INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.411

Corrigendum 2
(12/97)

Corrigendum 3
(09/98)

SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

Message Handling Systems

Information technology – Message Handling Systems (MHS) – Message store: Abstract service definition

Technical Corrigendum 2 & Corrigendum 3

ITU-T Recommendation X.411
Corrigendum 2 & Corrigendum 3
Superseded by a more recent version

(Previously CCITT Recommendation)

Superseded by a more recent version

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.399
MESSAGE HANDLING SYSTEMS	**X.400–X.499**
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999

For further details, please refer to ITU-T List of Recommendations.

ITU-T RECOMMENDATIONS SERIES

Series A	Organization of the work of the ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks and open system communications**
Series Y	Global information infrastructure
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 1999

INTERNATIONAL STANDARD 10021-4

ITU-T RECOMMENDATION X.411

INFORMATION TECHNOLOGY – MESSAGE HANDLING SYSTEMS (MHS) – MESSAGE TRANSFER SYSTEM: ABSTRACT SERVICE DEFINITION AND PROCEDURES

TECHNICAL CORRIGENDUM 2 & CORRIGENDUM 3

Source

ITU-T Recommendation X.411 Corrigendum 2 and Corrigendum 3 were approved on December 12, 1997 and September 25, 1998 respectively. Identical texts are also published as ISO/IEC International Standard 10021-4 Technical Corrigendum 2 and Corrigendum 3 respectively. They are published hereafter as a single consolidated text.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation the term *recognized operating agency (ROA)* includes any individual, company, corporation or governmental organization that operates a public correspondence service. The terms *Administration*, *ROA* and *public correspondence* are defined in the *Constitution of the ITU (Geneva, 1992)*.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, the ITU had/had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Page

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – MESSAGE HANDLING SYSTEMS (MHS) – MESSAGE TRANSFER SYSTEM: ABSTRACT SERVICE DEFINITION AND PROCEDURES

TECHNICAL CORRIGENDUM 2 AND CORRIGENDUM 3

1 Subclause 8.1.1.1.1.2

In 8.1.1.1.1.2 fifth paragraph "If strong-authentication ... ", *append* "or **certificate-selector**".

In 8.1.1.1.1.2 final paragraph first sentence append "and, optionally, additional certificates which provide a certification-path for the initiator's certificate". *Insert after the second sentence* "If the initiator is an MTS-user, the **initiator-certificate** shall contain the **OR-address** of the initiator in the *x400Address* component in its subject alternative name field (see 12.3.2.1 of ITU-T Rec. X.509 | ISO/IEC 9594-8), unless the security-policy provides an alternative binding of the certificate to the MTS-user. If the initiator is the MTS, the **initiator-certificate** shall contain the **MTA-name** of the initiator in an *mta-name* (see A.5.1 of ITU-T Rec. X.402 | ISO/IEC 10021-2) in the *otherName* component in its subject alternative name field, unless the security-policy provides an alternative binding of the certificate to the initiating MTA.". *In the final sentence, delete* "via the Change-credentials abstract-operation, or" *and append* "and, where the initiator has more than one certificate, a **certificate-selector** may be supplied to identify the certificate using any certificate selection criteria specified for certificate match (see 12.7.2 of ITU-T Rec. X.509 | ISO/IEC 9594-8)".

2 Subclause 8.1.1.1.2.2

In 8.1.1.1.2.2 fifth paragraph "If strong-authentication ...", *append to the first sentence* "and, optionally, a **responder-certificate** or **certificate-selector**".

