

Section Two - Abstract Models

6. Overview

This section presents abstract models of Message Handling which provide the architectural basis for the more detailed specifications that appear in other Recommendations in the set.

.I.gl:Message Handling; is a distributed information processing task that integrates the following intrinsically related sub-tasks:

- a) .I.gl:Message Transfer;: The non-real-time carriage of information objects between parties using computers as intermediaries.
- b) .I.gl:Message Storage;: The automatic storage for later retrieval of information objects conveyed by means of Message Transfer.

This section covers the following topics:

- a) Functional model
- b) Information model
- c) Operational model
- d) Security model

Note Message Handling has a variety of applications, one of which is Interpersonal Messaging, described in Recommendation X.420.

7. Functional Model

This clause provides a functional model of Message Handling. The concrete realization of the model is the subject of other Recommendations in the set.

The .I.gl:Message Handling Environment; (.I.ab:MHE;) comprises "primary" functional objects of several types, the Message Handling System (MHS), users, and distribution lists. The MHS in turn can be decomposed into lesser, "secondary" functional objects of several types, the Message Transfer System (MTS), user agents, message stores, and access units. The MTS in turn can be decomposed into still lesser, "tertiary" functional objects of a single type, message transfer agents.

The primary, secondary, and tertiary functional object types and selected access unit types are individually defined and described below.

As detailed below, functional objects are sometimes tailored to one or more applications of Message Handling, e.g., Interpersonal Messaging (see Recommendations X.420 and T.330). A functional object that has been tailored to an application understands the syntax and semantics of the contents of messages exchanged in that application.

As a local matter, functional objects may have capabilities beyond those specified in this Recommendation or others in the set. In particular, a typical user agent has message preparation, rendition, and storage capabilities that are not standardized.

7.1 Primary Functional Objects

The MHE comprises the Message Handling System, users, and distribution lists. These primary functional objects interact with one another. Their types are defined and described below.

The situation is depicted in Figure 1/X.402.

+----+ | 01 || 02 || 03 || 04 || 05 || 06 || 07 || 08 || 09 || 10 || 11 || 12 || 13 || 14 || 15 || 16 || 17 || 18 || 19 || 20 || 21 ||
| 22 || 23 || 24 || 25 || 26 || 27 || 28 || 29 | +----+

Figure .F.:1/X.402 The Message Handling Environment

7.1.1 The Message Handling System

The principal purpose of Message Handling is to convey information objects from one party to another. The functional object by means of which this is accomplished is called the .I.gl:Message Handling System; (.I.ab:MHS;).

The MHE comprises a single MHS.

7.1.2 Users

The principal purpose of the MHS is to convey information objects between users. A functional object (e.g., a person) that engages in (rather than provides) Message Handling is called a .I.gl:user;.

The following kinds of user are distinguished:

- a) .I.gl:direct user;: A user that engages in Message Handling by direct use of the MHS.
- b) .I.gl:indirect user;: A user that engages in Message Handling by indirect use of the MHS, i.e., through another

communication system (e.g., a postal system or the telex network) to which the MHS is linked.

The MHE comprises any number of users.

7.1.3 Distribution Lists

By means of the MHS a user can convey information objects to pre-specified groups of users as well as to individual users.

The functional object that represents a pre-specified group of users and other DLs is called a .I.gl:distribution list;

(.I.ab:DL;).

A DL identifies zero or more users and DLs called its .I.gl:members;. The latter DLs (if any) are said to be .I.gl:nested;.

Asking the MHS to convey an information object (e.g., a message) to a DL is tantamount to asking that it convey the object to its members. Note that this is recursive.

The right, or permission, to convey messages to a particular DL may be controlled. This right is called .I.gl:submit permission;. As a local matter the use of a DL can be further restricted.

The MHE comprises any number of DLs.

Note A DL might be further restricted, e.g., to the conveyance of messages of a prescribed content type.

7.2 Secondary Functional Objects

The MHS comprises the Message Transfer System, user agents, message stores, and access units. These secondary functional objects interact with one another. Their types are defined and described below.

The situation is depicted in Figure 2/X.402.

+----+ | 01 || 02 || 03 || 04 || 05 || 06 || 07 || 08 || 09 || 10 || 11 || 12 || 13 || 14 || 15 || 16 || 17 || 18 || 19 || 20 || 21 || 22 ||
| 23 || 24 || 25 || 26 || 27 || 28 || 29 | +----+

Figure .F.:2/X.402 The Message Handling System

7.2.1 The Message Transfer System

The MHS conveys information objects to individual users and to the members of DLs. The functional object that actually does this is called the .I.gl:Message Transfer System; (.I.ab:MTS;). The MTS is a store-and-forward communication system and can be considered the backbone of the MHS.

The MTS is general-purpose, supporting all applications of Message Handling. Additionally, the MTS may be tailored to one or more particular applications so it can carry out conversion.

The MHS comprises a single MTS.

7.2.2 User Agents

The functional object by means of which a single direct user engages in Message Handling is called a .I.gl:user agent; (.I.ab:UA;).

A typical UA is tailored to one or more particular applications of Message Handling.

The MHS comprises any number of UAs.

Note A UA that serves a human user typically interacts with him by means of input/output devices (e.g., a keyboard, display, scanner, printer, or combination of these).

7.2.3 Message Stores

A typical user must store the information objects it receives. The functional object that provides a (single) direct user with capabilities for Message Storage is called a .I.gl:message store; (.I.ab:MS;). Each MS is associated with one UA, but not every UA has an associated MS.

Every MS is general-purpose, supporting all applications of Message Handling. Additionally, an MS may be tailored to one or more particular applications so that it can more capably submit and support the retrieval of messages associated with that application.

The MHS comprises any number of MSs.

Note As a local matter a UA may provide for information objects storage that either supplements or replaces that of an MS.

7.2.4 Access Units

The functional object that links another communication system (e.g., a postal system or the telex network) to the MTS and via which its patrons engage in Message Handling as indirect users is called an .I.gl:access unit; (.I.ab:AU;).

A typical AU is tailored to a particular communication system and to one or more particular applications of Message Handling.

The MHS comprises any number of AUs.

7.3 Tertiary Functional Objects

The MTS comprises message transfer agents. These tertiary functional objects interact. Their type is defined and described

below.

The situation is depicted in Figure 3/X.402.

