 Introduction

In this chapter an overview is presented of the main C3I systems that are planned to be built for RNLA and RNLAF, and that should be operational in the next decade. An X.400 based network will be responsible for the communication between the different systems and is described in this chapter.
The LOTEX/BERDIS [6] system is discussed in section 6.2, and section 6.3 handles about ABCCIS and INTAL [7,8].

6.2 BERDIS/LOTEX

Within RNLA and RNLAF a need has shown up for an automated system for receiving, registrating, handling, constructing and sending of incoming-, outgoing-, and internal (telex) messages.
A message handling system will be built for the Ministery of Defence (MOD), army (RNLA) and Airforce (RNLAF). The computer systems for MOD and RNLA are called BERichten DIStributiesysteem (BERDIS), for RNLAF it is called LOcal Text EXchange (LOTEX). The configuration is shown in figure 6.1.

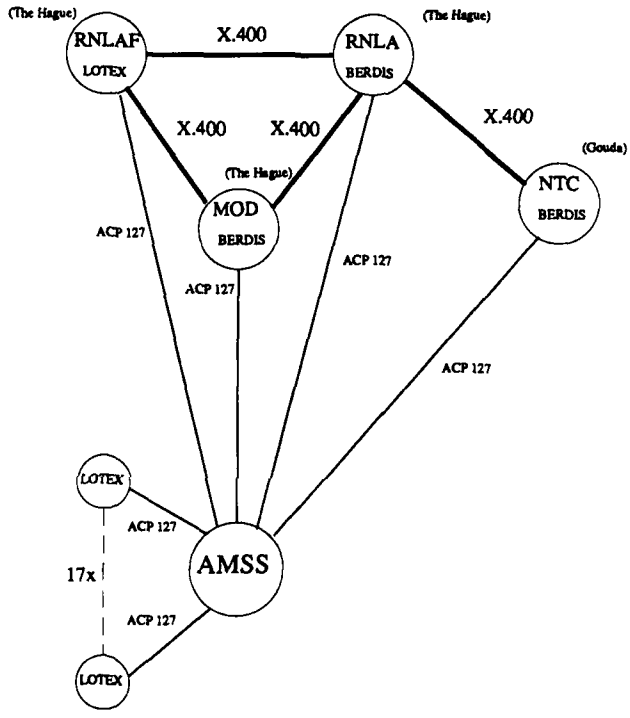

Fig. 6.1: BERDIS/LOTEX configuration in the Netherlands.

All together 21 systems will be built. In The Hague an X.400 (1984) based message handling network is implemented for the exchange of electronic messages between the ministery of defence and the headquarters of army and airforce. The National Territorial Command (NTC) in Gouda will only be connected to the army headquarter in The Hague (see fig.6.1).

The four computer systems discussed above (three in The Hague and one in Gouda) will all have an ACP 127 interface (LOTEX/BERDIS) and will be connected to the Automated Message Switching System (AMSS) in Hilversum/Arnhem. Via the AMSS communication will be possible with the other 17 LOTEX sites in the Netherlands, located on the bases and training centres of the airforce. All 21 locations will get Alcatel8300 equipment, and will only be able to communicate via the AMSS over a telex network (600 baud).
The AMSS will only be active till 1995. By then the centralised system, with AMSS as central node, will be replaced by a decentralised X.400 (1988) based communications system.

6.3 ABCCIS/INTAL

New C3I (Command, Control, Communication and Intelligence) systems are developed within the airforce. ABCCIS, an acronym for Airbase Command and Control Information System, is an integrated system to support the command and control processes concerning the preparation, use and monitoring of all weapon systems on an airbase. INTAL is an acronym for INTelligence at Airbase Level. It is an integrated system to support the command and control processes concerning the preparation, provision and evaluation of intelligence data on an airbase. Both ABCCIS and INTAL will be stand alone systems and will be located on a number of airbases in the Netherlands. Communication facilities are necessary for the exchange of electronic messages between the different INTAL and ABCCIS sites. Information about departed aircrafts, intelligence information, informal messages (e.g. invitations), etc. are sent from one airbase to another. Information is sent from INTAL to ABCCIS and from ABCCIS to INTAL. Orders are sent from higher national and NATO command centres to the airbases and status reports are sent back. For the exchange of all these messages an X.400 (1988) based network is proposed. The MTAs will be implemented in the host computers, and will control the routing of the messages. Users will be able to access the message transfer network via their User Agents (application programs, editors, etc.), which will be implemented either on the host computer or on the connected personal computers or workstations. UAs and MTAs are connected via LANs (Local Area Network) and/or the LTN (Local Transmission Network). Conveyance of the messages throughout the Netherlands will as yet be realized via the PTT/ASCON network. In 1995 NAFIN (Netherlands Armed Forces Integrated Network) will be responsible for lower layer

transport of all military data in the Netherlands, and will be connected to the LTN (ISDN, 2B + D, 64 Kbit/s) on all airbases.