In 8.1.1.1.2.2 append the following paragraph:

The **responder-certificate** is a **certificate** of the responder of the association, generated by a trusted source (e.g. a certification-authority) and, optionally, additional certificates which provide a certification-path for the responder's certificate. It may be supplied by the responder of the association, if the **responder-bind-token** is an **asymmetric-token**. If the responder is an MTS-user, the **responder-certificate** shall contain the **OR-address** of the responder in the *x400Address* component in its subject alternative name field (see 12.3.2.1 of ITU-T Rec. X.509 | ISO/IEC 9594-8), unless the security-policy provides an alternative binding of the certificate to the MTS-user. If the responder is the MTS, the **responder-certificate** shall contain the **MTA-name** of the responder in an *mta-name* (see A.5.1 of ITU-T Rec. X.402 | ISO/IEC 10021-2) in the *otherName* component in its subject alternative name field, unless the security-policy provides an alternative binding of the certificate to the responding MTA. The **responder-certificate** may be used to convey a verified copy of the public-asymmetric-encryption-key (**subject-public-key**) of the responder of the association. The responder's public-asymmetric-encryption-key may be used by the initiator to validate the **responder-bind-token**. If the initiator is known to have, or have access to, the responder's **certificate** (e.g. via the Directory), the **responder-certificate** may be omitted and, where the responder has more than one certificate, a **certificate-selector** may be supplied to identify the certificate using any certificate selection criteria specified for certificate match (see 12.7.2 of ITU-T Rec. X.509 | ISO/IEC 9594-8).

3 Subclause 8.2.1.1.1.26

*In 8.2.1.1.1.26 penultimate paragraph replace "*the message-token provides for non-repudiation-of-origin of the message content*" by "*the **message-token** may provide non-repudiation-of-origin of the message **content** subject to availability of an appropriate Public Key infrastructure*".*

4 Subclause 8.2.1.1.1.28

*In 8.2.1.1.1.28 third paragraph after "*to provide for non-repudiation-of-origin of the message **content***" insert "*subject to availability of an appropriate Public Key infrastructure*".*

5 Subclause 8.2.1.1.2.4

*In 8.2.1.1.2.4 penultimate paragraph after "*An asymmetric **proof-of-submission** may also provide for Non Repudiation of Submission*" insert "*subject to availability of an appropriate Public Key infrastructure*".*

6 Subclause 8.3.1.1.2.2

*In 8.3.1.1.2.2 penultimate paragraph after "*An asymmetric **proof-of-delivery** may also provide for Non Repudiation of Delivery*" insert "*subject to availability of an appropriate Public Key infrastructure*".*

7 Subclause 8.4.1.2

In 8.4.1.2 insert "simple-authentication" *before each occurrence of* "**credentials**" *in the first paragraph.*

8 Subclause 8.4.1.2.1.1

Delete the third paragraph of 8.4.1.2.1.1.

9 Subclause 8.4.1.2.1.2

Delete "(i.e. simple or strong)" *from the second paragraph of 8.4.1.2.1.2.*

10 Subclause 8.5.8

In 8.5.8 replace the bullet on "**recipient-name**" *by:*

> **recipient-name**: either the **OR-address-and-or-directory-name** of the intended-recipient of the **token**; or, for strong authentication in an MTA-bind, the **MTA-name** and optionally the **global-domain-identifier** of the peer MTA (i.e. the recipient of the bind-token); or, for strong authentication in an MTS-bind, the **MTA-name** and optionally the **global-domain-identifier** of the MTA where the token is generated by the MTS-user, or the **OR-address-and-optional-directory-name** of the MTS-user where the token is generated by the MTS; or, for strong authentication in an MS-bind, the **OR-address-and-optional-directory-name** of the MS-user (whether the token is generated by the MS or by the MS-user);

11 Figure 2

In Figure 2 (Part 1 of 29), before "-- Object Identifiers" insert:

-- IPM Information Objects

```
IPMPerRecipientEnvelopeExtensions
      ----
      FROM IPMSInformationObjects { joint-iso-itu-t mhs(6) ipms(1) modules(0)
      information-objects(2) version-1997(1) }
```

In Figure 2 (Part 4 of 29), replace the productions for **`InitiatorCredentials`** *and* **`ResponderCredentials`** *by:*

```
InitiatorCredentials ::= Credentials

ResponderCredentials ::= Credentials

Credentials ::= CHOICE {
      simple Password,
      strong [0] StrongCredentials,
      ... ,
      protected [1] ProtectedPassword }
```

