NISTIR 4608

Electronic Data Interchange in Message Handling Systems

Paul Markovitz

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Computer Systems Laboratory
Systems and Network Architecture Division
Gaithersburg, MD 20899

This Report Was Prepared With Funding Provided By The Internal Revenue Service Under Basic Agreement ID 90001-NIST, Project Element ID 90001-03-NIST.

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

NIST

NISTIR 4608

Electronic Data Interchange in Message Handling Systems

Paul Markovitz

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Computer Systems Laboratory
Systems and Network Architecture Division
Gaithersburg, MD 20899

This Report Was Prepared With Funding Provided By The Internal Revenue Service Under Basic Agreement ID 90001-NIST, Project Element ID 90001-03-NIST.

June 1991

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

Table of Contents

1. Introduction

Business related information, such as invoices and purchase orders, is often exchanged between companies. Mailing paper documents has been the traditional method of exchange. Since many business transactions today are processed by computers, transferring information electronically reduces paperwork and transcription errors, minimizes cost, and increases response time. The electronic transmission of business-oriented data is known as EDI (Electronic Data Interchange).

Companies participating in EDI are called trading partners. The typical EDI transaction involves exchanging information units, called EDI interchanges, between two trading partners. EDI interchanges are not structured to be human-readable, but rather to trigger responses from a computer process. For example, a transaction between a buyer application and a vendor application may automatically submit payment to the vendor or update the vendor's inventory; no human intervention is required. EDI interchanges contain all the information needed for their assembly and disassembly by a computer application, in addition to the data being transmitted.

There are many standardized formats for EDI interchanges. The three most widely recognized are X12, EDIFACT (Electronic Data Interchange for Administration, Commerce, and Transport), and UN/TDI (United Nations Trade Data Interchange). The X12 family of standards is approved by the ANSI (American National Standards Institute) and is prevalent in North America. EDIFACT and UN/TDI were developed by the UN/ECE (United Nations Economic Commission for Europe). UN/TDI is commonly used in Europe while EDIFACT is used internationally. X12, EDIFACT, and UN/TDI (as is true for most EDI standards) are not compatible.

EDI standards specify data formats (syntax), but are designed to be independent of communications protocols. Tapes, telex, and proprietary communications are all used to transmit EDI information. In addition to compatibility problems between dissimilar EDI applications, non-interoperating computer systems have prevented interconnection between compatible applications. In this case, an X12 application on Company A's system may be incapable of exchanging interchanges across a network with an X12 application on Company B's system. This connectivity problem is solved by the MHS (Message Handling System), as defined in the CCITT (Consultative Committee on International Telephony and Telegraphy) F.400 series of Recommendations [1] and X.400 series of Recommendations [2].

The MHS provides a global message transfer service. Although only one MHS application, the Interpersonal Messaging service and its corresponding P2 protocol is standardized, the general structure of the MHS facilitates the transfer of any message type, including messages containing EDI interchanges. Using the MHS, EDI interchanges may be transferred between compatible EDI applications implemented on heterogeneous computer systems. Any EDI format, including X12, EDIFACT, and UN/TDI may be transferred using the MHS.

There are two current approaches that utilize the MHS to transmit EDI data. Both approaches are based on extensions to existing MHS profiles. Guidelines developed by the CEC (Commission of the European Communities) specify encapsulating EDI information inside an IP (Interpersonal) message. This solution has been termed the P2 approach since it employs the P2 protocol, and is used extensively in Europe. Guidelines developed by the OIW (Open Systems Interconnection (OSI) Implementor's Workshop) label EDI information

to be transferred via the MHS as "undefined". The numeric value 0 is used to identify an undefined MHS message content protocol, thus, this second solution is called the P0 approach. Since a numeric value of 0 can identify any undefined message content protocol, bilateral agreements must be established between trading partners using the P0 approach. Conversion of MHS messages containing EDI data between the P0 and P2 format specifications can be performed by a gateway.

The CCITT recognized the need for one standardized solution for exchanging EDI information via the MHS. A special CCITT associate rapporteur subgroup was formed, and in June, 1990, completed two draft recommendations. The Recommendations: F.435, EDI Messaging Service, and X.435, EDI Messaging System, define the services and protocol required to convey EDI interchanges via the MHS.

The purpose of this paper is to explicate EDI messaging. Introductory information is presented in Sections 2 and 3. Section 2 overviews the MHS, the carrier service for EDI data, and Section 3 overviews IP messaging, which EDI messaging parallels. Section 4 details EDI messaging, including descriptions of both the EDI messaging system and services available to an EDI messaging user. Section 5 discusses the status of the EDI messaging draft Recommendations and concludes the paper.

Three appendices are also included in this paper. Appendix A contains a list of abbreviations. Appendix B provides a glossary of MHS terms, and Appendix C briefly describes EDI messaging elements of service.

2. MHS Overview

The MHS is one of several standardized OSI applications. It provides a general, application independent, message transfer service. The MHS was originally defined in the CCITT 1984 series of Recommendations and updated in the CCITT 1988 X.400 series of Recommendations. Public services available to the MHS user are defined in the CCITT 1988 F.400 series of Recommendations.

The purpose of the MHS is to enable users to exchange messages on a store-and-forward basis. The MHS user, which resides outside the MHS, may be a person or computer process. Users are classified as either direct users, which exchange messages via the MHS only, or indirect users, which exchange messages through a communications system linked to the MHS, such as a physical delivery system. A user that creates a message to be submitted to the MHS is called an originator. A user that receives a message delivered by the MHS is called a recipient.

The MHS comprises a variety of components. Section 2.1 describes these components as cooperating entities in the MHS functional model. Sections 2.2 through 2.7 discuss message structure, notifications, management domains, naming and addressing, directory services, and security respectively.

2.1. Functional Model

A functional model of the MHS is shown in Figure 1. The MHS is a collection of MTAs (Message Transfer Agents), MSs (Message Stores), UAs (User Agents), and AUs (Access Units). MTAs perform the store-and-forward message transfer function. MSs provide storage for messages. UAs enable users to access the MHS, and AUs provide links to

other communication systems (e.g., the postal system). A more detailed description of each of these entities follows.

MTAs comprise the MTS (Message Transfer System), the principal component of the MHS. A message is submitted to an MTA by an originating UA, MS or AU, transferred to the recipient MTA(s), and delivered to one or more recipient UAs, MSs, or AUs. If the message is addressed to multiple recipients, the appropriate MTAs perform any splitting (i.e., replicating) of the message needed for delivery to each recipient.

Messages are transferred between MTAs on a cooperating store-and-forward basis. Since no end-to-end association is required, the MTA serving the message recipient need not be active when the message leaves the originating MTA. The message may be stored at a relay (i.e., intermediate) MTA until the recipient MTA becomes operational.

MTA relaying allows messages to be transferred between MTAs that are not directly connected in the MTS. As shown in Figure 1, messages may be relayed from "MTA 1" to MTA 3" by either "MTA 2" or "MTA 4". "MTA 2", which has no associated UAs or AUs, is used only for relaying. An MTA examines addressing information on the message envelope (see Section 2.2) to determine whether a message needs to be relayed and which MTA will receive the relayed message.

MTAs transfer messages whose content may be encoded in any format. MTAs neither examine nor modify the content of messages except when performing a conversion. Conversion increases the effectiveness of the MHS by allowing users to submit messages in one encoded format (e.g., telex), and have them delivered in another encoded format (e.g., IA5). A UA can register with the MTA the encoded information types that may be delivered, and request the MTA to perform any required conversions.

The UA is the MHS component that enables a user to access the MHS, for both the origination and reception of messages. When submitting messages, the UA supplies to an MTA, either directly or indirectly via an MS, the message content, the address(es) of the message recipient(s), and the MTS services that are being requested. The message content is the information that the originator wants transferred to the message recipient(s). The address and service request data are used by the MTS to deliver the message. When receiving messages, the UA may accept delivery of messages directly from an MTA, or it may employ an MS to accept delivery of messages, and retrieve them from the MS at a later time.

UAs are grouped into classes based on the type of messages (i.e., Interpersonal messages) they transfer. There may be many different classes of UAs. As long as the recipient UA can interpret the data sent by the originating UA, meaningful communication can occur. Since UAs use services provided by the MTS, they must comply with the rules of interaction when submitting and accepting delivery of a message.

UAs provide many functions outside the realm of standardization. The originator's UA assists with creating and editing messages; the recipient's UA assists with displaying and printing messages. If an MS is not present, a UA also provides for message storage and management.

The MS is an optional MHS component that acts as an intermediary between a UA and MTA. The primary purpose of the MS is to provide a repository for the delivery of messages. The UA can retrieve messages from this repository. By using an MS to accept

delivery of messages, a UA is not required to be constantly available. This is especially useful for UA applications implemented on personal computers. The MS may also submit and forward messages on behalf of the UA, and notify the UA at the time of message delivery.

The AU is the MHS component that provides a gateway between the MHS and another communication system. AUs may, for example, provide intercommunication with telex, teletex, and facsimile systems. Another AU, the PDAU (Physical Delivery Access Unit) enables MHS users to send messages to users residing on a physical delivery system, such as the Postal Service. Communication through a PDAU is currently uni-directional; the transfer of messages from a physical delivery system to the MHS has not been standardized yet.