6.4 ABCCIS/INTAL and X.400

In the first chapters of this document the structure of an X.400 based Message Handling System is discussed. Section 5.3 deals with the additional elements, that are necessary in a military environment. In this section a possible architecture for an X.400 based message handling system in a C3I environment (ABCCIS/INTAL) is proposed.

ABCCIS and INTAL are stand alone computer systems that will be installed on a number of airbases of RNLAF. Both ABCCIS and INTAL consist of a number of host computers and some workstations. MTAs, responsible for conveyance of the messages, will be implemented in the host computers. User agents will both be implemented in the host computers and in the connected workstations.
In figure 6.2 is illustrated that a direct connection from one private management domain to another is typical: a direct connection from an airbase to a national or NATO command centre, without intervention of an administrative management domain (PTT, see section 2.1).

Important for C3I systems in a military environment are the elements of service concerning security, notifications for delivery and non-delivery, features like timed delivery and elements that control and restrict the use of distribution lists and directory services.
These are especially the features that are new defined in the X.400 specifications of 1988.

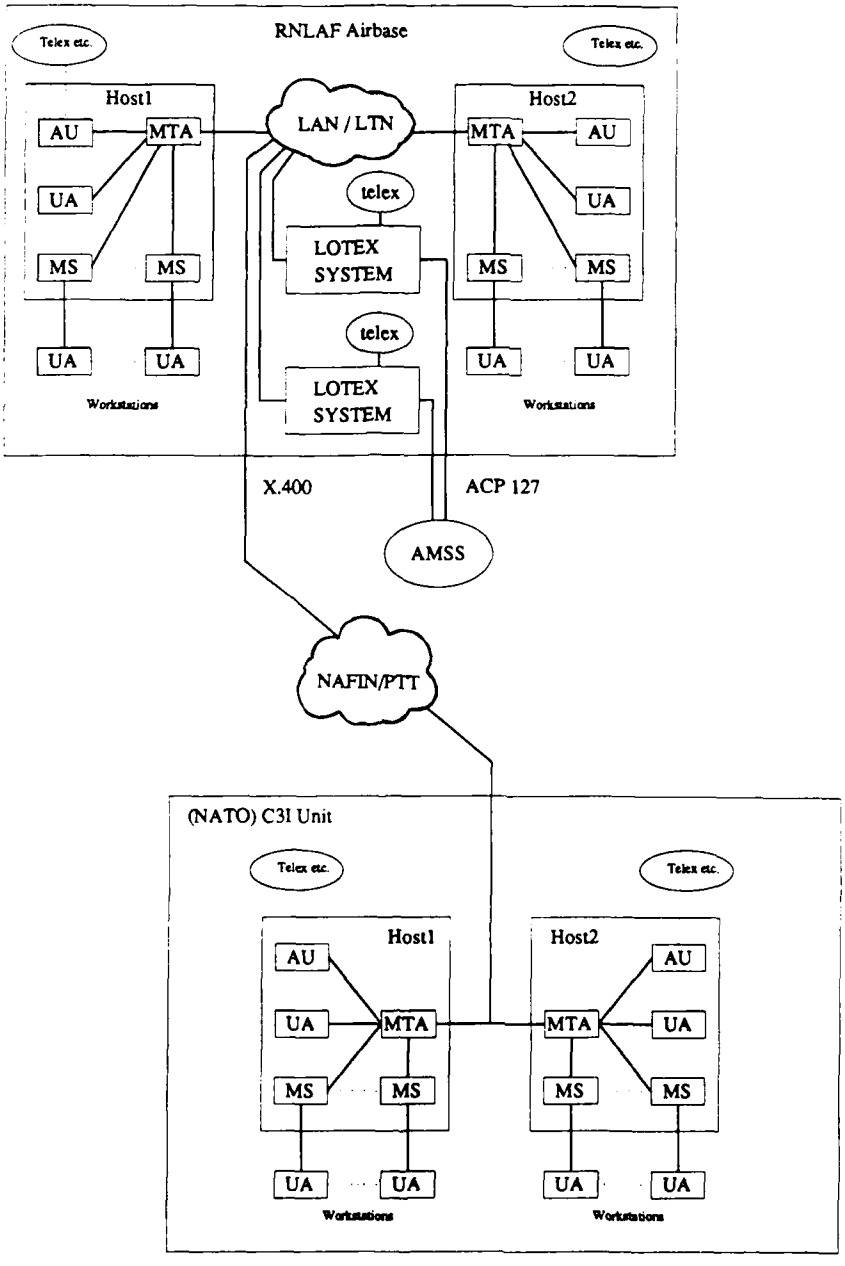

Fig. 6.2: MHS for ABCCIS/INTAL.