In Figure 2 (Part 4 of 29), replace the production for **`StrongCredentials`** *by:*

```
StrongCredentials ::= SET {
      bind-token [0] Token,
      certificate [1] Certificates OPTIONAL,
      ... ,
      certificate-selector [2] CertificateAssertion OPTIONAL }
```

In Figure 2 (Part 9 of 29), replace the production for **`ChangeCredentialsArgument`** *by:*

```
ChangeCredentialsArgument ::= SET {
      old-credentials [0] Credentials (WITH COMPONENTS { simple }),
      new-credentials [1] Credentials (WITH COMPONENTS { simple }) }
```

In Figure 2 (Part 10 of 29), delete the production for **`Credentials`**.

In Figure 2 (Part 11 of 29), in the production for **`PerRecipientMessageSubmissionExtensions`**, *insert the line* **`"IPMPerRecipientEnvelopeExtensions |"`** *before* **`"PrivateExtensions,"`**.

In Figure 2 (Part 13 of 29), in the production for **`MessageDeliveryExtensions`**, *insert the line* **`"IPMPerRecipientEnvelopeExtensions |"`** *before* **`"PrivateExtensions,"`**.

12 Subclause 12.1.1.1.1.2

In 12.1.1.1.1.2 fourth paragraph "If strong-authentication ...", *append* "or **certificate-selector**".

In 12.1.1.1.1.2 final paragraph first sentence append "and, optionally, additional certificates which provide a certification-path for the initiator's certificate". *Insert after the second sentence* "The **initiator-certificate** shall contain the **MTA-name** of the initiator in an *mta-name* (see A.5.1 of ITU-T Rec. X.402 | ISO/IEC 10021-2) in the *otherName* component in its subject alternative name field (see 12.3.2.1 of ITU-T Rec. X.509 | ISO/IEC 9594-8), unless the security-policy provides an alternative binding of the certificate to the initiating MTA.". *In the final sentence append* "and, where the initiator has more than one certificate, a **certificate-selector** may be supplied to identify the certificate using any certificate selection criteria specified for certificate match (see 12.7.2 of ITU-T Rec. X.509 | ISO/IEC 9594-8)".

13 Subclause 12.1.1.1.2.2

In 12.1.1.1.2.2 fourth paragraph "If strong-authentication ...", *append to the first sentence* "and, optionally, a **responder-certificate** or **certificate-selector**".

In 12.1.1.1.2.2 append the following paragraph:

The **responder-certificate** is a **certificate** of the responder of the association, generated by a trusted source (e.g. a certification-authority) and, optionally, additional certificates which provide a certification-path for the responder's certificate. It may be supplied by the responder of the association, if the **responder-bind-token** is an **asymmetric-token**. The **responder-certificate** shall contain the **MTA-name** of the responder in an *mta-name* (see A.5.1 of ITU-T Rec. X.402 | ISO/IEC 10021-2) in the *otherName* component in its subject alternative name field (see 12.3.2.1 of ITU-T Rec. X.509 | ISO/IEC 9594-8), unless the security-policy provides an alternative binding of the certificate to the responding MTA. The **responder-certificate** may be used to convey a verified copy of the public-asymmetric-encryption-key (**subject-public-key**) of the responder of the association. The responder's public-asymmetric-encryption-key may be used by the initiator to validate the **responder-bind-token**. If the initiator is known to have, or have access to, the responder's **certificate** (e.g. via the Directory), the **responder-certificate** may be omitted and, where the responder has more than one certificate, a **certificate-selector** may be supplied to identify the certificate using any certificate selection criteria specified for certificate match (see 12.7.2 of ITU-T Rec. X.509 | ISO/IEC 9594-8).