+----+ | 01 || 02 || 03 || 04 || 05 || 06 || 07 || 08 || 09 || 10 || 11 || 12 || 13 || 14 || 15 || 16 || 17 || 18 || 19 || 20 || 21 || 22 ||
| 23 || 24 || 25 || 26 || 27 || 28 || 29 | +----+

Figure .F.:3/X.402 The Message Transfer System

7.3.1 Message Transfer Agents

The MTS conveys information objects to users and DLs in a store-and-forward manner. A functional object that provides one link in the MTS' store-and-forward chain is called a .I.gl:message transfer agent; (.I.ab:MTA;).

Every MTA is general-purpose, supporting all applications of Message Handling. Additionally, an MTA may be tailored to one or more particular applications so it can carry out conversion.

The MTS comprises any number of MTAs.

7.4 Selected AU Types

As described above, the MHS interworks with communication systems of other types via AUs. Several selected AU types--physical delivery, telematic, and telex--are introduced in the clauses below.

7.4.1 Physical Delivery

A .I.gl:physical delivery access unit; (.I.ab:PDAU;) is an AU that subjects messages (but neither probes nor reports) to physical rendition and that conveys the resulting physical messages to a physical delivery system.

The transformation of a message into a physical message is called .I.gl:physical rendition;. A .I.gl:physical message; is a physical object (e.g., a letter and its paper envelope) that embodies a message.

A .I.gl:physical delivery system; (.I.ab:PDS;) is a system that performs physical delivery. One important kind of PDS is postal systems. .I.gl:Physical delivery; is the conveyance of a physical message to a patron of a PDS, one of the indirect users to which the PDAU provides Message Handling capabilities.

Among the applications of Message Handling supported by every PDAU is Interpersonal Messaging (see Recommendation X.420).

7.4.2 Telematic

Telematic access units, which support Interpersonal Messaging exclusively, are introduced in Recommendation X.420.

7.4.3 Telex

Telex access units, which support Interpersonal Messaging exclusively, are introduced in Recommendation X.420.

8. Information Model

This clause provides an information model of Message Handling. The concrete realization of the model is the subject of other Recommendations in the set.

The MHS and MTS can convey information objects of three classes: messages, probes, and reports. These classes are listed in the first column of Table 4/X.402. For each listed class, the second column indicates the kinds of functional objects--users, UAs, MSs, MTAs, and AUs--that are the ultimate sources and destinations for such objects.

Table .T.:4/X.402 Conveyable Information Objects

+-----+-----+ Infor- Functional Object mation +-----+ Object user UA MS MTA AU
+-----+-----+ message SD - - - - probe S - - D - report D - - S - +-----
+-----+ +- Legend -----+ S ultimate source D ultimate destination +-----+

The information objects, summarized in the table, are individually defined and described in the clauses below.

8.1 Messages

The primary purpose of Message Transfer is to convey information objects called .I.gl:message;s from one user to others. A message has the following parts, as depicted in Figure 4/X.402:

a) .I.gl:envelope;; An information object whose composition varies from one transmittal step to another and that variously identifies the message's originator and potential recipients, documents its previous conveyance and directs its subsequent conveyance by the MTS, and characterizes its content.

b) .I.gl:content;; An information object that the MTS neither examines nor modifies, except for conversion, during its conveyance of the message.

+----+ | 01 || 02 || 03 || 04 || 05 || 06 || 07 || 08 || 09 || 10 || 11 || 12 || 13 || 14 || 15 || 16 || 17 || 18 || 19 || 20 || 21 || 22 ||
| 23 || 24 || 25 || 26 || 27 || 28 || 29 | +----+

Figure .F.:4/X.402 A Message's Envelope and Content

One piece of information borne by the envelope identifies the type of the content. The .I.gl:content type; is an identifier (an

ASN.1 Object Identifier or Integer) that denotes the syntax and semantics of the content overall. This identifier enables the MTS to determine the message's deliverability to particular users, and enables UAs and MSs to interpret and process the content.

Another piece of information borne by the envelope identifies the types of encoded information represented in the content. An .I.gl:encoded information type; (.I.ab:EIT;) is an identifier (an ASN.1 Object Identifier or Integer) that denotes the medium and format (e.g., IA5 text or Group 3 facsimile) of individual portions of the content. It further enables the MTS to determine the message's deliverability to particular users, and to identify opportunities for it to make the message deliverable by converting a portion of the content from one EIT to another.

8.2 Probes

A second purpose of Message Transfer is to convey information objects called .I.gl:probe;s from one user up to but just short of other users (i.e., to the MTAs serving those users). A probe describes a class of message and is used to determine the deliverability of such messages.

A message described by a probe is called a .I.gl:described message;.

A probe comprises an envelope alone. This envelope contains much the same information as that for a message. Besides bearing the content type and encoded information types of a described message, the probe's envelope bears the length of its content.

The submission of a probe elicits from the MTS largely the same behavior as would submission of any described message, except that DL expansion and delivery are forgone in the case of the probe. In particular, and apart from the consequences of the suppression of DL expansion, the probe provokes the same reports as would any described message. This fact gives probes their utility.

8.3 Reports

A third purpose of Message Transfer is to convey information objects called reports to users. Generated by the MTS, a report relates the outcome or progress of a message's or probe's transmittal to one or more potential recipient.

The message or probe that is the subject of a report is called its .I.gl:subject message; or .I.gl:subject probe;.

A report concerning a particular potential recipient is conveyed to the originator of the subject message or probe unless the potential recipient is a member recipient. In the latter case, the report is conveyed to the DL of which the member recipient is a member. As a local matter (i.e., by policy established for that particular DL), the report may be further conveyed to the DL's owner; either to another, containing DL (in the case of nesting) or to the originator of the subject message or probe (otherwise); or both.

The outcome that a single report may relate are of the following kinds:

- a) .I.gl:delivery report;; delivery, export, or affirmation of the subject message or probe, or DL expansion.
- b) .I.gl:non-delivery report;; non-delivery or non-affirmation of the subject message or probe.

A report may comprise one or more delivery and/or non-delivery reports.

A message or probe may provoke several delivery and/or non-delivery reports concerning a particular potential recipient.

Each marks the passage of a different transmittal step or event.

9. Operational Model

This clause provides an operational model of Message Handling. The concrete realization of the model is the subject of other Recommendations in the set.

The MHS can convey an information object to individual users, DLs, or a mix of the two. Such conveyance is accomplished by a process called transmittal comprising steps and events. The process, its parts, and the roles that users and DLs play in it are defined and described below.