7 CONCLUSIONS

With respect to the possibilities of using an X.400 based Message Handling System in a military C^3I environment the following conclusions can be drawn:

- Commercial X.400 electronic messaging standards and protocols should be adopted in military environments. Message Handling Systems are introduced in the commercial world, based on the standards, provided by CCITT and ISO. Special military standards (STAMINA, STANAG) are based on these commercial standards. For the introduction of message handling systems in a military environment, the commercial available implementations of X.400 (1988) are well suitable. The few extensions and modifications that will be needed shouldn't cause serious difficulties.

- X.400 (1988) is a revised (improved) version of X.400 (1984). Additional functional components are defined and a variety of new features are added. A great number of these features are especially suitable in military environments (e.g. security). An extension mechanism is introduced, that enables the MTA to treat *unknown* extensions, providing a way to carry future (and military) extensions.

- Special military requirements should be fulfilled by definition of additional protocol elements and extensions on the existing commercial standards. By following the superset-concept upward compatibility with future extensions will be possible. STAMINA defines a new profile (A/3211M), that is a superset on the existing commercial standard (A/3211, X.400).

- X.400 defines a standard for the exchange of electronic messages between computer systems of different sizes, from different vendors and running on different operating systems. The use of commercial products based on this international standard assures interoperability, enabling users to exchange information between equipment that differs in use and location, without any knowledge of the different technical characteristics.

REFERENCES

[1] CCITT X.400 - Series of Recommendations, Blue Book draft, 1988:

X.400/ISO 10021-1 - (Message Handling Systems/Information Processing Systems - Text Communication - MOTIS) System and Service Overview.
X.402/ISO 10021-2 - (Message Handling Systems/Information Processing Systems - Text Communication - MOTIS) Overall Architecture.
X.403 - (Message Handling Systems) Conformance Testing.
X.407/ISO 10021-3 - (Message Handling Systems/Information Processing Systems - Text Communication - MOTIS) Abstract Service Definition Conventions.
X.408 - (Message Handling Systems) Encoded Information Type Conversion Rules.
X.411/ISO 10021-7 - (Message Handling Systems/Information Processing Systems - Text Communication - MOTIS) Message Transfer System.
X.413/ISO 10021-4 - (Message Handling Systems/Information Processing Systems - Text Communication - MOTIS) Message Store.
X.419/ISO 10021-5 - (Message Handling Systems/Information Processing Systems - Text Communication - MOTIS) Protocol Specifications.
X.420/ISO 10021-6 - (Message Handling Systems/Information Processing Systems - Text Communication - MOTIS) Interpersonal Messaging System.

[2] CCITT X.500/ISO 9594-1 - (Information Processing Systems) The Directory - Overview.

[3] Allied Data Publication ACP 127, NATO SUPP-3(A), January 1983, [NATO Unclassified].

[4] Allied Data Publication, ADatP - 3 part I, NATO Message Text Formatting System (FORMETS), February 1986, [NATO Unclassified].

[5] Standard Automated Message Interface for NATO ACCIS (STAMINA), February 1989, [NATO Unclassified].

[6] Berichten Distributiesysteem/Local Text Exchange (BERDIS/LOTEX), (In Dutch).
Functionele specificaties, May 1988, TVA-nummer 7010-0-127-010/0
Technisch voorschrift voor aanschaffing, May 1989, TVA nummer 7010-0-127-010/1

[7] Functional System Design Airbase Command and Control Information System, FEL TNO, November 1988, [NATO Confidential].

[8] Functional System Design System for Intelligence Processing at Airbase Level, FEL TNO, June 1989, [NATO Secret].

[9] Klaus Kühn. Electronic Messaging in a Military Environment, *proceedings AFCEA Europe symposium (9th), Brussels, October 1988.*

[10] Jim Craigie. ISO 10021 - X.400(88): a Tutorial for those Familiar with X.400(84). *Computer Networks and ISDN Systems 16 (153-160), October 1988.*

[11] W. Janssen. A functional profile for military message handling, SHAPE Technical Centre, December 1988, STC TM-847, [NATO Unclassified].