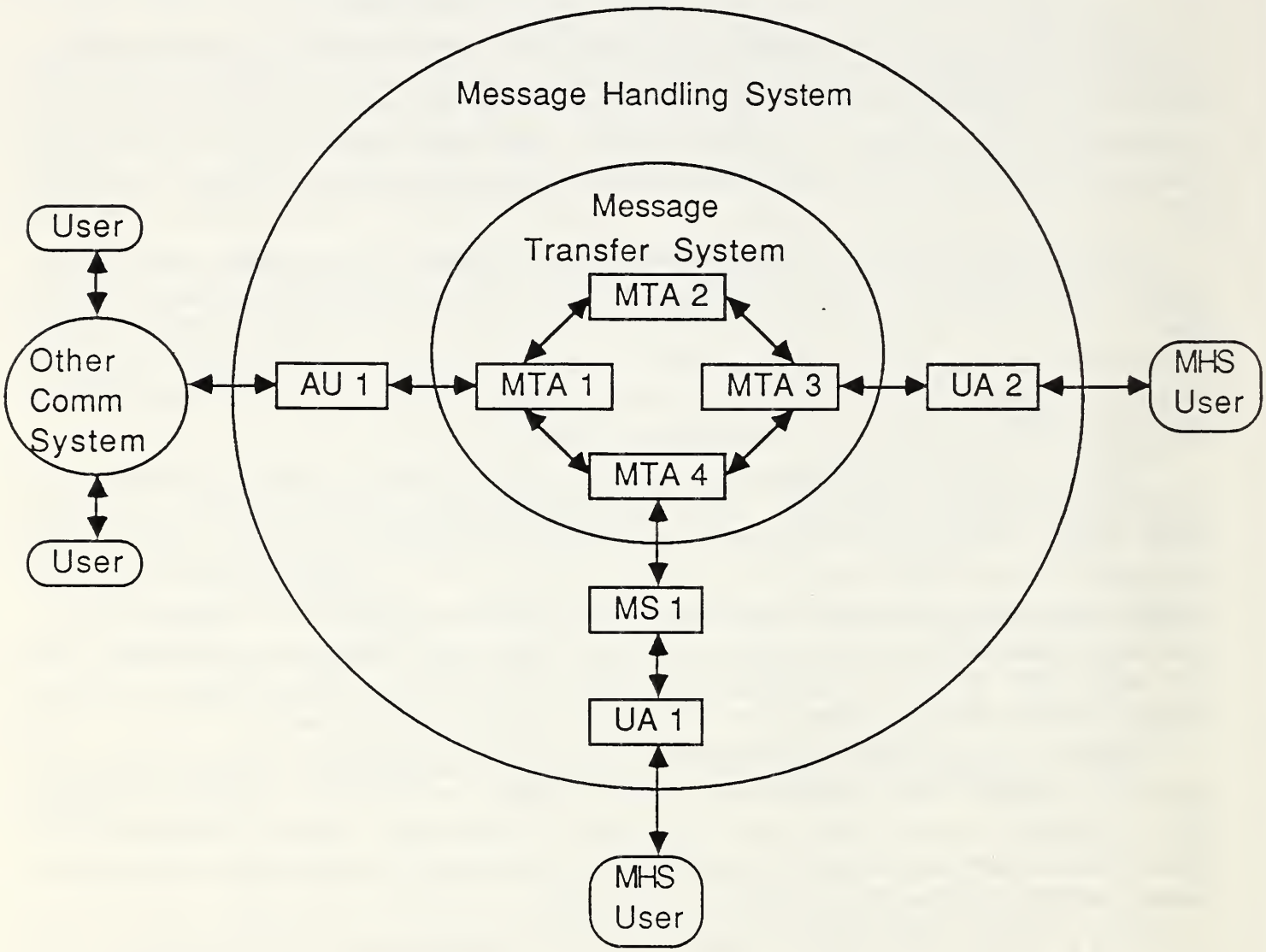

Figure 1

MHS Functional Model

2.2. Message Structure

The structure of an MHS message is shown in Figure 2. It consists of a message envelope and a message content. As with a postal message, the envelope represents the information required by the MTS to deliver the message, such as the address(es) of the recipient(s) and any special handling instructions. The message content represents the information that the originator wants conveyed to the message recipient(s).

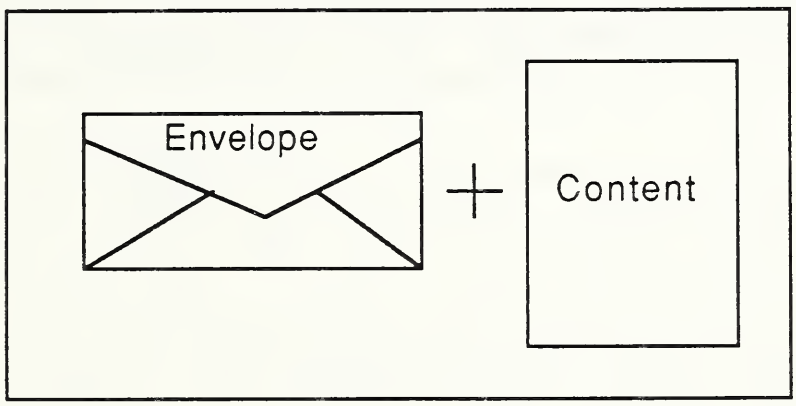

Figure 2
MHS Message Structure

2.3. Notifications

The basic MT (Message Transfer) service provides notification of message non-delivery. When a message cannot be delivered by the MTS, a non-delivery notification is generated and returned to the originator. The content of the non-delivery notification contains status information about the subject message. The OIW Agreements [5] define the following Quality of Service time targets based on the subject message's grade of delivery.

Grade of Delivery	95% Delivered Before
Urgent	4 hours
Normal	24 hours
Non-Urgent	36 hours

The MT service also provides notification of delivery as an optional service. If a message originator requests acknowledgement of successful delivery, a delivery notification is returned to the originator by the MTS upon delivery of the subject message.

2.4. Management Domains

MTAs can be managed by different organizations or administrations. An administration is either the central PTT (Postal Telephone and Telegraph) service in a country or, as in the United States, a common carrier recognized by the CCITT. The collection of MTAs and UAs owned and operated by an administration is called an ADMD (Administration Management Domain). The collection of MTAs and UAs owned and operated by a private organization is called a PRMD (Private Management Domain). Figure 3 shows how PRMDs can cooperate with ADMDs and with each other to provide the message transfer service. All ADMDs must comply with the CCITT Recommendations. PRMDs that wish to use a message transfer system provided by an ADMD must comply with the CCITT Recommendations at the point of interconnection.

CCITT has mandated that Transport Class 0 and the CONS (Connection Oriented Network Service) be used in message systems provided by ADMDs. The OIW Agreements allow PRMDs to use either Transport Class 0 and CONS or Transport Class 4 and either CONS or the CLNS (Connectionless Network Service) at OSI layers 3 and 4. Transport Class 4 and the CLNS are the alternatives most widely implemented in the United States. If a PRMD that does not use Transport Class 0 and CONS wishes to interoperate with an ADMD, a relay MTA containing both Transport and Network Layer implementations must be provided by either the PRMD or the ADMD.

2.5. Naming and Addressing

Users of the MHS are identified by O/R (Originator/Recipient) names. An O/R name comprises an O/R address, a directory name, or both.

An O/R address is a set of attributes and associated values which uniquely identifies a user for the delivery of messages. Four forms of O/R addresses are described in the F.400 Recommendations: mnemonic, terminal, numeric, and postal. The mnemonic O/R address provides a hierarchical, machine-oriented means of addressing users. The terminal O/R address identifies users with terminals belonging to various networks. The numeric O/R address identifies users with numeric keypads, and the postal O/R address identifies recipients of messages and notifications for physical delivery.

The mnemonic O/R address is the only form supported by the OIW Agreements [5]. It consists of the following standard and domain defined attributes:

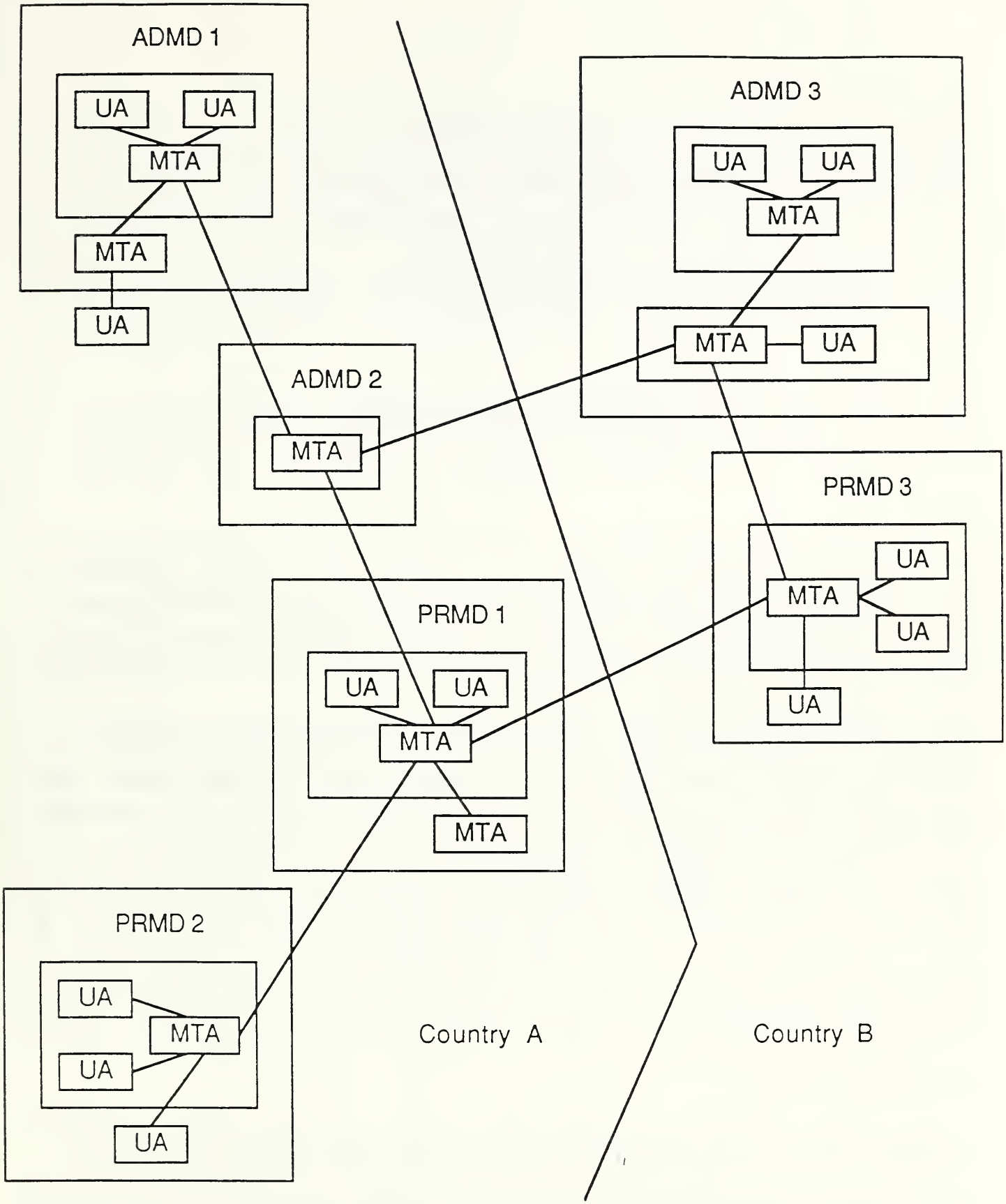

Figure 3

Management Domains

Standard Attributes
Country Name
Administration Management Domain Name
Private Management Domain Name
Organization Name
Organization Unit Name
Personal Name
Common Name

Domain Defined Attributes
Type
Value

The country name and ADMD name attributes must be present in every O/R address. The OIW Agreements allow the ADMD name to be represented by a single space (i.e., any ADMD) if, for example, an O/R address identifies a user belonging to a PRMD that uses the services of multiple ADMDs. The remaining O/R address attributes are optional, however, at least one other standard attribute must be present. Domain defined attributes are used to convey system addressing information that is external to the MHS.

An O/R name may also contain a directory name. A directory name is "looked up" in a directory to find the corresponding O/R address. The CCITT and ISO have developed a directory service standard, however, only a limited number of directory service products based on this standard are currently available. As an interim alternative, many MHS implementations provide proprietary directory service functionality.

An O/R name may reference a distribution list (DL) as well as a single user. DLs enable an originator to specify a group of recipients with a single O/R name. DLs may be nested, in that a member of a DL may be another DL. Since the specification of a DL is identical to that of a single recipient, an originator may unknowingly address a message to a DL. To prevent incurring the costs associated with the delivery of multiple messages, an originator has the option of prohibiting the MHS from expanding (i.e., splitting the message as needed for delivery to all recipients) DLs.

2.6. Directory Services

The directory defined in the X.500 series of Recommendations provides capabilities beneficial to the MHS. These capabilities can be divided into the following four categories.