9.1 Transmittal

The conveyance or attempted conveyance of a message or probe is called .I.gl:transmittal;. Transmittal encompasses a message's conveyance from its originator to its potential recipients, and a probe's conveyance from its originator to MTAs able to affirm the described messages' deliverability to the probe's potential recipients. Transmittal also encompasses the conveyance or attempted conveyance to the originator of any reports the message or probe may provoke.

A transmittal comprises a sequence of transmittal steps and events. A .I.gl:transmittal step; (or .I.gl:step;) is the conveyance of a message, probe, or report from one functional object to another "adjacent" to it. A .I.gl:transmittal event; (or .I.gl:event;) is processing of a message, probe, or report within a functional object that may influence the functional object's selection of the next transmittal step or event.

The information flow of transmittal is depicted in Figure 5/X.402. The figure shows the kinds of functional objects--direct

users, indirect users, UAs, MSs, MTAs, and AUs--that may be involved in a transmittal, the information objects--messages, probes, and reports--that may be conveyed between them, and the names of the transmittal steps by means of which those conveyances are accomplished.

The figure highlights the facts that a message or report may be retrieved repeatedly and that only the first conveyance of a retrieved object from UA to user constitutes receipt.

+-----+	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22	
23 24 25 26 27 28 29	+-----+	+- Legend -----+ M message ORG origination EXP export P probe SBM submission DLV delivery R report IMP import RTR retrieval TRN transfer REC receipt +-----+

Figure .F.:5/X.402 The Information Flow of Transmittal

One event plays a distinguished role in transmittal. Splitting replicates a message or probe and divides responsibility for its immediate recipients among the resulting information objects. The potential recipients associated with a particular instance of a message or probe are called the .I.gl:immediate recipient;s. An MTA stages a splitting if the next step or event required in the conveyance of a message or probe to some immediate recipients differs from that required in its conveyance to others. Each of the step and event descriptions which follow assumes that the step or event is appropriate for all immediate recipients, a situation that can be created, if necessary, by splitting.

9.2 Transmittal Roles

Users and DLs play a variety of roles in a message's or probe's transmittal. These roles are informally categorized as "source" roles, "destination" roles, or statuses to which users or DLs can be elevated.

A user may play the following "source" role in the transmittal of a message or probe:

a) .I.gl:originator;; The user (but not DL) that is the ultimate source of a message or probe.

A user or DL may play any of the following "destination" roles in the transmittal of a message or probe:

a) .I.gl:intended recipient;; One of the users and DLs the originator specifies as a message's or probe's intended destinations.

b) .I.gl:originator-specified alternate recipient;; The user or DL (if any) to which the originator requests that a message or probe be conveyed if it cannot be conveyed to a particular intended recipient.

c) .I.gl:member recipient;; A user or DL to which a message (but not a probe) is conveyed as a result of DL expansion.

d) .I.gl:recipient-assigned alternate recipient;; The user or DL (if any) to which an intended, originator-specified alternate, or member recipient may have elected to redirect messages.

A user or DL may attain any of the following statuses in the course of a message's or probe's transmittal:

a) .I.gl:potential recipient;; Any user or DL to (i.e., toward) which a message or probe is conveyed at any point during the course of transmittal. Necessarily an intended, originator-specified alternate, member, or recipient-assigned alternate recipient.

b) .I.gl:actual recipient; (or .I.gl:recipient;): A potential recipient for which delivery or affirmation takes place.

9.3 Transmittal Steps

The kinds of steps that may occur in a transmittal are listed in the first column of Table 5/X.402. For each listed kind, the second column indicates whether this Recommendation and others in the set standardize such steps, the third column the kinds of information objects--messages, probes, and reports-- that may be conveyed in such a step, the fourth column the kinds of functional objects--users, UAs, MSs, MTAs, and AUs--that may participate in such a step as the object's source or destination.

The table is divided into three sections. The steps in the first section apply to the "creation" of messages and probes, those in the last to the "disposal" of messages and reports, and those in the middle section to the "relaying" of messages, probes, and reports.

Table .T.:5/X.402 Transmittal Steps

Objects				ard-				Information				Functional				Stand-			
Objects	Objects							Transmittal Step	ized?	M	P	R	user						
UA MS MTA AU								origination	No	x	x	-	S	D	-	-	-	-	-
submission	Yes	x	x	-	-	S	SD D	-											
No	x	x	x	-	-	D	S	transfer	Yes	x	x	x	-	-	-	SD	-	export	No
D																			
Yes	x	-	x	-	D	S	-	receipt	No	x	-	x	D	D	S	-	retrieval		

+-----+ +- Legend -----+ | M message S source x permitted | | P probe D destination
 | | R report | +-----+

The kinds of transmittal steps, summarized in the table, are individually defined and described in the clauses below.

9.3.1 Origination

In an .I.gl:origination; step, either a direct user conveys a message or probe to its UA, or an indirect user conveys a message or probe to the communication system that serves it. This step gives birth to the message or probe and is the first step in its transmittal.

The user above constitutes the message's or probe's originator. In this step, the originator identifies the message's or probe's intended recipients. Additionally, for each intended recipient, the originator may (but need not) identify an originator-specified alternate recipient.

9.3.2 Submission

In a .I.gl:submission; step, a message or probe is conveyed to an MTA and thus entrusted to the MTS. Two kinds of submission are distinguished:

a) .I.gl:indirect submission;; A transmittal step in which the originator's UA conveys a message or probe to its MS and in which the MS effects direct submission. Such a step follows origination.

This step may be taken only if the user is equipped with an MS.

b) .I.gl:direct submission;; A transmittal step in which the originator's UA or MS conveys a message or probe to an MTA. Such a step follows origination or occurs as part of indirect submission.

This step may be taken whether or not the user is equipped with an MS.

Indirect and direct submission are functionally equivalent except that additional capabilities may be available with the former. Indirect submission may differ from direct submission in other respects (e.g., the number of open systems with which that embodying a UA must interact) and for that reason be preferable to direct submission.

The UA or MS involved in direct submission is called the .I.gl:submission agent;. A submission agent is made known to the MTS by a process of registration, as a result of which the submission agent and MTS keep one another informed of their names, their locations, and any other characteristics required for their interaction.

9.3.3 Import

In an .I.gl:import; step, an AU conveys a message, probe, or report to an MTA. This step injects into the MTS an information object born in another communication system, and follows its conveyance by that system.

Note The concept of importing is a generic one. How this step is effected varies, of course, from one type of AU to another.

9.3.4 Transfer

In a .I.gl:transfer; step, one MTA conveys a message, probe, or report to another. This step transports an information object over physical and sometimes organizational distances and follows direct submission, import, or (a prior) transfer.