ACRONYMS AND ABBREVIATIONS

ASCON	Automatic Switched Telecommunications Network
ABCCIS	Airbase Command and Control Information System
ACCIS	Automated Command and Control Information System
ACP 127	Allied Communication Publication 127
AdatP-3	Allied Data Publication 3
ADMD	Administrative Management Domain
AMSS	Automated Message Switching System
AU	Access Unit
BERDIS	Berichten Distributiesysteem
C3I	Command, Control, Communication and Information
CCITT	Consultative Committee for International Telephone and Telegraph
DL	Distribution List
IA5	International Alphabet 5
INTAL	Intelligence at Airbase Level
IOM	Interorganizational Message
IPM	Interpersonal Message
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
LOTEX	Local Text Exchange
LTN	Local Transmission Network
MD	Management Domain
MHS	Message Handling System
MOD	Ministery of Defence
MOTIS	Message Oriented Text Interchange System
MS	Message Store
MTA	Message Transfer Agent
MTS	Message Transfer System
NACISA	NATO Communications and Information Systems Agency
NAFIN	Netherlands Armed Forces Integrated Network
NATO	North Atlantic Treaty Organization
NTC	National Territorial Command
O/R	Originator/Recipient

OSI	Open Systems Interconnection
PC	Personal Computer
PDAU	Physical Delivery Access Unit
PRMD	Private Management Domain
PTT	Post Telegraph Telephone
RNLA	Royal Netherlands Army
RNLAF	Royal Netherlands Airforce
STAMINA	Standard Automated Message Interface for NATO ACCIS
STANAG	Standard NATO Agreement
TNO	Toegepast Natuurwetenschappelijk Onderzoek Netherlands Organization for Apllied Scientific Research
UA	User Agent

ELEMENTS OF SERVICE OF MHS (1988)

ACCESS MANAGEMENT

This element of service enables a UA and MTA to establish access to one another and to manage information associated with access establishment. The element of service permits the UA and MTA to identify and validate the identity of the other.

ADDITIONAL PHYSICAL RENDITION

Element of service allows an originating user to request the PDAU to provide the additional rendition facilities (e.g.,kind of paper, coloured printing, etc.).

ALTERNATE RECIPIENT ALLOWED

Element of service enables originating UA to specify whether MTS may deliver a message to an alternate recipient in case the message cannot be delivered to the intended recipient. The alternate recipient must be assigned to receive the message ('ALTERNATE RECIPIENT ASSIGNMENT').

ALTERNATE RECIPIENT ASSIGNMENT

Element of service enables a UA to have certain messages delivered to it for which the addressing attributes contain certain inconsistencies or lacks. Specified is which attributes will have to give an exact match and which attributes won't be essential for delivery of a message. An organization may for example address all messages to certain UA for which country name, administration management domain name en organization name are correct, but for which a personal name is specified that doesn't exist. These messages can be dealed with manually now.

AUTHORIZING USERS INDICATION

Element of service enables originator to specify to the recipient who authorized the sending of the message.

AUTO-FORWARDED INDICATION

Element of service enables recipient to determine that the received IP message is an auto-forwarded IP message. Recipient IPM UA can for example decide to prevent further auto-forwarding.

BASIC PHYSICAL RENDITION

Element of service enables PDAU to convert an MHS message into a physical message.

BLIND COPY RECIPIENT INDICATION

Element of service enables originator to specify the names of one or more additional recipients of a message. The names are not disclosed to the other recipients.

BODY PART ENCRYPTION INDICATION

Element of service enables originator to indicate that a body part of an IP-message is encrypted.

CONTENT CONFIDENTIALITY

Element of service enables the originator to encrypt the message content.

CONTENT INTEGRITY

Element of service enables the originator to provide the recipient(s) of the message with a means to validate on a per-recipient basis that the content of the message has not been modified.

CONTENT TYPE INDICATION

This element of service enables the originating UA to indicate the content type of each submitted message. An example of a content type is the contents generated by the IPM (Inter Personal Message) class of cooperating UAs.

CONVERSION PROHIBITION

Element of service enables originating UA to prevent MTS from any encoded information type conversion(s) on a message.

CONVERSION PROHIBITION IN CASE OF LOSS OF INFORMATION

Element of service enables originating UA to instruct MTS not to perform any information type conversion(s) on a presented message in case this conversion will result in a loss of information.

CONVERTED INDICATION

Element of service enables MTS to inform the recipient UA about performed encoded information type conversions on a delivered message.

COUNTER COLLECTION

Element of service allows an originating user to instruct PDS to keep the physical message ready for counter collection at a specified post office.