(1) User-friendly naming: The originator or recipient of a message can be identified by means of a directory name, rather than a machine oriented O/R address. At any time the MHS (i.e., a UA or MTA) can obtain the latter from the former by consulting the directory.

(2) Distribution lists: A group whose membership is stored in the directory can be used as a DL. The originator simply supplies the name of the list. At the DL's expansion point the MHS can obtain the directory names (and then the O/R addresses) of the individual recipients by consulting the directory.

(3) Recipient UA capabilities: The MHS capabilities of a recipient or originator can be stored in a directory entry. At any time the MHS can obtain (and then act upon) those capabilities by consulting the directory.

(4) Authentication: Before two MHS functional entities (two MTAs, or a UA and an MTA) communicate with one another, each establishes the identity of the other. This can be done by using authentication capabilities of the MHS based on information stored in the directory.

2.7. Security

To protect against security threats, the MHS provides a variety of security services. Use of these services is optional by the MHS user. MHS security, which is based mainly on cryptographic techniques, may be used in conjunction with physical security and computer security (COMPUSEC).

MHS security services can be divided into seven classes: origin authentication, secure access management, data confidentiality, data integrity services, non-repudiation, message secure labeling, and security management services. Origin authentication pertains to the identification of peer communication partners. Secure access management protects resources from unauthorized use. Data confidentiality protects data from being disclosed. Data integrity services are used to counter active threats to the MHS. Non-repudiation provides third party proof of the submission, transfer, delivery, and receipt of messages. Message security labeling associates security labels with MHS components, and security management services provide for the registration of security labels, among other services.

Many security services require secure UAs, but not secure MTAs. For example, since MTAs neither view nor alter the content of a message, secure MTAs are not needed to provide data confidentiality. Other services, however, require secure MTAs. Non-repudiation of submission may require an MTA to generate proof of submission to a trusted third party.

3. IPMS Overview

The IPM (Interpersonal Messaging) service and corresponding P2 protocol comprise, at this time, the only standardized application for the MHS. Although many varied information types can be conveyed in the IPM service, the structure of Interpersonal Messaging facilitates its most common usage, the person-to-person transfer of brief, text messages.

Since the proposed EDI messaging standard parallels the IP messaging standard, an introduction to IP messaging is provided here. Section 3.1 presents MHS components as functional providers of the IPM service. Section 3.2 describes the IP message structure, and Section 3.3 discusses IP notifications.

3.1. Functional Model

A functional model of the IPMS is shown in Figure 4. Within the IPMS is a specific class of cooperating UAs, called IPM-UAs. IPM-UAs enable users to engage in IP messaging (i.e., originate and receive messages conforming to the P2 protocol).

To transfer an IP message, a message originator provides an IPM-UA with the message content, the O/R name of the recipient(s), and any requested services. The IPM-UA generates the IP message header (see Section 3.2), the envelope information, and submits the message to the MTS. The MTS delivers the message to the recipient's IPM-UA, which presents the message to the recipient IPM user.

The IPMS model shown in Figure 4 also contains an MS (Message Store), a TLMA (Telematic Agent), a PTLXAU (Public Telex Access Unit), and a PDAU (Physical Delivery Access Unit). The MS may be used to store and manage IP messages, and to submit and accept delivery of IP messages on behalf of the IPM-UA. The TLMA and PTLXAU are access units allowing teletex and telex users to intercommunicate with the IPM service. The PDAU allows IPM users to send messages to a postal-like service outside the IPM service.

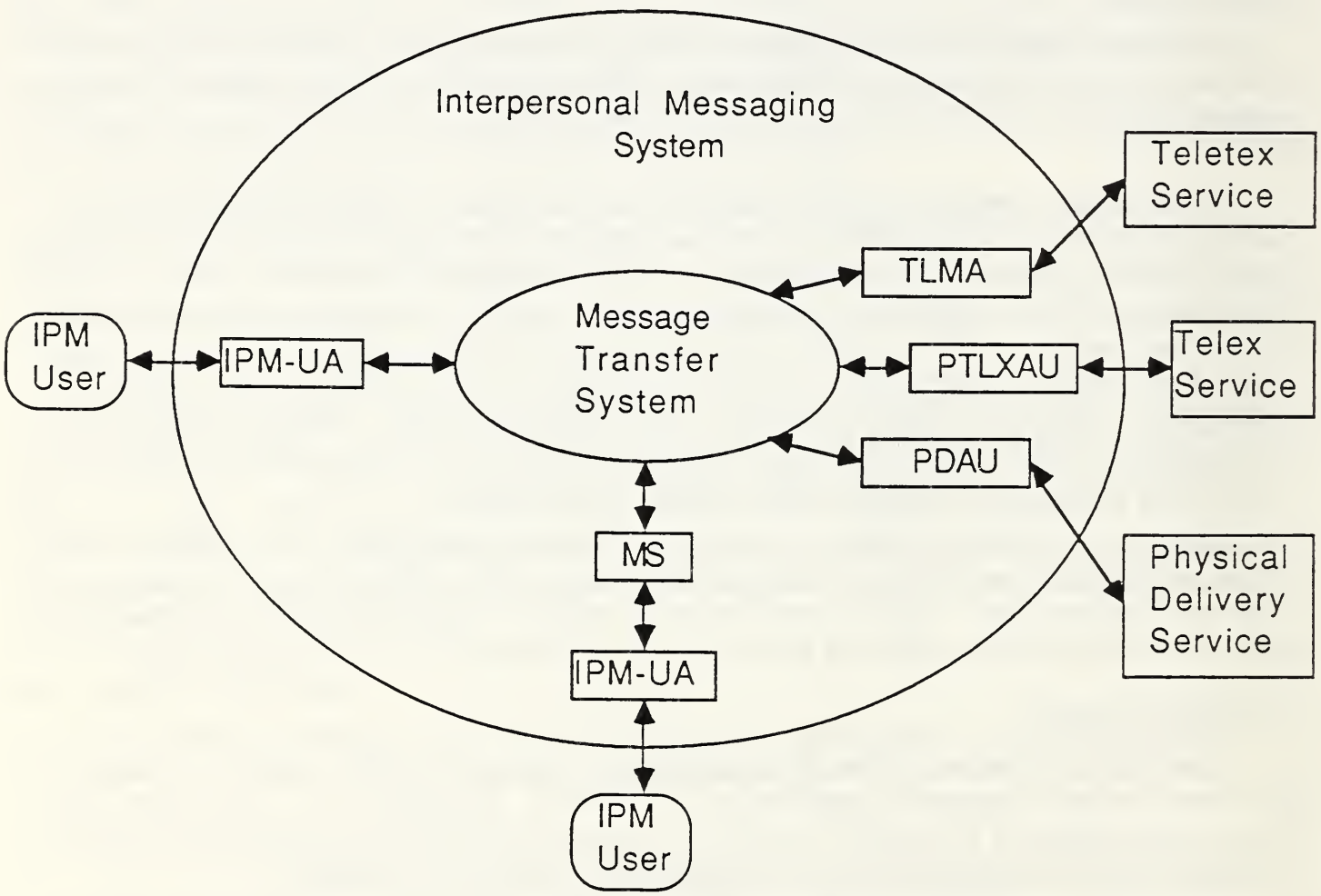

Figure 4

IPMS Functional Model

3.2. Message Structure

The structure of an IP message is shown in Figure 5. The IP message is divided into a message header and one or more message bodyparts. The message header contains a structured representation of information about the message (e.g., the message originator, primary and copy recipients, subject, expiration date, importance, message cross reference, and others). The message body can be partitioned into several bodyparts of different types such as IA5 (International Alphabet #5), G3Fax (Group 3 Facsimile), and Forwarded Interpersonal Message. When an IP message is forwarded, the header and body of the original message become one bodypart of the forwarded message.

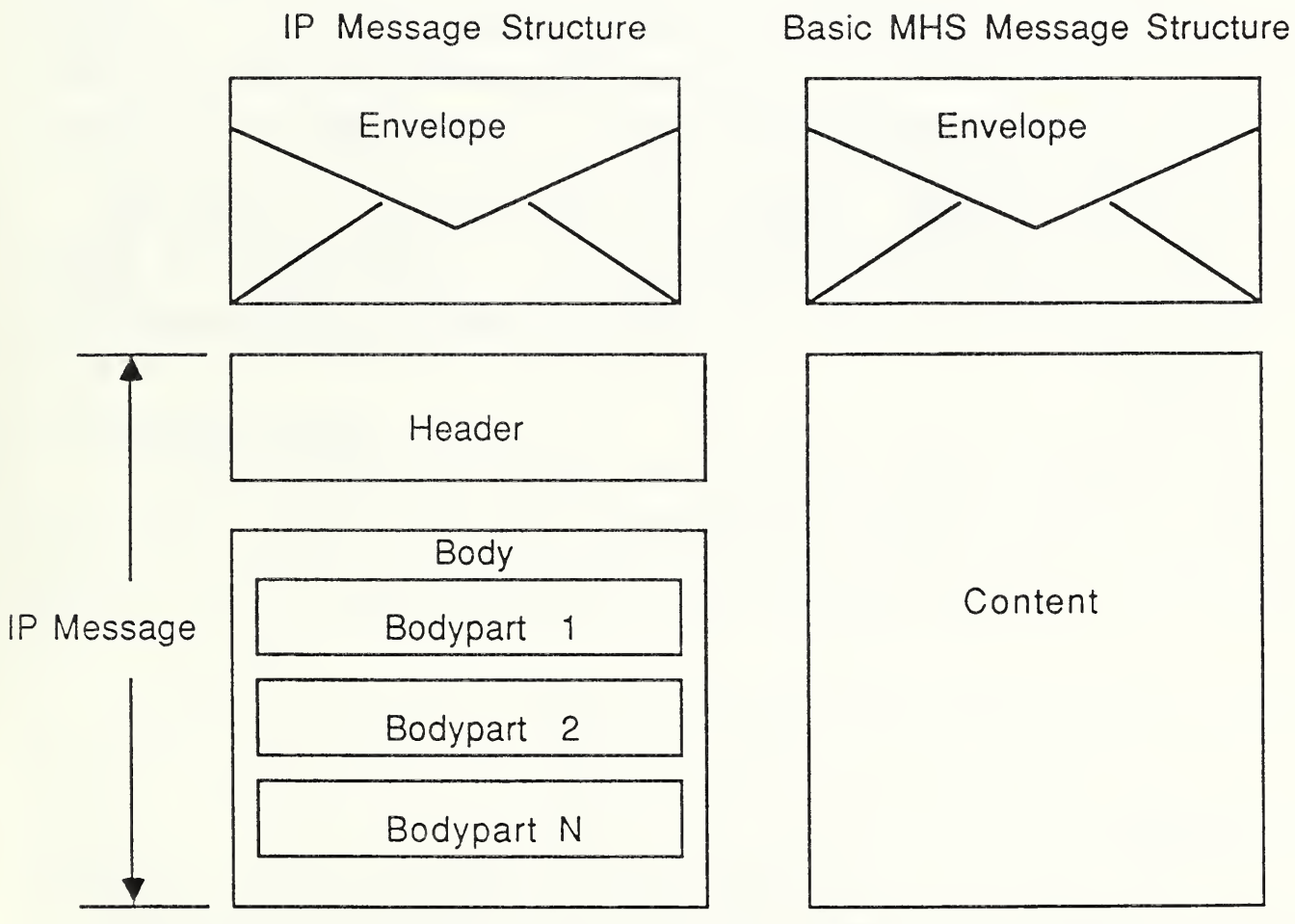

Figure 5

IP Message Structure

An IPM user may specify which bodypart types may be delivered to the IPM-UA. The MTS may convert a bodypart from one type to another, so as to make a message deliverable.