This step may be taken, of course, only if the MTS comprises several MTAs.

The following kinds of transfer are distinguished, on the basis of the number of MDs involved:

a) .I.gl:internal transfer;; A transfer involving MTAs within a single MD.

b) .I.gl:external transfer;; A transfer involving MTAs in different MDs.

9.3.5 Export

In an .I.gl:export; step, an MTA conveys a message, probe, or report to an AU. This step ejects from the MTS an information object bound for another communication system. It follows direct submission, import, or transfer.

As part of this step, the MTA may generate a delivery report.

Note The concept of exporting is a generic one. How this step is effected varies, of course, from one type of AU to another.

9.3.6 Delivery

In a .I.gl:delivery; step, an MTA conveys a message or report to an MS or UA. The MS and UA are those of a potential recipient of the message, or the originator of the report's subject message or probe. This step entrusts the information object to a representative of the user and follows direct submission, import, or transfer. It also elevates the user in question to the status of an actual recipient.

As part of this step, in the case of a message, the MTA may generate a delivery report.

The MS or UA involved is called the .I.gl:delivery agent;. A delivery agent is made known to the MTS by a process of registration, as a result of which the delivery agent and MTS keep one another informed of their names, their locations, and any other characteristics required for their interaction.

9.3.7 Retrieval

In a .I.gl:retrieval; step, a user's MS conveys a message or report to its UA. The user in question is an actual recipient of the message or the originator of the subject message or probe. This step non-destructively retrieves the information object from storage. This step follows delivery or (a prior) retrieval.

This step may be taken only if the user is equipped with an MS.

9.3.8 Receipt

In a .I.gl:receipt; step, either a UA conveys a message or report to its direct user, or the communication system that serves an indirect user conveys such an information object to that user. In either case, this step conveys the object to its ultimate destination.

In the case of a direct user, this step follows the object's delivery or first retrieval (only). In the case of an indirect user, it follows the information object's conveyance by the communication system serving the user. In either case, the user is a potential recipient (and, in the case of a direct user, an actual recipient) of the message in question, or the originator of the subject message or probe.

9.4 Transmittal Events

The kinds of events that may occur in a transmittal are listed in the first column of Table 6/X.402. For each listed kind, the second column indicates the kinds of information objects--messages, probes, and reports--for which such events may be staged, the third column the kinds of functional objects--users, UAs, MSs, MTAs, and AUs---that may stage such events.

All the events occur within the MTS.

Table .T.:6/X.402 Transmittal Events

Information										Functional			Objects																		
Transmittal Event										M	P	R	user	UA	MS	MTA	AU														
splitting										x	x	-	-	-	x	-	joining	x	x	x	-	-	-	x							
name resolution										x	x	-	-	-	x	-	DL expansion	x	-	-	-	-	x	-	redirection	x	x	-	-	-	
conversion										x	x	-	-	-	x	-	non-delivery	x	-	x	-	-	-	x	-	non-affirmation	-	x	-	-	-
affirmation										-	x	-	-	-	x	-	routing	x	x	x	-	-	-	x	-						
Legend										M message x permitted					P probe			R report													

The kinds of transmittal events, summarized in the table, are individually defined and described in the clauses below.

9.4.1 Splitting

In a .I.gl:splitting; event, an MTA replicates a message or probe, dividing responsibility for its immediate recipients among the resulting information objects. This event effectively allows an MTA to independently convey an object to various potential recipients.

An MTA stages a splitting when the next step or event required in the conveyance of a message or probe to some immediate recipients differs from that required in its conveyance to others.

9.4.2 Joining

In a .I.gl:joining; event, an MTA combines several instances of the same message or probe, or two or more delivery and/or non-delivery reports for the same subject message or probe.

An MTA may, but need not stage a joining when it determines that the same events and next step are required to convey several highly related information objects to their destinations.

9.4.3 Name Resolution

In a .I.gl:name resolution; event, an MTA adds the corresponding O/R address to the O/R name that identifies one of a message's or probe's immediate recipients.

9.4.4 DL Expansion

In a .I.gl:DL expansion; event, an MTA resolves a DL among a message's (but not a probe's) immediate recipients to its members which are thereby made member recipients. This event removes indirection from the immediate recipients' specification.

A particular DL is always subjected to DL expansion at a pre-established location within the MTS. This location is called the DL's .I.gl:expansion point; and is identified by an O/R address.

As part of this event, the MTA may generate a delivery report.

DL expansion is subject to submit permission. In the case of a nested DL, that permission must have been granted to the DL of which the nested DL is a member. Otherwise, it must have been granted to the originator.

9.4.5 Redirection

In a .I.gl:redirection; event, an MTA replaces a user or DL among a message's or probe's immediate recipients with an originator-specified or recipient-assigned alternate recipient.

9.4.6 Conversion

In a .I.gl:conversion; event, an MTA transforms parts of a message's content from one EIT to another, or alters a probe so it appears that the described messages were so modified. This event increases the likelihood that an information object can be delivered or affirmed by tailoring it to its immediate recipients.

The following kinds of conversion are distinguished, on the basis of how the EIT of the information to be converted and the EIT to result from the conversion are selected:

- a) .I.gl:explicit conversion;: A conversion in which the originator selects both the initial and final EITs.
- b) .I.gl:implicit conversion;: A conversion in which the MTA selects the final EITs based upon the initial EITs.

9.4.7 Non-delivery

In a .I.gl:non-delivery; event, an MTA determines that the MTS cannot deliver a message to its immediate recipients, or cannot deliver a report to the originator of its subject message or probe. This event halts the conveyance of an object the MTS deems unconveyable.

As part of this event, in the case of a message, the MTA generates a non-delivery report.

An MTA stages a non-delivery, e.g., when it determines that the immediate recipients are improperly specified, that they do not accept delivery of messages like that at hand, or that the message has not been delivered to them within pre-specified time limits.

9.4.8 Non-affirmation

In a .I.gl:non-affirmation; event, an MTA determines that the MTS could not deliver a described message to a probe's immediate recipients. This event partially or fully determines the answer to the question posed by a probe.

As part of this event, the MTA generates a non-delivery report.

An MTA stages a non-affirmation, e.g., when it determines that the immediate recipients are improperly specified or would not accept delivery of a described message.

9.4.9 Affirmation

In an .I.gl:affirmation; event, an MTA determines that the MTS could deliver any described message to a probe's immediate recipients. This event partially or fully determines the answer to the question posed by a probe, and elevates the immediate recipients to the status of actual recipients.