COUNTER COLLECTION WITH ADVICE

Element of service allows an originating user to instruct PDS to keep the physical message ready for counter collection at a specified post office, and to inform the recipient via telephone, teletex or telex.

CROSS REFERENCING INDICATION

Element of service enables originator to convey with a message the globally unique identification of one or more other messages. This will enable the recipient to retrieve easily a copy of the referenced message(s) from storage.

DEFERRED DELIVERY

Element of service that enables originating UA to instruct MTS to deliver a message no sooner than a specified time and date. Delivery will take place as soon as possible after specified time and date.

DEFERRED DELIVERY CANCELLATION

Element of service enables originating UA to instruct MTS to cancel a previous submitted deferred delivery message.

DELIVERY NOTIFICATION

Element of service enables originating UA to be informed explicitly upon successful delivery of a message. The notification contains an indication of the message and time and date of delivery. In case of multi-destination delivery the notification can be given on a per-message base or for all messages together.

DELIVERY TIME STAMP INDICATION

Element of service enables MTS to inform recipient UA about the time and date on which the MTS delivered a message.

DELIVERY VIA BUREAUFAX SERVICE

Element of service enables originating user to instruct the PDAU and associated PDS to use the Bureaufax Service for transport and delivery.

DESIGNATION OF RECIPIENT BY DIRECTORY NAME

Element of service enables the originator to use a directory name instead of the O/R address of the intended recipient.

DISCLOSURE OF OTHER RECIPIENTS

Element of service enables the originator UA of a multi-destination message to specify whether the different recipient UAs are informed about the O/R names of the other recipient UAs

DL EXPANSION HISTORY INDICATION

Element of service provides to the recipient at delivery information about the distribution list(s) through which the message has arrived.

DL EXPANSION PROHIBITED

Element of service enables the originator to specify that if any of the recipients refers directly or indirectly to a distribution list, no expansion will occur. If not prohibited a non-delivery notification will be sent to the originator.

EMS (EXPRESS MAIL SERVICE)

Element of service enables originating user to instruct the PDS to use the accelerated letter circulation and delivery service or some national equivalent for transport and delivery of the message.

EXPIRY DATE INDICATION

Element of service enables originator to specify a date and time after which an IP message is considered invalid. Recipient may for example then decide to delete or file the message.

EXPLICIT CONVERSION

Element of service enables originating UA to instruct MTS to perform a certain conversion on a message.

FORWARDED IP MESSAGE INDICATION

Element of service allows a forwarded IP-message to be conveyed as the body or one of the body parts of an IP-message.

GRADE OF DELIVERY SELECTION

Element of service enables originating UA to add a priority to a message. The different priorities are: 'urgent', 'non-urgent' and 'normal'. The time-periods required for transfer will be in accordance with these priorities.

HOLD FOR DELIVERY

Element of service enables UA to request MTS to hold all messages and notifications till a later time. UA may specify when it won't be able to take delivery of messages and notifications, and also, when it will be again.

IMPLICIT CONVERSION

Element of service enables originating UA to instruct MTS to perform an implicit conversion on all presented messages for a certain period of time.

IMPORTANCE INDICATION

Element of service enables originator to indicate the importance of a message. The possible classifications are: low, normal and high.

INCOMPLETE COPY INDICATION

Element of service enables originator to indicate that in this IP Message one or more body-parts of the original message (with the same IP-Message identification) are missing.

IP MESSAGE IDENTIFICATION

Element of service is used by cooperating IPM UAs for identification of sent and received IP-messages (for example used in receipt notifications).

LANGUAGE INDICATION

Element of service enables originating UA to indicate the language type(s) of a submitted IP-message.

LATEST DELIVERY DESIGNATION

Element of service enables the originator to specify a time before which delivery should occur. If the Mts cannot deliver by the time specified, the message is not delivered and is cancelled.

MESSAGE FLOW CONFIDENTIALITY

Element of service enables the originator to protect information which might be derived from observation of the message flow.

MESSAGE IDENTIFICATION

Element of service is used to distinguish the messages from each other. It is assigned by the originating MTA when the message is submitted, and is chosen to be different from that of any other message, probe or delivery report within the MTS.

MESSAGE ORIGIN AUTHENTICATION

Element of service enables originator of a message to proof origination to recipient and to any MTA through which the message is transferred (i.e. a signature).

MESSAGE SECURITY LABELLING

Element of service enables the originator to define which parts of the MHS may handle the message. For example to refrain the message from being delivered to a recipient with insufficient security clearance.