The structure of an IP message is analogous to an office memo. As shown in Figure 6, the header of the memo corresponds to the IP message header. The information conveyed in the memo (i.e., the memo body) corresponds to the body of the IP message.

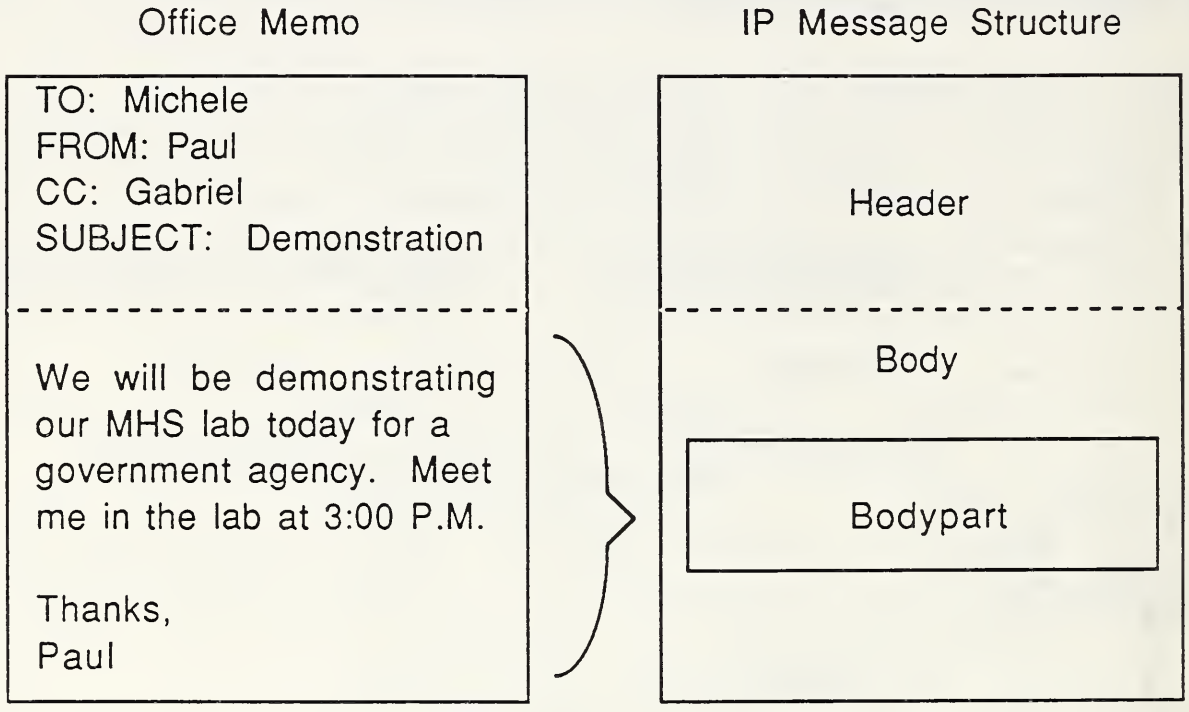

Figure 6

IP Message Structure for an Office Memo

3.3. Notifications

In the IPM service, an originator may request a notification of when a message is received by a recipient. This receipt notification is generated automatically after some recipient action, such as reading the message. Since there is no time constraint on IP notifications, an extended length of time may pass before the recipient reads the message, and a receipt notification is returned to the originator.

An originator may also request a non-receipt notification. A non-receipt notification is automatically generated if the recipient's IPM-UA auto-forwards the message to another user, or if the recipient's IPM-UA discards the message prior to receipt.

4. EDI Messaging

EDI may be defined as the computer-to-computer transfer of structured business data. This definition allows both the interactive and store-and-forward transfer of a variety of information types. EDI messaging limits EDI by providing only the store-and-forward mode of transfer, and by emphasizing X12, EDIFACT, and UN/TDI data formats. Although the X12, EDIFACT, and UN/TDI standards are emphasized, EDI messaging is structured so that any EDI interchange, including privately defined interchanges, may be conveyed by the MHS.

EDI messaging is based on the 1988 X.400 series of Recommendations. Since the IPM service is an existing MHS standard, the possibility of incorporating EDI interchanges into IP messages was investigated early in the development of EDI messaging. This proposal was rejected because the needs of EDIMG (EDI Messaging) users are different from the needs of IPM users. EDIMG users are typically computer processes that transfer large, confidential messages. IPM users are typically people who transfer short messages that are not confidential. Some functions needed by EDIMG users are not present in the IPM service, and some IPM services are irrelevant to EDI messaging users. The final solution was to create a messaging service that is equal to, but separate from, IP messaging. The EDI messaging system, protocol, and message structure are designed to parallel IP messaging counterparts.

The remainder of this section details EDI messaging. Section 4.1 presents MHS components as functional providers of the EDI messaging service. Section 4.2 describes the structure of EDI messages. Section 4.3 discusses EDIM responsibility and notifications. Section 4.4 overviews EDIM forwarding, and Sections 4.5 through 4.7 describe directory services, security and physical delivery respectively.

4.1. Functional Model

A functional model of the EDIMS (EDI messaging system) is presented in Figure 7. This model is similar to the IPMS functional model presented in Figure 4. Within the EDIMS is a specific class of cooperating UAs, called EDI-UAs. EDI-UAs enable users to engage in EDI messaging (i.e., originate and receive messages conforming to the EDI messaging protocol, Pedi).

To transfer an EDIM (EDI message) an originating EDI messaging user provides an EDI interchange, and, optionally, other information associated with the interchange to an EDI-UA. The EDI-UA generates the EDIM header (see Section 4.2) and envelope information (e.g., recipient O/R names) from data contained in the interchange. The resulting EDI message is submitted to the MTS. The MTS delivers the message to the recipient's EDI-UA, which presents the message to the recipient EDI messaging user.

EDI-UAs provide a simple, easily defined interface between an EDI application and the MHS. Since EDI-UAs parse the interchange to extract required information, EDI applications should only require minimal modification to convey interchanges via the MHS.

The EDIMS model shown in Figure 7 also contains an EDI-MS and a PDAU. The EDI-MS may be used to store and manage EDIMs, and to submit and accept delivery of EDIMs on behalf of the EDI-UA. The PDAU allows EDI messaging users to send messages to a postal like service outside the EDIMS. No other EDI-AU is currently defined for EDI messaging.

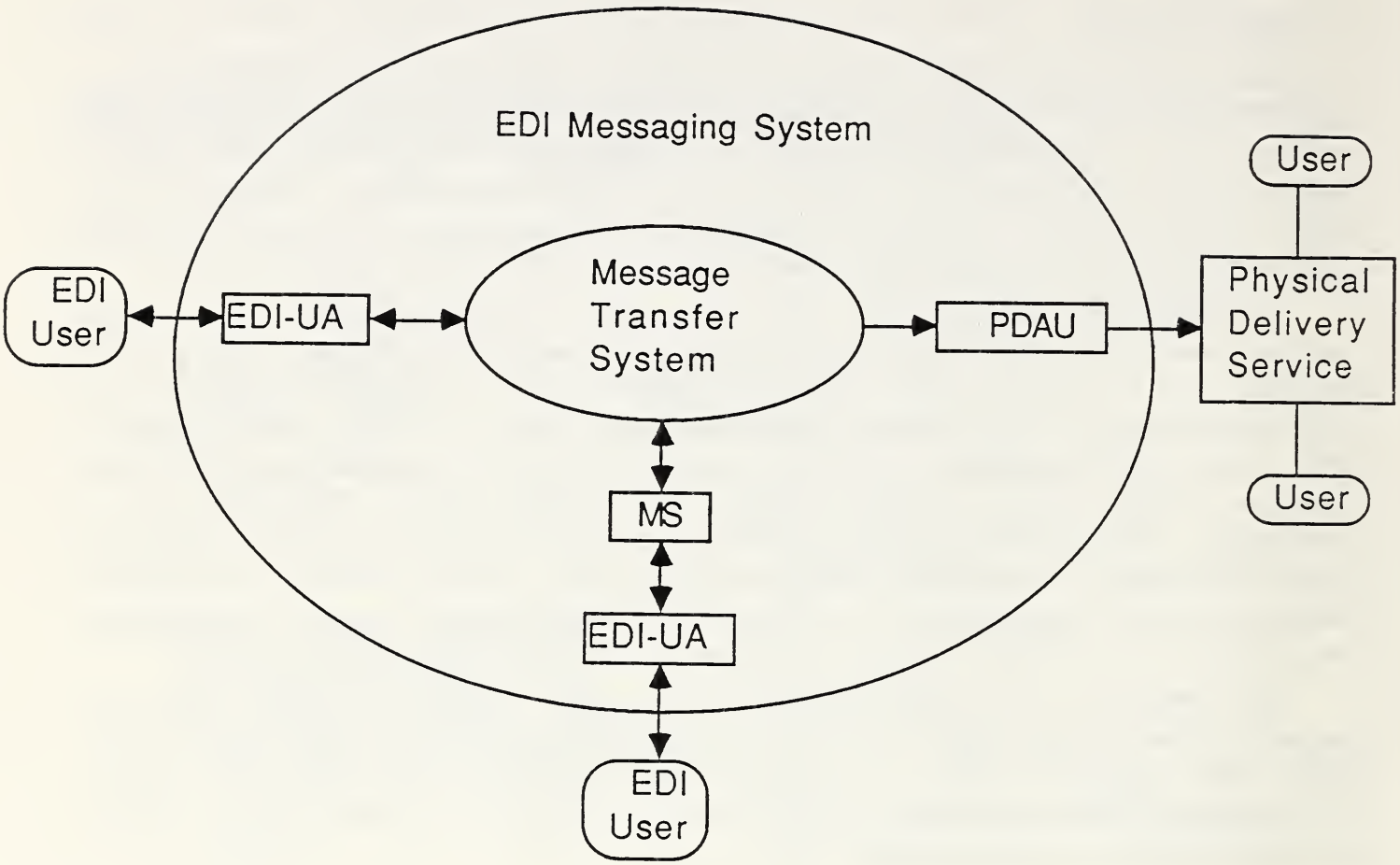

Figure 7

EDIMS Functional Model

4.2. Message Structure

The structure of an EDIM (EDI message) is shown in Figure 8. The EDIM is divided into a message header and one or more message bodyparts. One bodypart comprising an EDI interchange must be present when the message is first submitted to the MHS. That is, an EDIM can contain at most one EDI interchange. Other bodyparts are optional and are used to transmit information relating to the interchange, such as drawings and explanatory text. Additional bodyparts can contain any type of data (e.g., IA5) except they cannot be or contain EDI interchanges.