As part of this event, the MTA may generate a delivery report.

An MTA stages an affirmation once it determines that the immediate recipients are properly specified and, if the immediate recipients are users (but not DLs), would accept delivery of any described message. If the immediate recipients are DLs, and MTA stages an affirmation if the DL exists and the originator has the relevant submit permission.

9.4.10 Routing

In a .I.gl:routing; event, an MTA selects the "adjacent" MTA to which it will transfer a message, probe, or report. This event incrementally determines an information object's route through the MTS and (obviously) may be taken only if the MTS comprises several MTAs.

The following kinds of routing are distinguished, on the basis of the kind of transfer for which they prepare:

- a) .I.gl:internal routing;: A routing preparatory to an internal transfer (i.e., a transfer within an MD).
- b) .I.gl:external routing;: A routing preparatory to an external transfer (i.e., a transfer between MDs).

An MTA stages a routing when it determines that it can stage no other event, and take no step, regarding an object.

10. Security Model

This clause provides an abstract security model for Message Transfer. The concrete realization of the model is the subject of other Recommendations in the set. The security model provides a framework for describing the security services that counter potential threats (see annex D) to the MTS and the security elements that support those services.

The security features are an optional extension to the MHS that can be used to minimise the risk of exposure of assets and resources to violations of a security policy (threats). Their aim is to provide features independently of the communications services provided by other lower or higher entities. Threats may be countered by the use of physical security, computer security (.I.ab:COMPUSEC;), or security services provided by the MHS. Depending on the perceived threats, certain of the

MHS security services will be selected in combination with appropriate physical security and COMPUSEC measures. The security services supported by the MHS are described below. The naming and structuring of the services are based on ISO 7498-2.

Note - Despite these security features, certain attacks may by be mounted against communication between a user and the MHS or against user-to-user communication (e.g. in the case of users accessing their UAs). To counter these attacks requires extensions to the present security model and services which are **for further study**.

In many cases, the broad classes of threats are covered by several of the services listed.

The security services are supported through use of service elements of the Message Transfer Service message envelope. The envelope contains security relevant arguments as described in Recommendation X.411. The description of the security services takes the following general form. In clause 10.2 the services are listed, with, in each case, a definition of the service and an indication of how it may be provided using the security elements in Recommendation X.411. In clause 10.3 the security elements are individually described, with, in each case, a definition of the service element and references to its constituent arguments in Recommendation X.411.

Many of the techniques employed rely on encryption mechanisms. The security services in the MHS allow for flexibility in the choice of algorithms. However, in some cases only the use of asymmetric encryption has been fully defined in this Recommendation. A future version of this Recommendation may make use of alternative mechanisms based on symmetric encipherment.

Note The use of the terms "security service" and "security element" in this clause are not to be confused with the terms "service" and "element of service" as used in Recommendation X.400. The former terms are used in the present clause to maintain consistency with ISO 7498-2.

10.1 Security Policies

Security services in the MHS must be capable of supporting a wide range of security policies which extend beyond the confines of the MHS itself. The services selected and the threats addressed will depend on the individual application and levels of trust in parts of the system.

A security policy defines how the risk to and exposure of assets can be reduced to an acceptable level.

In addition, operation between different domains, each with their own security policy, will be required. As each domain will be subject to its own overall security policy, covering more than just the MHS, a bilateral agreement on interworking between two domains will be required. This must be defined so as not to conflict with the security policies for either domain and effectively becomes part of the overall security policy for each domain.

10.2 Security Services

This clause defines the Message Transfer security services. The naming and structuring of the services are based on ISO 7498-2.

MHS security services fall into several broad classes. These classes and the services in each are listed in Table 7/X.402. An asterisk (*) under the heading of the form X/Y indicates that the service can be provided from a functional object of type X to one of type Y.

Table .T.:7/X.402 Message Transfer Security Services

+-----+-----+ UA/UA MS/MTA UA/MTA MTA/UA			
SERVICE	UA/MS UA/MTA MTA/MTA MS/UA	+ - ORIGIN AUTHENTICATION	-----
+-----+ Message Origin Authentication	* * - * - - - -	Probe Origin Authentication	- -
* * - - - - Report Origin Authentication	- - - - * * - -	Proof of Submission	- - - - - - * -
Proof of Delivery	* - - - - - - Note	+ - SECURE ACCESS MANAGEMENT	
+ Peer Entity Authentication	- * * * * * * * *	Security Context	- * * * * * * * * + - DATA
CONFIDENTIALITY	+-----+ Connection Confidentiality		- * * * * * * * *
Content Confidentiality	* - - - - - - -	Message Flow Confidentiality	* - - - - - - - + - DATA
INTEGRITY SERVICES	+-----+ Connection Integrity		- * * * * * * * * Content
Integrity	* - - - - - - -	Message Sequence Integrity	* - - - - - - - + - NON-REPUDIATION
+-----+ Non-repudiation of Origin		* - - * - - - -	Non-repudiation of
Submission	- - - - - - * -	Non-repudiation of Delivery	* - - - - - - - Message Security Labelling
* * * * * * * * + - SECURITY MANAGEMENT SERVICES	+-----+ Change Credentials		
- * - * * * * -	Register	- * - * - - - -	+-----+

+-----+ Note This service is provided by the recipient's MS to the originator's UA.

Throughout the security service definitions that follow, reference is made to Figure 6/X.402, which reiterates the MHS functional model in simplified form. The numeric labels are referenced in the text.

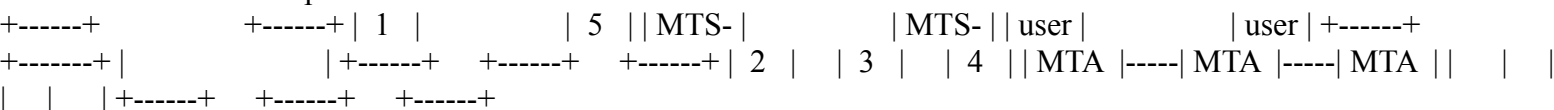


Figure .F.:6/X.402 Simplified MHS Functional Model

10.2.1 Origin Authentication Security Services

These security services provide for the authentication of the identity of communicating peer entities and sources of data.

10.2.1.1 Data Origin Authentication Security Services

These security services provide corroboration of the origin of a message, probe, or report to all concerned entities (i.e., MTAs or recipient MTS-users). These security services cannot protect against duplication of messages, probes, or reports.

10.2.1.1.1 Message Origin Authentication Security Service

The Message Origin Authentication Service enables the corroboration of the source of a message.