MESSAGE SEQUENCE INTEGRITY

Element of service enables the originator to provide the recipient with a means to verify the sequence of the messages, to protect the message from reordening.

MULTI-DESTINATION DELIVERY

Element of service enables originating UA to specify that a messages should be delivered at more than one recipient UA.

MULTI-PART BODY

Element of service allows an originator to send an IP-message with a body that is partitioned into several parts. The nature and attributes of each body part are conveyed along with the body part.

NON-DELIVERY NOTIFICATION

Element of service enables the MTS to notify an originating UA if a submitted message was not delivered to the specified recipient UA(s). The reason of non-delivery is included as part of the notification. In case of a multi-destination message, a non-delivery notification can either refer to one or to all of the recipient UAs.

NON RECEIPT NOTIFICATION REQUEST INDICATION

Element of service enables originator to ask for a notification in case a message is unreceivable. The recipient UA will send a non-receipt notification when any of the following events will occur :

- The IP message was auto-forwarded to another recipient.
- IP message was discarded by recipient's IPM UA prior to receipt.
- Connection to recipient was closed before receipt of the message.

NON-REPUDIATION OF DELIVERY

Element of service enables the originator of a message to obtain irrevocable proof that the message was delivered, to protect against an attempt of recipient to deny delivery.

NON-REPUDIATION OF ORIGIN

Element of service enables the originator to provide recipient with irrevocable proof of the origin of the message, to protect against an attempt of originator to revoke the message or its content.

NON-REPUDIATION OF SUBMISSION

Element of service enables the originator of a message to obtain irrevocable proof that the message was submitted to the MTS for delivery to a specified recipient. This will protect against an attempt of MTS to deny submission.

OBSOLETING INDICATION

Element of service enables originator to indicate that one or more submitted IP messages are expired.

ORDINARY MAIL

Element of service enables the PDS to transport and deliver the letter produced from the MHS message in the mode available through the ordinary letter mail service in the country of destination.

ORIGINAL ENCODED INFORMATION TYPES INDICATION

Element of service enables an originating UA to specify to the MTS the encoded information types of a message being submitted, and to inform the recipient UA about these information types.

ORIGINATOR INDICATION

Element of service enable originator UA to specify its identity in a user-friendly way to recipient UA (nickname in stead of O/R name).

ORIGINATOR REQUESTED ALTERNATE RECIPIENT

Element of service enables the originator to define an alternate recipient for each intended recipient.

PHYSICAL DELIVERY NOTIFICATION BY MHS

Element of service allows an originating user to request that MHS sends an explicit notification to the originator about successful or unsuccessful delivery of the physical message. The notification will only provide information and no physical record is created.

PHYSICAL DELIVERY NOTIFICATION BY PDS

Element of service allows an originating user to request that PDS sends an explicit notification to the originator about successful or unsuccessful delivery of the physical message. The notification serves as a record of delivery for the originating user to retain for reference.

PHYSICAL FORWARDING ALLOWED

Element of service enables the PDS to forward the physical message to a forwarding address if the recipient has changed his address and indicated this to the PDS.

PHYSICAL FORWARDING PROHIBITED

Element of service enables originating user to instruct PDS not to forward the physical message to a forwarding address.

PREVENTION OF NON-DELIVERY NOTIFICATION

Element of service enables UA to prevent MTS from sending a non-delivery notification to originating UA in case the message cannot be delivered.

PRIMARY AND COPY RECIPIENTS INDICATION

Element of service enables originator to indicate which users are primary and which users are copy recipients of a message. Each recipient will be able to notice to which category belongs. The difference between primary en copy recipients is not defined. The primary

recipients might for example be expected to react on a message whereas copy recipients may remain silent.

PROBE

Element of service enables a UA to verify before submission whether a particular message could be delivered. The MTS provides the submission information and generates delivery and/or non delivery notifications indicating whether a message containing the same information could be delivered.

PROBE ORIGIN AUTHENTICATION

Element of service enables the originator of a probe to proof origination of the probe to any MTA through which the probe is transferred.

PROOF OF DELIVERY

Element of service enables originator to ask the recipient(s) of a messages for a proof that a message was actually delivered.

PROOF OF SUBMISSION

Element of service enables originator to ask the MTS for a proof that a message was actually submitted to MTS for delivery to the intended recipient.

RECEIPT NOTIFICATION REQUEST INDICATION

Element of service enables originator to ask for a notification when the IP message being sent is received.

REDIRECTION DISALLOWED BY ORIGINATOR

Element of service enables the originator to instruct MTS that the submitted message will not be redirected, in case recipient will ask for redirection.