The other EDI message component is the message header. The header contains a structured representation of information about the message. It comprises mappings from the

interchange bodypart and various service data. Examples of service data include the EDI message types contained in the message (e.g., invoices, purchase orders), the bodypart type (e.g., EDIFACT), the date and time the originator expects the message to lose its validity, cross referencing information between bodyparts contained in the message and in other EDI messages, any EDI messages made obsolete by the message, any related messages (EDI messages, IP messages, or others), and various security services.

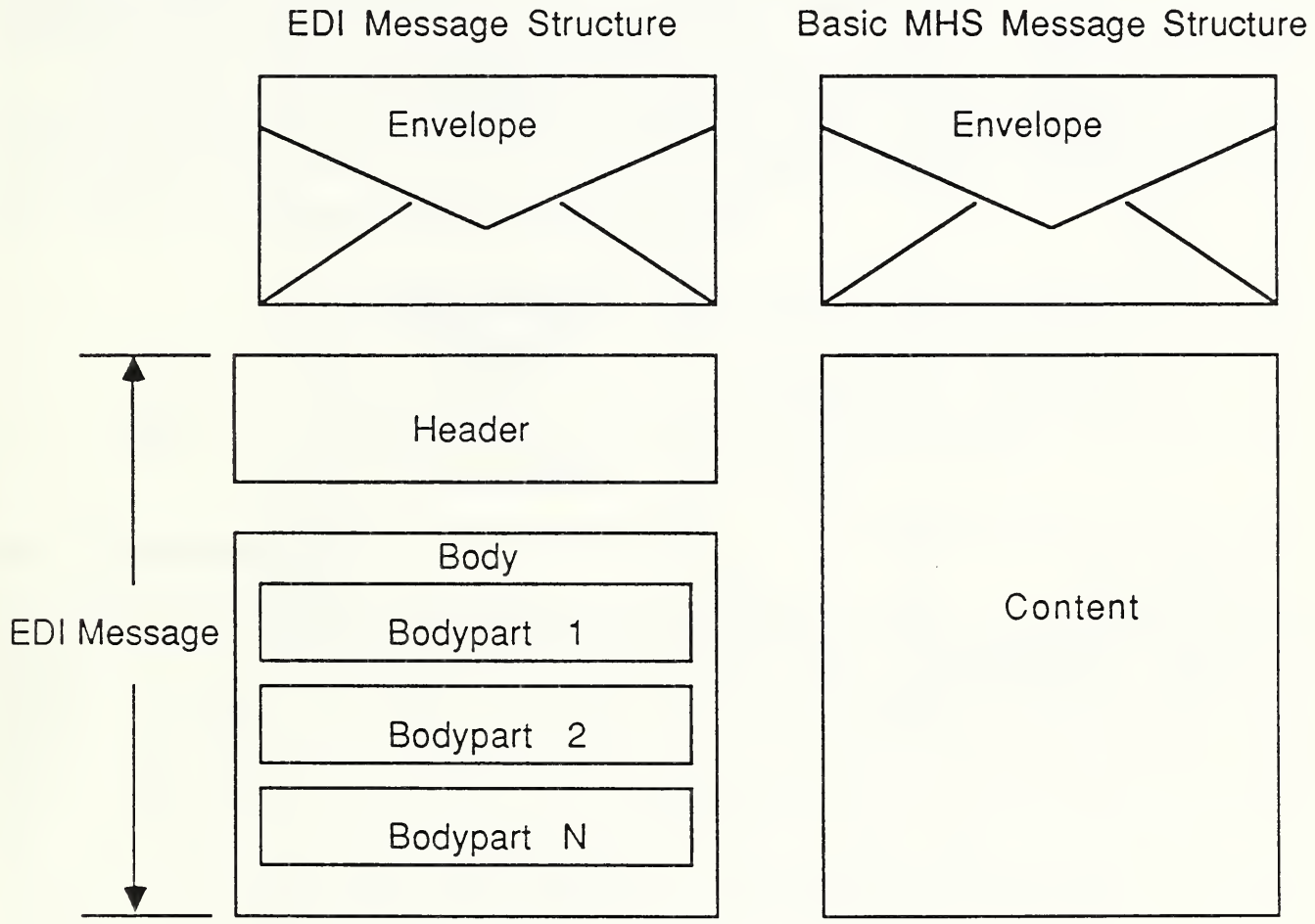

Figure 8

EDI Message Structure

The relationship between an EDIFACT interchange and an EDI message is shown in Figure 9. The entire interchange is mapped into one bodypart. Some information in the interchange headers is also mapped into the message header. Although Figure 9 relates an EDIFACT interchange to an EDI message, X12, UN/TDI, and privately defined interchanges can

be similarly mapped.

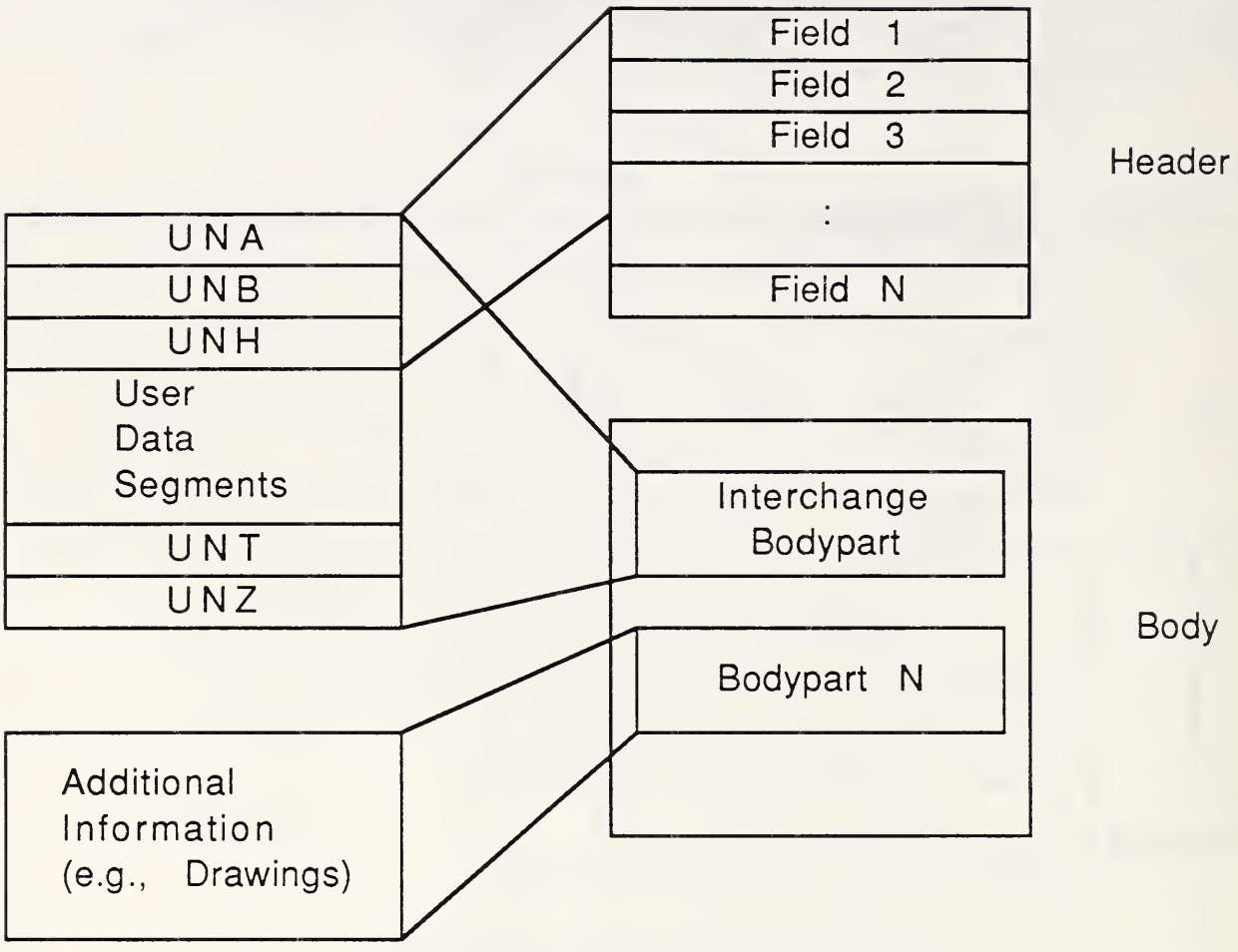

Figure 9

EDI Message Structure for EDIFACT Message

4.3. EDIM Responsibility and Notifications

EDIM responsibility provides a means for tracing the paths of EDI messages among EDI-UAs. It indicates whether an EDI message is made available to an EDI messaging user. When an EDI message is received, an EDI-UA must accept, refuse or forward EDIM responsibility. Knowledge of this decision may be vital to an originator.

To inform an originator of a recipient's decision regarding EDIM responsibility, an EDIN (EDI Notification) is returned. The EDIN conveys one of three values: PN (Positive Notification), NN (Negative Notification), or FN (Forwarded Notification). An EDI-UA generates a PN if EDIM responsibility is accepted (i.e., the message is made available to the

recipient EDI messaging user), an NN if it is refused (i.e., the message will not be made available to the recipient EDI messaging user), and an FN if it is forwarded (i.e., the message, along with EDIM responsibility, has been forwarded to another EDI-UA). The decision regarding EDIM responsibility may be made by the EDI-UA automatically, or after receiving external stimuli from the user. A field in the EDIN allows the EDI-UA to specify who authorized the notification.

An originator may request any combination of PN, NN, and FN (or none at all) from any message recipient. Although notification is typically returned to the originator, the originator may specify an alternate receiver for the EDIN.

The delivery of notifications in EDI messaging is considered more urgent than in the basic MT service, due to the business-oriented content of the subject messages. This urgency is reflected in the EDIN delivery time targets documented in F.435. The EDIN time targets are based on the subject message's grade of delivery.

Grade of Delivery	95% Delivered Before
Urgent	15 minutes
Normal	60 minutes
Non-Urgent	4 hours

4.4. EDIM Forwarding

EDIM forwarding is the transferring of a message received by an EDI-UA to one or more EDI-UAs. EDIM responsibility may be accepted prior to forwarding a message, or may be forwarded with the message. A message may not be forwarded if EDIM responsibility is refused. If EDIM responsibility is forwarded, the EDI-UA receiving the forwarded message has the same obligations as did the forwarding EDI-UA, which is to accept, refuse, or forward EDIM responsibility. If notification is requested for the message, the recipient's EDI-UA must also return to the originator the appropriate EDIN. Since there is no constraint on the number of times EDIM responsibility may be forwarded, multiple FNs and a PN may be generated for a single EDI message that is forwarded several times before EDIM responsibility is accepted. The originator has the option of prohibiting EDIM responsibility from being forwarded.

The need for forwarding can be exemplified by a large organization employing a centralized EDI-UA. This EDI-UA would receive all messages entering the organization, perform various functions such as logging and auditing, then forward the messages to different EDI-UAs within the organization.