This security service can be provided using either the Message Origin Authentication or the Message Argument Integrity security element. The former can be used to provide the security service to any of the parties concerned (1-5 inclusive in the figure), whereas the latter can only be used to provide the security service to MTS-users (1 or 5 in the figure). The security element chosen depends on the prevailing security policy.

10.2.1.1.2 Probe Origin Authentication Security Service

The Probe Origin Authentication security service enables the corroboration of the source of a probe.

This security service can be provided by using the Probe Origin Authentication security element. This security element can be used to provide the security service to any of the MTAs through which the probe is transferred (2-4 inclusive in the figure).

10.2.1.1.3 Report Origin Authentication Security Service

The Report Origin Authentication security service enables the corroboration of the source of a report.

This security service can be provided by using the Report Origin Authentication security element. This security element can be used to provide the security service to the originator of the subject message or probe, as well as to any MTA through which the report is transferred (1-5 inclusive in the figure).

10.2.1.2 Proof of Submission Security Service

This security service enables the originator of a message to obtain corroboration that it has been received by the MTS for delivery to the originally specified recipient(s).

This security service can be provided by using the Proof of Submission security element.

10.2.1.3 Proof of Delivery Security Service

This security service enables the originator of a message to obtain corroboration that it has been delivered by the MTS to its intended recipient(s).

This security service can be provided by using the Proof of Delivery security element.

10.2.2 Secure Access Management Security Service

The Secure Access Management security service is concerned with providing protection for resources against their unauthorised use. It can be divided into two components, namely the Peer Entity Authentication and the Security Context security services.

10.2.2.1 Peer Entity Authentication Security Service

This security service is provided for use at the establishment of a connection to confirm the identity of the connecting entity. It may be used on the links 1-2, 2-3, 3-4, or 4-5 in the figure and provides confidence, at the time of usage only, that an entity is not attempting a masquerade or an unauthorised replay of a previous connection.

This security service is supported by the Authentication Exchange security element. Note that use of this security element may yield other data as a result of its operation that in certain circumstances can be used to support a Connection Confidentiality and/or a Connection Integrity security service.

10.2.2.2 Security Context Security Service

This security service is used to limit the scope of passage of messages between entities by reference to the Security Labels associated with messages. This security service is therefore closely related to the Message Security Labelling security service, which provides for the association of messages and Security Labels.

The Security Context security service is supported by the Security Context and the Register security elements.

10.2.3 Data Confidentiality Security Services

These security services provide for the protection of data against unauthorised disclosure.

10.2.3.1 Connection Confidentiality Security Service

The MHS does not provide a Connection Confidentiality security service. However, data for the invocation of such a security service in underlying layers may be provided as a result of using the Authentication Exchange security element to provide the Peer Entity Authentication security service. The security service may be required on any of links 1-2, 2-3, 3-4, or 4-5 in the figure.

10.2.3.2 Content Confidentiality Security Service

The Content Confidentiality security service provides assurance that the content of a message is only known to the sender and recipient of a message.

It may be provided using a combination of the Content Confidentiality and the Message Argument Confidentiality security elements. The Message Argument Confidentiality security element can be used to transfer a secret key which is used with the Content Confidentiality security element to encipher the message content. Using these security elements the service is provided from MTS-user 1 to MTS-user 5 in the figure, with the message content being unintelligible to MTAs.

10.2.3.3 Message Flow Confidentiality Security Service

This security service provides for the protection of information which might be derived from observation of message flow. Only a limited form of this security service is provided by the MHS.

The Double Enveloping Technique enables a complete message to become the content of another message. This could be used to hide addressing information from certain parts of the MTS. Used in conjunction with traffic padding (which is beyond the scope of this Recommendation) this could be used to provide message flow confidentiality. Other elements of this service, such as routing control or pseudonyms, are also beyond the scope of this Recommendation.

10.2.4 Data Integrity Security Services

These security services are provided to counter active threats to the MHS.

10.2.4.1 Connection Integrity Security Service

The MHS does not provide a Connection Integrity security service. However, data for the invocation of such a security service in underlying layers may be provided by using the Authentication Exchange security element to provide the Peer Entity Authentication security service. The security service may be required on any of links 1-2, 2-3, 3-4, or 4-5 in the figure.

10.2.4.2 Content Integrity Security Service

This security service provides for the integrity of the contents of a single message. This takes the form of enabling the determination of whether the message content has been modified. This security service does not enable the detection of message replay, which is provided by the Message Sequence Integrity security service.

This security service can be provided in two different ways using two different combinations of security elements.

The Content Integrity security element together with the Message Argument Integrity security element and, in some cases, the Message Argument Confidentiality security element can be used to provide the security service to a message recipient, i.e., for communication from MTS-user 1 to MTS-user 5 in the figure. The Content Integrity security element is used to compute a Content Integrity Check as a function of the entire message content. Depending on the method used to compute the Content Integrity Check, a secret key may be required, which may be confidentially sent to the message recipient using the Message Argument Confidentiality security element. The Content Integrity Check is protected against change using the Message Argument Integrity security element. The integrity of any confidential message arguments is provided using the Message Argument Confidentiality security element.

The Message Origin Authentication security element can also be used to provide this security service.

10.2.4.3 Message Sequence Integrity Security Service

This security service protects the originator and recipient of a sequence of messages against re-ordering of the sequence. In doing so it protects against replay of messages.

This security service may be provided using a combination of the Message Sequence Integrity and the Message Argument Integrity security elements. The former provides a sequence number to each message, which may be protected against change by use of the latter. Simultaneous confidentiality and integrity of the Message Sequence Number may be provided by use of the Message Argument Confidentiality security element.

These security elements provide the service for communication from MTS-user 1 to MTS-user 5 in the figure, and not to the

intermediate MTAs.

10.2.5 Non-Repudiation Security Services

These security services provide irrevocable proof to a third party after the message has been submitted, sent, or delivered, that the submission, sending, or receipt did occur as claimed. Note that for this to function correctly, the security policy must explicitly cover the management of asymmetric keys for the purpose of non-repudiation services if asymmetric algorithms are being used.

10.2.5.1 Non-repudiation of Origin Security Service

This security service provides the recipient(s) of a message with irrevocable proof of the origin of the message, its content, and its associated Message Security Label.

This security service can be provided in two different ways using two different combinations of security elements. Note that its provision is very similar to the provision of the (weaker) Content Integrity security service.