REDIRECTION OF INCOMING MESSAGES

Element of service enables UA to instruct MTS to redirect incoming messages to another UA or DL.

REGISTERED MAIL

Element of service enables originating user to instruct PDS to handle the physical message as registered mail.

REGISTERED MAIL TO ADDRESSEE IN PERSON

Element of service enables originating user to instruct PDS to handle the physical message as registered mail and deliver it to the addressee only.

REPLY REQUEST INDICATION

Element of service allows an originator to ask the recipient for an IP-message in reply of the IP-message being submitted. The date on which reply is expected may be specified.

REPLYING IP MESSAGE INDICATION

Element of service allows the originator of an IP-message to indicate that the IP-message is being sent in reply to another IP-message.

REPORT ORIGIN AUTHENTICATION

Element of service enables the originator of a message or probe to authenticate origination of a report (i.e. a signature).

REQUEST FOR FORWARDING ADDRESS

Element of service enables originating user to instruct the PDS to provide the forwarding address if the recipient has changed his address and indicated this to the PDS.

REQUESTED DELIVERY METHOD

Element of service enables recipient UA to specify the aimed method(s) of message delivery. If the specified method(s) cannot be satisfied non-delivery will result.

RESTRICTED DELIVERY

Element of service enables recipient UA to specify that messages from certain UAs or DLs will not be accepted.

RETURN OF CONTENT

Element of service enables originating UA to ask for a return of the content of a message, together with a non-delivery notification. In case of any encoded information type conversion on the message this will be prevented however.

SECURE ACCESS MANAGEMENT

Element of service enables MTS user and MTS to establish secure access to one another, or to establish an association between an MTA and another MTA.

SENSITIVITY INDICATION

Element of service enables originator to indicate the relative security to be betrayed upon receipt of a message.

SPECIAL DELIVERY

Element of service enables originating user to instruct the PDS to use the special delivery service for transport of the letter produced from the MHS message.

STORED MESSAGE ALERT

Element of service enables the user of an MS to specify some criteria that cause an alert to be generated to the user when a message arrives that satisfies these criteria.

STORED MESSAGE AUTO-FORWARD

Element of service enables the user of an MS to specify which messages stored in MS should be auto-forwarded to specified users or DL s. The user of the MS can select several sets of criteria chosen from the attributes available in the MS.

STORED MESSAGE DELETION

Element of service enables a recipient UA to delete a message from the MS.

STORED MESSAGE FETCHING

Element of service enables a recipient UA to fetch from the MS a message or a part of a message.

STORED MESSAGE LISTING

Element of service enables a recipient UA to list information about the stored messages.

STORED MESSAGE SUMMARY

Element of service enables recipient UA to get a count of the number of stored messages that satisfy some specified criteria.

SUBJECT INDICATION

Element of service allows the originator to indicate the subject of an IP-message being sent.

SUBMISSION TIME STAMP INDICATION

Element of service enables MTS to inform originating UA and each recipient UA about the time and date on which the message was submitted to the MTS.

TYPED BODY

Element of service permits the nature and attributes of the body to be conveyed along with the body. Supported body types are:

- IANo.5 text for unformatted messages
- Forwarded IP messages

UNDELIVERABLE MAIL WITH RETURN OF PHYSICAL MESSAGE

Element of service enables PDS to return the physical message without delay, with reason indicated to the originator, if it cannot be delivered to the addressee.

USE OF DISTRIBUTION LIST

Element of service enables an originating UA to specify a distribution list (DL) instead of all the individual recipients (UAs and/or nested DLs).

USER / UA CAPABILITIES REGISTRATION

This element of service enables a UA to indicate to its MTA some information about the content type(s), maximum content length and/or encoded information type(s) of messages that it is willing to have delivered to it.

NEW ELEMENTS OF SERVICE IN 1988

- Aditional Physical rendition,
- Basic Physical Rendition,
- Content Confidentiality,
- Content Integrity,
- Conversion Prohibition in Case of Loss of Information,
- Counter Collection,
- Counter Collection With Advice,
- Delivery via Bureaufax Service,
- Designation of Recipient by Directory Name,
- DL Expansion History Indication,
- DL Expansion Prohibited,
- EMS (Express Mail Service),
- Incomplete Copy Indication,
- Language Indication,
- Latest Delivery Designation,
- Message Flow Confidentiality,
- Message Origin Authentication,
- Message Security Labelling,
- Message Sequence Integrity,
- Non-repudiation of Delivery,
- Non-repudiation of Origin,
- Non-repudiation of Submission,
- Ordinary Mail,
- Originator Requested Alternate Recipient,
- Physical Delivery Notification by MHS,
- Physical Delivery Notification by PDS,
- Physical Forwarding Allowed,
- Physical Forwarding Prohibited,
- Probe Origin Authentication,
- Proof of Delivery,
- Proof of Submission,