An EDI-UA may forward one message to multiple recipients, optionally adding and removing bodyparts in the process. If, for example, the centralized EDI-UA described above receives a message with two bodyparts, one interchange bodypart and one additional bodypart containing a drawing, the EDI-UA may forward the drawing bodypart to one EDI-UA, and forward the interchange bodypart to a different EDI-UA.

To forward a message to multiple recipients, the forwarding EDI-UA creates a new EDI message with a new header for each recipient. The header, body, and, optionally, the

envelope of the original message become one bodypart in the forwarded message (see Figure 10). Bodyparts may be added and/or removed from the forwarded message. If a bodypart is removed, a place holder is inserted indicating the type of bodypart removed. In the above example, the forwarding EDI-UA would create two EDI messages. One message would contain a forwarded interchange bodypart and a place holder identifying a removed additional bodypart. The second message would contain a forwarded additional bodypart (i.e., the drawing) and a place holder identifying a removed interchange bodypart. The structure of these forwarded EDI messages is shown in Figure 11.

Several restrictions apply to the adding and removing of bodyparts. EDIM responsibility must be accepted before bodyparts can be added or removed. A bodypart must be removed in its entirety; portions of bodyparts may not be removed nor may the content of bodyparts be modified. Also, an EDIM header may never be removed from a message. Since a forwarded bodypart contains an EDIM header (see Figure 10), forwarded bodyparts may never be removed.

If a forwarding EDI-UA does not add or remove bodyparts, the EDI-UA may forward EDIM responsibility along with the message. Although a message may be forwarded to multiple recipients, EDIM responsibility may only be forwarded to one of the recipients.

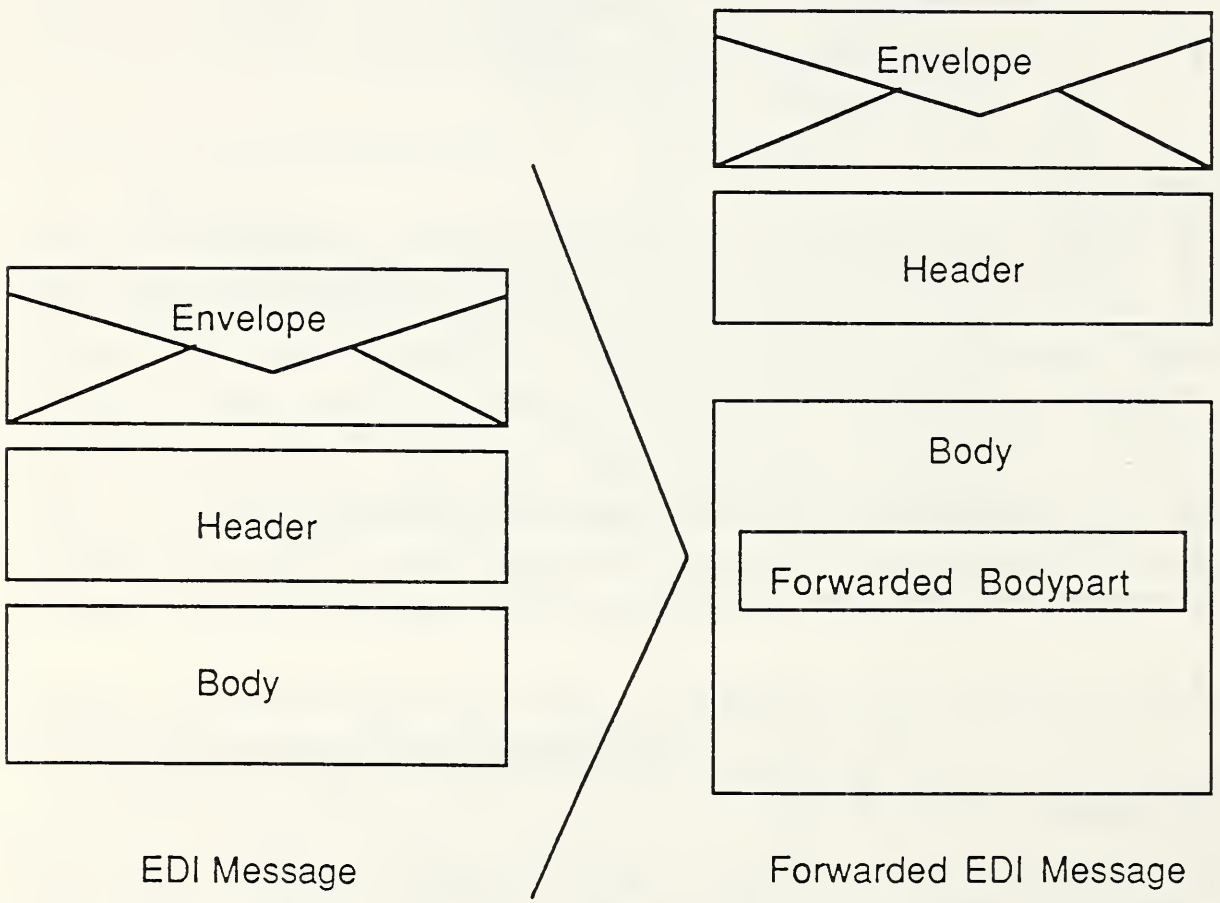

Figure 10

Forwarded EDIM Structure

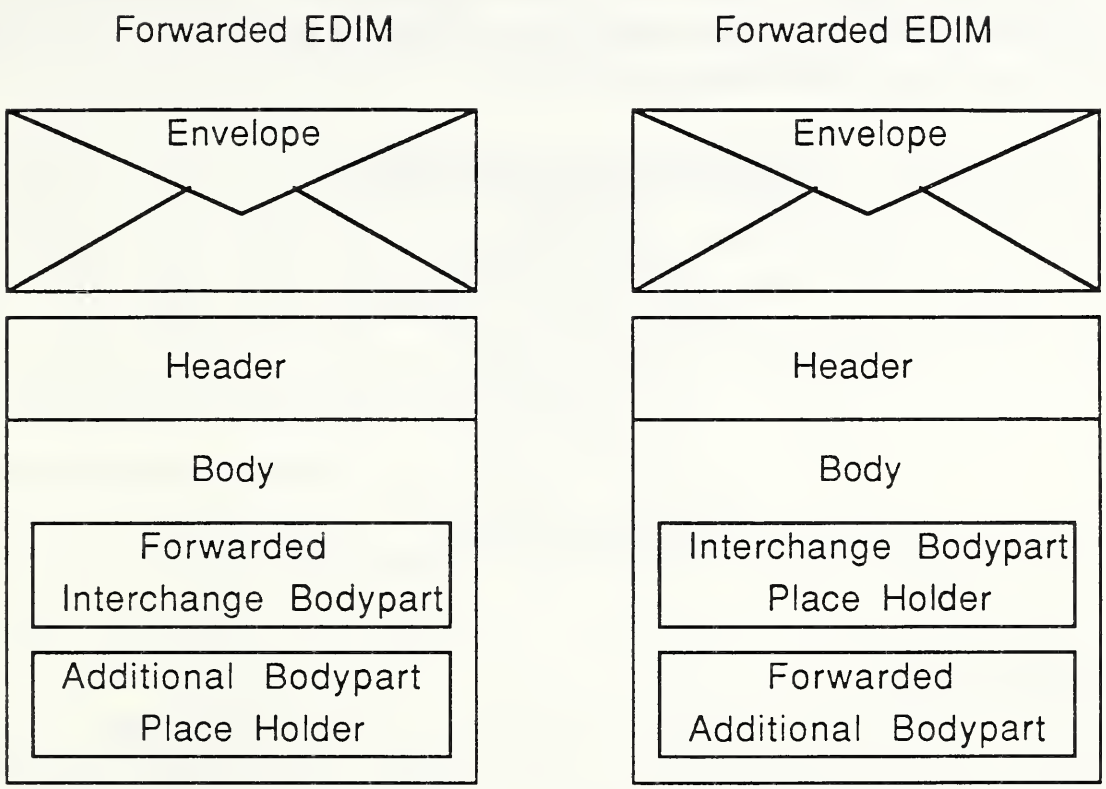

Figure 11

Example of Removed EDIM Bodyparts

4.5. Directory Services

The Directory defined in the X.500 series of Recommendations provides capabilities beneficial to EDI messaging. Two major EDI messaging functions are provided by the Directory: name resolution and capabilities assessment. If the Directory is not available, these functions may be performed as a local matter.

EDI users use unique alphanumeric names to identify each other. The names may be globally unique, or simply unique within a particular EDI trading community. It is considered vital for EDI applications to use existing naming practices. Since EDI messaging users are identified by O/R addresses, an EDI-UA can use the Directory to obtain a recipient's O/R address based on the alphanumeric name provided by the message originator. This process is

called name resolution.

The Directory may also be used to assess the capabilities of an EDI messaging user. A variety of capabilities used in EDI messaging may be stored in the Directory. The following EDI capabilities are listed in Recommendation F.435.

EDI Capabilities in Directory
standard
standard version
standard syntax identifier
document type
document version
document release
controlling agency
association assigned code
EDI character set

4.6. Security Services

The MHS security services described in Section 2.7 of this paper, being of a generic message handling nature, are applicable to EDI messaging. For example, the identity of EDI-UAs can be associated with Message Security Labels. Using these labels, MHS security services requiring UA validation (e.g., MHS origin authentication services) may be performed. In addition, the integrity and confidentiality of data, which are extremely important in the context of EDI, may be provided using the MHS data integrity and data confidentiality services.

Services beyond those provided by the MHS are needed to protect against specific vulnerabilities of the EDIMS, such as manipulation of information by EDI messaging users. To counter these vulnerabilities, the following EDI messaging security capabilities are provided: proof and non-repudiation of EDIN, proof and non-repudiation of content received, and proof of content originated. EDI-UAs are responsible for the provision of these additional security services.

Proof and Non-repudiation of EDIN are used to confirm the receipt of an EDI message by a recipient's EDI-UA. Non-repudiation of EDIN is the stronger of the two services protecting against any attempt by the recipient's EDI-UA to falsely deny sending the EDIN. These services may be provided by transmitting, as part of the notification, the Message Security Label associated with the recipient's EDI-UA.

Proof and Non-repudiation of Content Received are used to confirm that the message content received by a recipient's EDI-UA was the same as the message content originated. Non-repudiation of Content Received is the stronger of the two services protecting against any attempt by the recipient's EDI-UA to falsely deny receiving the content of the EDI message. A recipient's EDI-UA may provide these services by returning the complete original message content in the EDI notification. Non-repudiation of Content Received may also be provided by means of a bilaterally agreed notarization mechanism, or by using asymmetric encryption techniques.

Non-repudiation of Content Originated is used to confirm the originated message content to a recipient's EDI-UA. This service protects the recipient's EDI-UA from any attempt by the originator to falsely deny originating the message content. This service may be provided by sending asymmetric cryptographic keys in the message content, or by use of a bilaterally agreed notarization mechanism.

In addition to the above security capabilities, some pervasive security mechanisms may be provided for EDI messaging as a local matter. These pervasive mechanisms include Secure EDI-MS Audit Trail, Secure MT Audit Trail, EDI-MS Archive, and MT Archive. The Secure MS Audit Trail facility would monitor and record EDI-UA actions on the EDI-MS. The Secure MT Audit Trail facility would monitor and record all MTA actions. The EDI-MS Archive facility would provide recovery from EDI-MS failure, and the MT Archive facility would provide recovery from MTA failure.