The Content Integrity security element together with the Message Argument Integrity security element and, in some cases, the Message Argument Confidentiality security element can be used to provide the service to a message recipient, i.e., for communication from MTS-user 1 to MTS-user 5 in the figure. The Content Integrity security element is used to compute a Content Integrity Check as a function of the entire message content. Depending on the method used to compute the Content Integrity Check, a secret key may be required, which may be confidentially sent to the message recipient using the Message Argument Confidentiality security element. The Content Integrity Check and, if required, the Message Security Label are protected against change and/or repudiation using the Message Argument Integrity security element. Any confidential message arguments are protected against change and/or repudiation using the Message Argument Confidentiality security element.

If the Content Confidentiality security service is not required, the Message Origin Authentication security element may also be used as a basis for this security service. In this case the security service may be provided to all elements of the MHS, i.e., for all of 1-5 in the figure.

10.2.5.2 Non-Repudiation of Submission Security Service

This security service provides the originator of the message with irrevocable proof that the message was submitted to the MTS for delivery to the originally specified recipient(s).

This security service is provided using the Proof of Submission security element in much the same way as that security element is used to support the (weaker) Proof of Submission security service.

10.2.5.3 Non-Repudiation of Delivery Security Service

This security service provides the originator of the message with irrevocable proof that the message was delivered to its originally specified recipient(s).

This security service is provided using the Proof of Delivery security element in much the same way as that security element is used to support the (weaker) Proof of Delivery security service.

10.2.6 Message Security Labelling Security Service

This security service allows Security Labels to be associated with all entities in the MHS, i.e., MTAs and MTS-users. In conjunction with the Security Context security service it enables the implementation of security policies defining which parts of the MHS may handle messages with specified associated Security Labels.

This security service is provided by the Message Security Label security element. The integrity and confidentiality of the label are provided by the Message Argument Integrity and the Message Argument Confidentiality security elements.

10.2.7 Security Management Services

A number of security management services are needed by the MHS. The only management services provided within Recommendation X.411 are concerned with changing credentials and registering MTS-user security labels.

10.2.7.1 Change Credentials Security Service

This security service enables one entity in the MHS to change the credentials concerning it held by another entity in the MHS. It may be provided using the Change Credentials security element.

10.2.7.2 Register Security Service

This security service enables the establishment at an MTA of the Security Labels which are permissible for one particular MTS-user. It may be provided using the Register security element.

10.2.7.3 MS-Register Security Service

The security service enables the establishment of the security label which are permissible for the MS-user.

10.3 Security Elements

The following clauses describe the security elements available in the protocols described within Recommendation X.411 to support the security services in the MHS. These security elements relate directly to arguments in various services described in Recommendation X.411. The objective of this clause is to separate out each element of the Recommendation X.411 service definitions that relate to security, and to define the function of each of these identified security elements.

10.3.1 Authentication Security Elements

These security elements are defined in order to support authentication and integrity security services.

10.3.1.1 Authentication Exchange Security Element

The Authentication Exchange security element is designed to authenticate, possibly mutually, the identity of an MTS-user to an MTA, an MTA, an MS to a UA, or a UA to an MS to an MTS-user. It is based on the exchange or use of secret data, either passwords, asymmetrically encrypted tokens, or symmetrically encrypted tokens. The result of the exchange is corroboration of the identity of the other party, and, optionally, the transfer of confidential data which may be used in providing the Connection Confidentiality and/or the Connection Integrity security service in underlying layers. Such an authentication is only valid for the instant that it is made and the continuing validity of the authenticated identity depends on whether the exchange of confidential data, or some other mechanism, is used to establish a secure communication path. The establishment and use of a secure communication path is outside the scope of this Recommendation.

This security element uses the Initiator Credentials argument and the Responder Credentials result of the MTS-bind, MS-bind and MTA-bind services. The transferred credentials are either passwords or tokens.

10.3.1.2 Data Origin Authentication Security Elements

These security elements are specifically designed to support data origin authentication services, although they may also be used to support certain data integrity services.

10.3.1.2.1 Message Origin Authentication Security Element

The Message Origin Authentication security element enables anyone who receives or transfers message to authenticate the identity of the MTS-user that originated the message. This may mean the provision of the Message Origin Authentication or the Non-repudiation of Origin security service.

The security element involves transmitting, as part of the message, a Message Origin Authentication Check, computed as a function of the message content, the message Content Identifier, and the Message Security Label. If the Content Confidentiality security service is also required, the Message Origin Authentication Check is computed as a function of the enciphered rather than the unenciphered message content. By operating on the message content as conveyed in the overall message (i.e., after the optional Content Confidentiality security element), any MHS entity can check the overall message integrity without the need to see the plaintext message content. However, if the Content Confidentiality security service is used, the Message Origin Authentication security element cannot be used to provide the Non-repudiation of Origin security service.

The security element uses the Message Origin Authentication Check, which is one of the arguments of the Message Submission, Message Transfer, and Message Delivery services.

10.3.1.2.2 Probe Origin Authentication Security Element

Similar to the Message Origin Authentication security element, the Probe Origin Authentication security element enables any MTA to authenticate the identity of the MTS-user which originated a probe.

This security element uses the Probe Origin Authentication Check, which is one of the arguments of the Probe Submission service.

10.3.1.2.3 Report Origin Authentication Security Element

Similar to the Message Origin Authentication security element, the Report Origin Authentication security element enables any MTA or MTS-user who receives a report to authenticate the identity of the MTA which originated the report.

This security element uses the Report Origin Authentication Check, which is one of the arguments of the Report Delivery service.

10.3.1.3 Proof of Submission Security Element

This security element provides the originator of a message with the means to establish that a message was accepted by the MHS for transmission.

The security element is made up of two arguments: a request for Proof of Submission, sent with a message at submission time, and the Proof of Submission, returned to the MTS-user as part of the Message Submission results. The Proof of Submission is generated by the MTS, and is computed as a function of all the arguments of the submitted message, the Message Submission Identifier, and the Message Submission Time.

The Proof of Submission argument can be used to support the Proof of Submission security service. Depending on the security policy in force, it may also be able to support the (stronger) Non-repudiation of Submission security service.

The Proof of Submission Request is an argument of the Message Submission service. The Proof of Submission is one of the results of the Message Submission service.

10.3.1.4 Proof of Delivery Security Element

This security element provides the originator of a message with the means to establish that a message was delivered to the destination by the MHS.

The security element is made up of a number of arguments. The message originator includes a Proof of Delivery Request with the submitted message, and this request is delivered to each recipient with the message. A recipient may then compute the Proof of Delivery as a function of a number of arguments associated with the message. The proof of delivery is returned by the MTS to the message originator, as part of a report on the results of the original Message Submission.