- Redirection Disallowed by Originator,
- Redirection of Incoming Messages,
- Registered Mail,
- Registered Mail to Addressee in Person,
- Report Origin Authentication,
- Request for Forwarding Address,
- Requested Delivery Method,
- Restricted Delivery,
- Secure Access Management,
- Special Delivery,
- Stored Message Alert,
- Stored Message Auto-forward,
- Stored Message Deletion,
- Stored Message Fetching,
- Stored Message Listing,
- Stored Message Summary,
- Undeliverable Mail with Return of Physical Message,
- Use of Distribution List,
- User / UA Capabilities Registration.

REPORT DOCUMENTATION PAGE (MOD-NL)

1. DEFENSE REPORT NUMBER (MOD-NL)	2. RECIPIENT'S ACCESSION NUMBER	3. PERFORMING ORGANIZATION REPORT NUMBER
TD89-3866		FEL-89-B260
4. PROJECT/TASK/WORK UNIT NO.	**5. CONTRACT NUMBER**	**6. REPORT DATE**
20357	-	SEPTEMBER 18, 1989
7. NUMBER OF PAGES	**8. NUMBER OF REFERENCES**	**9. TYPE OF REPORT AND DATES COVERED**
44	11	FINAL REPORT

10. TITLE AND SUBTITLE
MESSAGE HANDLING IN A MILITARY ENVIRONMENT

11. AUTHOR(S)
W.A. LEVENBACH

12. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
PHYSICS AND ELECTRONICS LABORATORY TNO, P.O. BOX 96864, 2509 JG THE HAGUE
OUDE WAALSDORPERWEG 63, THE HAGUE, THE NETHERLANDS

13. SPONSORING/MONITORING AGENCY NAME(S)
TNO DIVISION OF NATIONAL DEFENSE RESEARCH, THE NETHERLANDS

14. SUPPLEMENTARY NOTES
THE PHYSICS AND ELECTRONICS LABORATORY IS PART OF THE NETHERLANDS ORGANIZATION FOR APPLIED SCIENTIFIC RESEARCH

15. ABSTRACT (MAXIMUM 200 WORDS, 1044 POSITIONS)
THIS REPORT DEALS WITH THE USE OF MESSAGE HANDLING SYSTEMS (MHS) IN A MILITARY C^3I ENVIRONMENT. THE MAIN ELEMENTS OF MHS, AS THEY ARE DEFINED IN THE X.400 SERIES OF RECOMMENDATIONS OF CCITT/ISO, ARE BRIEFLY DISCUSSED.
A SLIGHT DIFFERENCE BETWEEN THE MILITARY AND A COMMERCIAL ENVIRONMENT CAUSES SPECIAL REQUIREMENTS FOR MILITARY MESSAGE HANDLING. THESE MILITARY DEMANDS ARE DISCUSSED ALONG WITH THE NOW USED STANDARD FOR MILITARY MESSAGE HANDLING (ACP 127) IN TELEX BASED SYSTEMS. THE MOST RECENT VERSION OF X.400/MOTIS (1988), DEFINING THE STANDARD FOR COMMERCIAL MHSS, SEEMS ALSO TO DEFINE A GOOD STANDARD FOR USE IN A MILITARY ENVIRONMENT (WITH SOME EXTENSIONS AND MODIFICATIONS). THE USE OF COMMERCIAL AVAILABLE X.400/MOTIS SYSTEMS IS THEREFORE A GOOD CHOICE FOR CREATION, SUBMISSION AND DELIVERY OF MESSAGES IN A MILITARY ENVIRONMENT.

16. DESCRIPTORS	IDENTIFIERS
COMMAND, CONTROL, COMMUNICATION & INTELLIGENCE	MESSAGE HANDLING
COMMUNICATION NETWORKS	MILITARY ENVIRONMENT
DATA TRANSMISSION	X.400/MOTIS
PROTOCOLS	
TELECOMMUNICATION	

17a. SECURITY CLASSIFICATION (OF REPORT)	17b. SECURITY CLASSIFICATION (OF PAGE)	17c. SECURITY CLASSIFICATION (OF ABSTRACT)
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED

18. DISTRIBUTION/AVAILABILITY STATEMENT	17d. SECURITY CLASSIFICATION (OF TITLES)
UNLIMITED AVAILABLE	UNCLASSIFIED