4.7. Physical Delivery Service

One service provided by the EDIMS is the delivery of EDIMs to a PD (Physical Delivery) system. When submitting a message destined for physical delivery, the originating EDI-UA provides the postal O/R address of the recipient. The postal O/R address may be obtained from a directory. The MTS delivers the message to the recipient's PDAU (Physical Delivery Access Unit), which, acting as a gateway, transfers the message to the PD system.

PDAUs represent a special case with the generation of EDINs. If notification is requested by the originator and an EDIM can be rendered for physical delivery, an FN is generated. A PDAU may never return a PN. If the message cannot be rendered for physical delivery, an NN is generated by the PDAU.

PDAUs provide uni-directional communication with PD systems. The origination of messages and notifications from a PD system is currently beyond the scope of EDI messaging.

5. Conclusion

The MHS enables an established global network for the effective and reliable transfer of messages. Use of the MHS has been stimulated in the U.S. by GOSIP [3], which mandates that federal agencies use MHS products to transfer electronic messages. The benefits of exchanging EDI data via the MHS have become apparent, and several methods exist today which utilize the MHS for EDI transmissions. The problem with existing methods is that they lack international acceptance.

The CCITT has recently developed a proposed EDI messaging standard which will replace existing methodologies. EDI messaging is specified in two CCITT draft Recommendations: X.435, EDI Messaging System, and F.435, EDI Messaging Service. Together, the Recommendations define the technical aspects and services provided by EDI messaging as an MHS application. Other issues, such as security, directory services, and physical delivery are also explicated in the Recommendations.

One topic that was not completed for inclusion in the Recommendations is EDI charging. EDI charging services would allow reverse charging and split charging for both EDI messages and notifications. This issue must be presented to the CCITT Study Group III (accounting) for resolution. The EDI charging issue also illuminated the need to distinguish messages from notifications within the MTS, so that appropriate billing can occur. This matter will be

addressed by the CCITT Question 18/Study Group VII.

The two draft Recommendations are currently in the possession of the CCITT Secretariat, where they are being translated into Spanish and French. Publication is expected in mid 1991. EDI messaging implementations may be available in the beginning of 1992.

Some vendors may opt to release their first EDI messaging products based on the 1984 X.400 Recommendations. Although EDI messaging uses the 1988 X.400 Recommendations as a base standard, downgrading rules are specified in X.435 so that MTAs conforming to the 1984 Recommendations can submit, relay, and receive EDI messages. EDI messaging implementations conforming to the 1984 Recommendations will not offer 1988 X.400 services, such as MHS security.

As with the MHS, the use of EDI messaging will be spurred by GOSIP. EDI messaging is a planned addition to the GOSIP requirements, and is scheduled to be included in Version 3 of GOSIP, if EDI messaging products are available in 1992. Also, FIPS (Federal Information Processing Standard) 161 [4], released by the National Institute of Standards and Technology, mandates the use of GOSIP compliant protocols for transmitting EDI data via telecommunications.

With the draft Recommendations completed, future work on EDI messaging will be conducted by the CCITT Question 18/Study Group VII. Implementation agreements for EDI messaging will be developed by the MHS special interest group of the OIW.

REFERENCES

(1) CCITT 1988 F.400, Series of Recommendations.

(2) CCITT 1988 X.400, Series of Recommendations.

(3) Government Open Systems Interconnection Profile (GOSIP), Version 2. FIPS 146-1.

(4) Electronic Data Interchange (EDI). FIPS 161.

(5) Stable Implementation Agreements for Open Systems Interconnection Protocols Version 3 December 1989. NIST Special Publication 500-177.

BIBLIOGRAPHY

(1) Blum, Daniel, "Getting the Message", Network World, February 19, 1990.

(2) Brown, Patricia, "CCITT Subcommittee Nears Completion of EDI-to-X.400 Standard", OSI Product & Equipment News, Volume 3, Number 9, April 26, 1990.

(3) "EDI's Role in a Strategy for Digital Data Interchange", An Evaluation Report Submitted to OASD/CALS Policy Office and the MAP/TOP Steering Committee, November 26, 1989.

(4) Genilloud, Guy, "X.400 MHS: First Steps Towards an EDI Communication Standard", Computer Communication Review, Volume 20, Number 2, April 1990.

APPENDIX A: Abbreviations

This appendix provides a list of abbreviations used in this paper.

ADMD	Administration Management Domain
ANSI	American National Standards Institute
AU	Access Unit
CCITT	Consultative Committee on International Telephony and Telegraphy
CEC	Commission of European Communities
CONS	Connection Oriented Network Service
CLNS	Connectionless Network Layer Service
DL	Distribution List
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EDIM	Electronic Data Interchange Message
EDIMG	Electronic Data Interchange Messaging
EDIMS	Electronic Data Interchange Messaging System
EDIN	Electronic Data Interchange Notification
FIPS	Federal Information Processing Standard
FN	Forwarded Notification
GOSIP	Government Open Systems Interconnection Profile
G3Fax	Group 3 Facsimile
IA5	International Alphabet No. 5
IP	Interpersonal
IPM	Interpersonal Messaging
IPMS	Interpersonal Messaging System
MHS	Message Handling System
MS	Message Store
MT	Message Transfer
MTA	Message Transfer Agent
MTS	Message Transfer System
NN	Negative Notification
OIW	Open Systems Interconnection Implementor's Workshop
O/R	Originator/Recipient
OSI	Open Systems Interconnection
PD	Physical Delivery
PDAU	Physical Delivery Access Unit
PN	Positive Notification
PRMD	Private Management Domain
PTLXAU	Public Telex Access Unit
PTT	Postal Telephone and Telegraph
TLMA	Telematic Agent
UA	User Agent
UN/ECE	United Nations/Economic Commission for Europe
UN/TDI	United Nations/Trade Data Interchange

APPENDIX B: Glossary

This appendix provides a glossary of MHS terms that may apply to EDI messaging. The explanations provided are not necessarily definitions in the strict sense.

Access Unit – An MHS component that links another communication system (e.g., a physical delivery system) to the MTS and via which its patrons engage in message handling as indirect users.

Actual Recipient – A potential recipient for which delivery takes place.

Administration Domain Name – A standard attribute of an O/R address form that identifies an ADMD relative to the country denoted by the country name.

Administration Management Domain – A management domain managed by an Administration.

Alternate Recipient – A user or distribution list to which the originator can (but need not) request that a message or probe be conveyed if and only if it cannot be conveyed to a particular preferred recipient.

Attribute – An information item, a component of an attribute list, that describes a user or distribution list, and that can also locate it in relation to a physical or organizational structure of the MHS (or the network underlying it).

Attribute List – An ordered set of attributes that constitutes an O/R address.

Attribute Type – An identifier that denotes a class of information (e.g., personal names). It is a part of an attribute.

Attribute Value – An instance of a class of information an attribute type denotes (e.g., a particular personal name). It is a part of an attribute.

Base Service – The sum of features inherent in a service.

Body – A component of a message. Other components are the heading and the envelope.

Body Part – A component of the body of a message.

Common Name – A standard attribute of an O/R address form that identifies a user or distribution list relative to the entity denoted by another attribute (e.g., organizational name).

Content – The piece of information that the originating UA wishes delivered to the recipient UA.

Content Type – An identifier on a message envelope that identifies the type (i.e., syntax and

semantics) of the message content.

Conversion – A transmittal event in which an MTA transforms parts of a message's content from one encoded information type to another, or alters a probe so it appears that the described messages were so modified.

Cooperating User Agent – A UA that cooperates with another recipient's UA in order to facilitate the communication between the originator and recipient.

Country Name – A standard attribute of an O/R address form that identifies a country.

Delivery – The interaction by which the Message Transfer Agent transfers to a recipient User Agent the content of a message plus the delivery envelope.

Delivery Notification – An information object that acknowledges delivery or non-delivery of a message or probe.

Direct Submission – A transmittal step in which the originator's UA or MS conveys a message or probe to an MTA.

Direct User – A user that engages in message handling by direct use of the MTS.

Directory – A collection of open systems cooperating to provide directory services.

Directory Name – The name of an entry in a directory.

Distribution List – A component of the Message Handling Environment that represents a pre-specified group of users and other distribution lists and that is a potential destination for the information objects an MHS conveys.

Distribution List Expansion – A transmittal event in which an MTA resolves a distribution list, among a message's immediate recipients, to its members.

Distribution List Name – An O/R name allocated to represent a collection of O/R addresses and directory names.

Domain Defined Attribute – An attributed used to convey non-standard information.

EDI Application – A computer process that creates and/or processes EDI messages.

EDI Interchange – Communication between two partners in the form of a structured set of messages and service segments starting with an interchange control header and ending with an interchange control trailer. In the context of EDI messaging, the contents of the primary bodypart of an EDI message.

EDI Message – The specific content that is sent from one EDI-UA to another.

EDI Messaging – EDI messaging consists of the exchange and associated procedures of EDI messages and EDI notifications.

EDI Messaging Service – A service that provides an EDI messaging user with features to assist in communicating with other EDI messaging users.

EDI Messaging Environment – The environment in which EDI messaging takes place comprising the EDI messaging system and EDI messaging users.

EDI Messaging System – The functional object by means of which users communicate with one another in EDI messaging, comprising the Message Transfer Service, EDI user agents, EDI message stores, and EDI access units.

EDI Messaging User – A user that engages in EDI messaging.

EDI Notification – An information object that indicates to the originator of an EDI message the disposition of EDIM responsibility for the EDI message.

EDIM Responsibility – An indication of whether an EDI message has been made available to a specific user by its EDI user agent/message store.

EDI User – An information object not necessarily belonging to the EDI messaging environment. In the context of message handling the EDI user is largely identical with an EDI messaging user.

EDI User Agent – An MHS component by means of which a single EDIMG user engages in EDI messaging.

Electronic Data Interchange – The computer-to-computer exchange of structured business data, such as invoices and purchase orders.

Encoded Information Type – An identifier of the medium and format (e.g., IA5 text) of information represented by an individual portion of the content.

Envelope – A place in which the information to be used in the submission, delivery and relaying of a message is contained.

Heading – Component of a message. Other components are envelope and body.

Indirect Submission – A transmittal step in which an AU conveys a message or probe originated outside the MHS to an MTA.

Indirect User – A user that engages in message handling by indirect use of the MHS, i.e.,

though another communication system (e.g., a physical delivery system) to which the MHS is linked.

Intercommunication – A relationship between services where one of the services is a message handling service, enabling the users of the message handling service to communicate with users of other services.

Interpersonal Messaging – Communication between persons by exchanging messages.

Interpersonal Messaging Service – Messaging service between users based on the Message Transfer Service.

IP-message – The content of a message in the IPM service.

Management Domain – The set of MHS entities managed by an Administration or organization that includes at least one MTA.

Message – In the context of Message Handling Systems, the unit of information transferred by the MTS. It consists of an envelope and a content.

Message Handling Environment – The environment in which message handling takes place, comprising the MHS, users, and distribution lists.

Message Handling Service – Service provided by the Message Handling Systems.