The Proof of Delivery can be used to support the Proof of Delivery security service. Depending on the security policy in force, it may also be able to support the (stronger) Non-repudiation of Delivery security service.

The Proof of Delivery Request is an argument of the Message Submission, Message Transfer, and Message Delivery services. The Proof of Delivery is both one of the results of the Message Delivery service and one of the arguments of the Report Transfer and Report Delivery services.

Note - Non-receipt of a Proof of Delivery does not imply non-delivery.

10.3.2 Secure Access Management Security Elements

These security elements are defined in order to support the Secure Access Management security service and the security management services.

10.3.2.1 Security Context Security Element

When an MTS-user or an MTA binds to an MTA or MTS-user, the bind operation specifies the security context of the connection. This limits the scope of passage of messages by reference to the labels associated with messages. Secondly, the Security Context of the connection may be temporarily altered for submitted or delivered messages.

The Security Context itself consists of one or more Security Labels defining the sensitivity of interactions that may occur in line with the security policy in force.

Security Context is an argument of the MTS-bind and MTA-bind services.

10.3.2.2 Register Security Element

The Register security element allows the establishment at an MTA of an MTS-user's permissible security labels.

This security element is provided by the Register service. The Register service enables an MTS-user to change arguments, held by the MTS, relating to delivery of messages to that MTS-user.

10.3.2.3 MS-Register Security Element

The MS-Register security element allows the establishment of the MS-user's permissible security labels.

This security element is provided by the MS-Register service. The MS-Register services enables an MS-user to change arguments held by the MS relating to the retrieval of messages to that MS-user.

10.3.3 Data Confidentiality Security Elements

These security elements, based on the use of encipherment, are all concerned with the provision of confidentiality of data passed from one MHS entity to another.

10.3.3.1 Content Confidentiality Security Element

The Content Confidentiality security element provides assurance that the content of the message is protected from eavesdropping during transmission by use of an encipherment security element. The security element operates such that only the recipient and sender of the message know the plaintext message content.

The specification of the encipherment algorithm, the key used, and any other initialising data are conveyed using the Message Argument Confidentiality and the Message Argument Integrity security elements. The algorithm and key are then used to encipher or decipher the message contents.

The Content Confidentiality security element uses the Content Confidentiality Algorithm Identifier, which is an argument of the Message Submission, Message Transfer, and Message Delivery services.

10.3.3.2 Message Argument Confidentiality Security Element

The Message Argument Confidentiality security element provides for the confidentiality, integrity, and, if required, the irrevocability of recipient data associated with a message. Specifically, this data will comprise any cryptographic keys and related data that is necessary for the confidentiality and integrity security elements to function properly, if these optional security elements are invoked.

The security element operates by means of the Message Token. The data to be protected by the Message Argument Confidentiality security element constitutes the Encrypted Data within the Message Token. The Encrypted Data within the Message Token is unintelligible to all MTAs.

The Message Token is an argument of the Message Submission, Message Transfer, and Message Delivery services.

10.3.4 Data Integrity Security Elements

These security elements are provided to support the provision of data integrity, data authentication, and non-repudiation services.

10.3.4.1 Content Integrity Security Element

The Content Integrity security element provides protection for the content of a message against modification during transmission.

This security element operates by use of one or more cryptographic algorithms. The specification of the algorithm(s), the

key(s) used, and any other initialising data are conveyed using the Message Argument Confidentiality and the Message Argument Integrity security elements. The result of the application of the algorithms and key is the Content Integrity Check, which is sent in the message envelope. The security element is only available to the recipient(s) of the message as it operates on the plaintext message contents.

If the Content Integrity Check is protected using the Message Argument Integrity security element then, depending on the prevailing security policy, it may be used to help provide the Non-repudiation of Origin security service.

The Content Integrity Check is an argument of the Message Submission, Message Transfer, and Message Delivery services.

10.3.4.2 Message Argument Integrity Security Element

The Message Argument Integrity security element provides for the integrity, and, if required, the irrevocability of certain arguments associated with a message. Specifically, these arguments may comprise any selection of the Content Confidentiality Algorithm Identifier, the Content Integrity Check, the Message Security Label, the Proof of Delivery Request, and the Message Sequence Number.

The security element operates by means of the Message Token. The data to be protected by the Message Argument Integrity security element constitutes the signed-data within the Message Token.

The Message Token is an argument of the Message Submission, Message Transfer, and Message Delivery services.

10.3.4.3 Message Sequence Integrity Security Element

The Message Sequence Integrity security element provides protection for the sender and recipient of a message against receipt of messages in the wrong order, or duplicated messages.

A Message Sequence Number is associated with an individual message. This number identifies the position of a message in a sequence from one originator to one recipient. Therefore each originator-recipient pair requiring to use this security element will have to maintain a distinct sequence of message numbers. This security element does not provide for initialisation or synchronisation of Message Sequence Numbers.

10.3.5 Non-repudiation Security Elements

There are no specific Non-repudiation security elements defined in Recommendation X.411. The non-repudiation services may be provided using a combination of other security elements.

10.3.6 Security Label Security Elements

These security elements exist to support security labelling in the MHS.

10.3.6.1 Message Security Label Security Element

Messages may be labelled with data as specified in the prevailing security policy. The Message Security Label is available for use by intermediate MTAs as part of the overall security policy of the system.

A Message Security Label may be sent as a message argument, and may be protected by the Message Argument Integrity or the Message Origin Authentication security element, in the same manner as other message arguments.

Alternatively, if both confidentiality and integrity are required, the Message Security Label may be protected using the Message Argument Confidentiality security element. In this case the Message Security Label so protected is an originator-recipient argument, and may differ from the Message Security Label in the message envelope.

10.3.7 Security Management Security Elements

10.3.7.1 Change Credentials Security Element

The Change Credentials security element allows the credentials of an MTS-user or an MTA to be updated.

The security element is provided by the MTS Change Credentials service.

10.3.8 Double Enveloping Technique

Additional protection may be provided to a complete message, including the envelope parameters, by the ability to specify that the content of a message is itself a complete message, i.e., a Double Enveloping Technique is available.

This technique is available though the use of the Content Type argument which makes it possible to specify that the content of a message is an Inner Envelope. This Content Type means that the content is itself a message (envelope and content) for forwarding by the recipient named on the outer envelope to the recipient named on the Inner Envelope.

The Content Type is an argument of the Message Submission, Message Transfer, and Message Delivery services.