Message Handling System – A component of the Message Handling Environment that conveys information objects from one party to another.

Message Store – A component of the MHS that provides a single direct user with capabilities for message storage.

Message Transfer Agent – The component of the MHS that actually conveys information objects to users and distribution lists.

Message Transfer Service – Service that deals with the submission, transfer, and delivery of messages for other messaging services.

Message Transfer System – A component of the MHS that provides transfer between message transfer agents.

Open Systems Interconnection – A term referring to the capability of interconnecting different systems.

Mnemonic O/R Address – An O/R address that mnemonicly identifies a user or distribution list relative to the ADMD through which the user is accessed or the distribution list is

expanded.

Non-delivery – A transmittal event in which an MTA determines that the MTS cannot deliver a message or probe to one or more of its immediate recipients.

Numeric O/R Address – An O/R address that identifies a user of Message Handling Services by means of a numeric keypad.

O/R Address – An attribute list that distinguishes one user or distribution list from another and identifies the user's point of attachment to the MHS or the distribution list's point of expansion.

O/R Name – An information object by which a user can be designated as an originator, or a user or distribution list can be designated as a potential recipient of a message or probe.

Organization Name – A standard attribute of an O/R address which uniquely designates an organization for the purpose of sending and receiving messages.

Organization Unit – A standard attribute of an O/R address which uniquely designates an organizational unit for the purpose of sending and receiving messages.

Originator – A user, a person or computer process, that is the ultimate source of a message or probe.

Personal Name – A standard attribute of an O/R address that identifies a person relative to the entity denoted by another attribute (e.g., organization name). Components of a personal name are: surname, given name, initials, and generation qualifier.

Physical Delivery – The delivery of a message in physical form (e.g., a letter) through a physical delivery system.

Physical Delivery Access Unit – An access unit that subjects messages to physical rendition.

Physical Delivery Service – Service provided by a physical delivery system.

Physical Delivery System – A system that performs physical delivery (e.g., the postal system).

Physical Rendition – The transformation of an MHS message to a physical message, e.g., by printing the message on paper and enclosing it in a paper envelope.

Postal O/R Address – An O/R address that specifies the geographic area used for routing messages.

Potential Recipient – Any user or distribution list to which a message or probe is conveyed

during the course of transmittal.

Private Domain Name – A standard attribute of an O/R address which uniquely designates a private management domain for the purpose of sending and receiving messages.

Private Management Domain – A management domain managed by a company or non-commercial organization.

Probe – An information object that describes a class of messages that is used to determine the deliverability of such messages.

Recipient – A user, a person or computer process, who receives a message from the MHS.

Relaying – The interaction by which one Message Transfer Agent transfers a message to another Message Transfer Agent.

Report – An information object generated by the MTS reporting the transmittal status of a message or probe to one or more potential recipients.

Retrieval – A transmittal step in which a user's MS conveys a message or report to the user's UA.

Security Capabilities – The mechanisms that protect against various security threats.

Standard Attribute – An attribute whose type is bound to a certain class of information.

Subject Message – The message that is the subject of a report.

Terminal O/R Address – An O/R address that identifies a user by means of the network address of a terminal.

Transfer – A transmittal step in which one MTA conveys a message, probe, or report to another.

Transmittal – The conveyance of a message from its originator to its potential recipients or a probe from its originator to the MTAs serving the potential recipients.

User – A person or computer application or process who makes use of MHS.

User Agent – An MHS component by means of which a single direct user engages in message handling.

APPENDIX C: EDI Messaging Elements of Service

EDI messaging elements of service are features available to EDI messaging users. This appendix provides a brief description of these features. It should be noted that message transfer elements of service used in EDI messaging are not listed here. For a listing of message transfer elements of service, a user should refer to the CCITT F.400 Recommendation.

The Application Security Element allows the originator and the recipient to indicate in the heading of the EDIM, application security information in order to support end-to-end security services.

The Character Set element of service allows the originator to indicate in the heading of an EDIM, the character set used in the EDI body of the message.

The Cross Reference Information element of service allows the originator to indicate in the heading of an EDIM, information that can be used for cross referencing between application specific reference IDs within an EDI interchange and bodyparts of this or other EDIMs.

The EDI Forwarding element of service enables an EDI-UA to forward a received EDIM with or without changes, and an EDI-MS to forward a received EDIM without changes.

The EDI Message Type(s) element of service allows the originator to indicate in the heading of an EDIM, the type(s) of EDI messages contained in the EDI interchange (e.g. invoices, purchase orders, etc.).

The EDI Notification request element of service allows the originating EDI- UA to request that it be notified of a recipient's acceptance, refusal, or forwarding of EDIM responsibility, in any combination, for the message carrying this request. The originating EDI-UA conveys this request to the recipient EDI-UA/MS or AU.

The EDI Standard Indication element of service enables the originating EDI-UA to indicate in the heading of an EDIM, the type of EDI standard that is contained in this EDIM (e.g., X12).

The EDIM Identification element of service enables cooperating EDI-UAs to convey a globally unique identifier for each EDIM sent or received. EDI-UAs and EDIMG users use this identifier to refer to a previously sent or received EDIM (for example, in EDINs).

The EDIM Responsibility Forwarding Allowed Indication element of service allows an originating EDI-UA to indicate that the EDIM responsibility for this EDIM may be forwarded by the recipient EDI-UA.

The EDIN Receiver element of service allows the originator, or a forwarding EDI-UA/MS, to indicate to a recipient the O/R address to which requested notifications should be returned.

The Expiry Date/Time Indication element of service allows the originator to indicate to the recipient the date and time after which the originator considers the EDIM to be invalid. This element of service is used to convey the intent of the originator; the action taken by the recipient is a local matter.

The Incomplete Copy Indication element of service allows a forwarding EDI-UA to indicate that the forwarded EDIM is an incomplete copy of an EDIM with the same EDIM identifier in that one or more bodyparts of the original EDIM are absent.

The Interchange Header element of service enables the originating EDI-UA to place data elements of the EDI interchange headers in corresponding fields in the EDIM.

The Multi-part Body element of service allows an originator to send a recipient an EDIM with a body that is comprised of several parts. The type of each bodypart is conveyed along with the bodypart.

The Non-repudiation of Content Originated element of service enables an originating EDI-UA to provide a recipient EDI-UA with an irrevocable proof as to the authenticity and integrity of the content of the message as it was submitted into the message handling environment.

The Non-repudiation of Content Received element of service enables an originating EDI-UA to get from a recipient EDI-UA irrevocable proof that the original subject message content was received by the recipient EDI-UA and EDIM responsibility was accepted, forwarded, or refused. This service provides irrevocable proof as to the integrity of the content received and irrevocable proof as to the authenticity of the recipient of the message. It will protect against any attempt by the recipient(s) to subsequently deny having received the message content.

The Non-repudiation of Content Received Request element of service enables an originating EDI-UA to request the recipient EDI-UA to provide it with an irrevocable proof of the received message content by means of an EDIN.

The Non-repudiation of EDIN element of service provides the originator with irrevocable proof that the subject message was received by the recipient EDI-UA and EDIM responsibility was accepted, forwarded, or refused. This shall protect against any attempt by the recipient EDI-UA to deny subsequently that the message was received and that EDIM responsibility for the message has been accepted as indicated.

The Non-repudiation of EDIN Request element of service, used in conjunction with EDI Notification Request, enables the originating EDI-UA to request the responding EDI-UA to provide it with irrevocable proof of the origin of the EDIN.

The Obsoleting Indication element of service allows the originator to indicate to the recipient that one or more EDIMs previously sent by the originator are obsolete. This element of service is used to convey the intent of the originator; the action taken by the recipient is a local matter.

The Originator Indication element of service allows the identity of the originator to be conveyed to the recipient.

The Proof of Content Received element of service allows an originating EDI-UA to get from a recipient EDI-UA proof that the original subject message content was received by the recipient EDI-UA and EDIM responsibility was accepted, forwarded, or refused.

The Proof of Content Received Request element of service enables an originating EDI-UA to request the recipient EDI-UA to provide it with proof of the received message content by means of an EDIN.

The Proof of EDIN element of service allows the originator to obtain the means to corroborate that the subject message was received by the recipient EDI-UA and EDIM responsibility was accepted, forwarded, or refused.

The Proof of EDIN Request element of service, used in conjunction with EDI Notification Request, enables the originating EDI-UA to request the responding EDI-UA to provide it with a corroboration of the source of the EDIN

The Recipient Indication element of service allows the originator to provide the names of one or more EDIMG users who are intended recipients of the EDIM. In addition it is possible to specify an action request qualifier for each recipient, such as:

1. For action
2. Copy
3. Other as defined bilaterally

The action request qualifier is used to convey the intent of the originator; the action taken by the recipient is a local matter.

The Related Messages element of service allows the originator to associate with the EDIM being sent, the globally unique identifiers of one or more other messages which share the same identification space (e.g., IP messages).

The Services Indication element of service allows the originator to indicate in the heading of the EDIM various service requests to service suppliers that have bilateral meaning.

The Stored EDI Message Auto-forward element of service allows a user of an EDI-MS to have the message store automatically perform EDI forwarding, with or without accepting EDIM responsibility. The user of the EDI-MS may establish criteria for selecting EDIMs through use of the element of service MS Register. The complete EDIM, as received from the originator, is forwarded unchanged, and if requested, an appropriate EDIN is generated by the EDI-MS. EDIM responsibility forwarding is limited to only one recipient.

The Typed Body element of service permits the nature and characteristics of the body of an EDIM to be conveyed along with the body. Permissible bodypart types are EDI body, forwarded EDIM body, and externally defined bodyparts.

NIST-114A
(REV. 3-89)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NISTIR 4608

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
JUNE 1991

4. TITLE AND SUBTITLE

EDI and X.400

5. AUTHOR(S)

Paul Markovitz

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

10. SUPPLEMENTARY NOTES

[ ] DOCUMENT DESCRIBES A COMPUTER PROGRAM; SF-185, FIPS SOFTWARE SUMMARY, IS ATTACHED.

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

Electronic Data Interchange (EDI) identifies a family of standards used for the electronic transmission of business oriented data (e.g., invoices and purchase orders). EDI standards specify data formats, but are designed independent of a communications protocol. In June, 1990, the Consultative Committee on International Telephony and Telegraphy (CCITT) drafted two Recommendations (F.435:EDI Messaging Service, X.435: EDI Messaging System) which define a standardized service and protocol for transmitting EDI data via the Message Handling System (MHS). Using the MHS EDI data can be transferred between compatible EDI applications implemented on heterogeneous computer systems.

This paper introduces the Messaging Handling System, the carrier service for EDI data, and the Interpersonal Messaging Service, the only MHS application currently standardized and the model for the EDI Messaging Service. Following the introductory material is a detailed review of the EDI Messaging draft Recommendations. The transmission of EDI data via the MHS is described as well as the relationships between EDI Messaging and directory, security, and physical delivery services.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

EDI, IPMS, message transfer, MHS, standardization, X.400.

13. AVAILABILITY

[X] UNLIMITED

[ ] FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).

[ ] ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.

[X] ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
38

15. PRICE
A03

ELECTRONIC FORM