14 Figure 4

In Figure 4 (Part 1 of 7), before "-- Object Identifiers" insert:

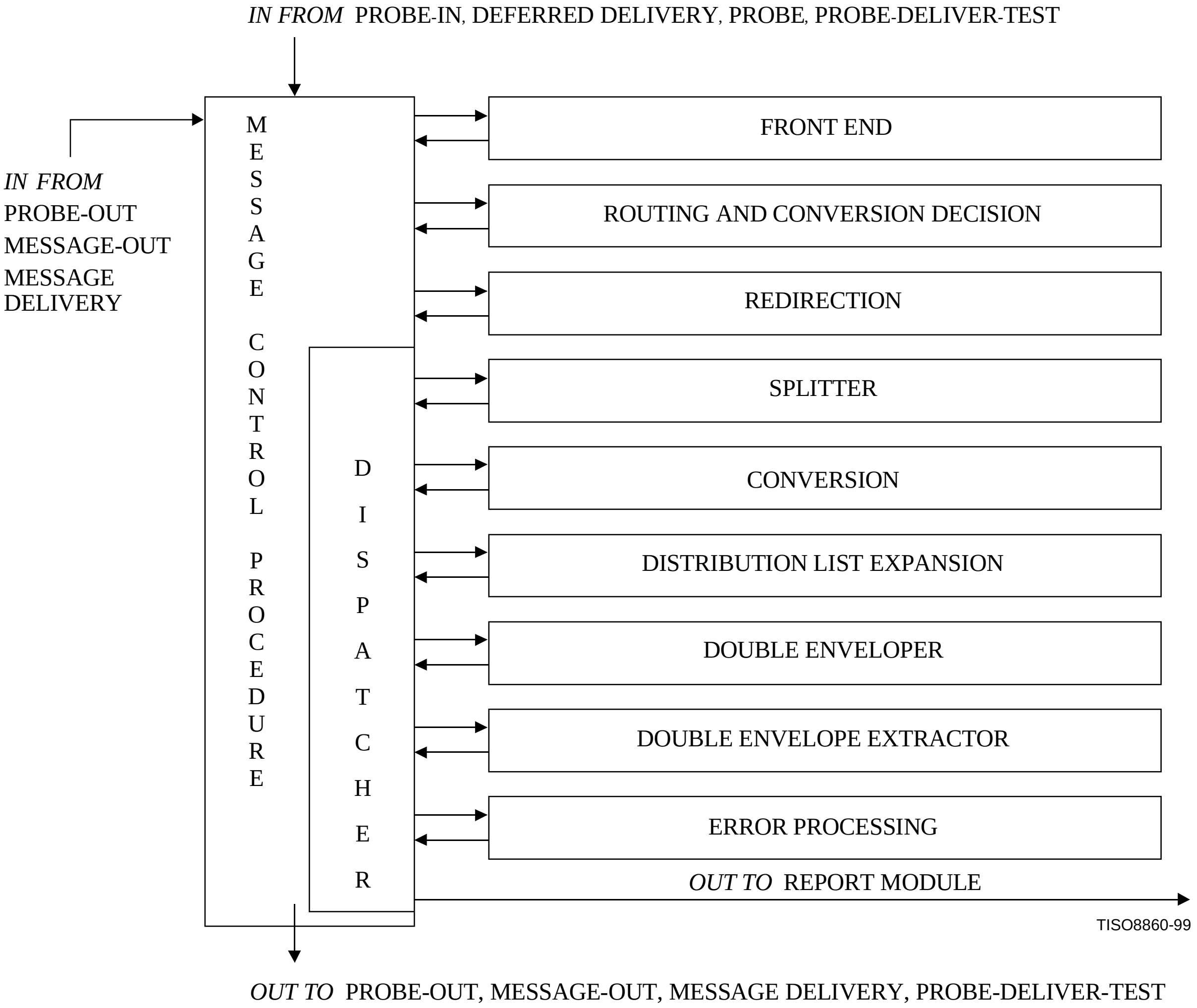
-- IPM Information Objects

```
IPMPerRecipientEnvelopeExtensions
      ----
      FROM IPMSInformationObjects { joint-iso-itu-t mhs(6) ipms(1) modules(0)
      information-objects(2) version-1997(1) }
```

In Figure 4 (Part 3 of 7), in the production for `PerRecipientMessageTransferExtensions`*, insert the line* `"IPMPerRecipientEnvelopeExtensions |"` *before* `"PrivateExtensions,"`.

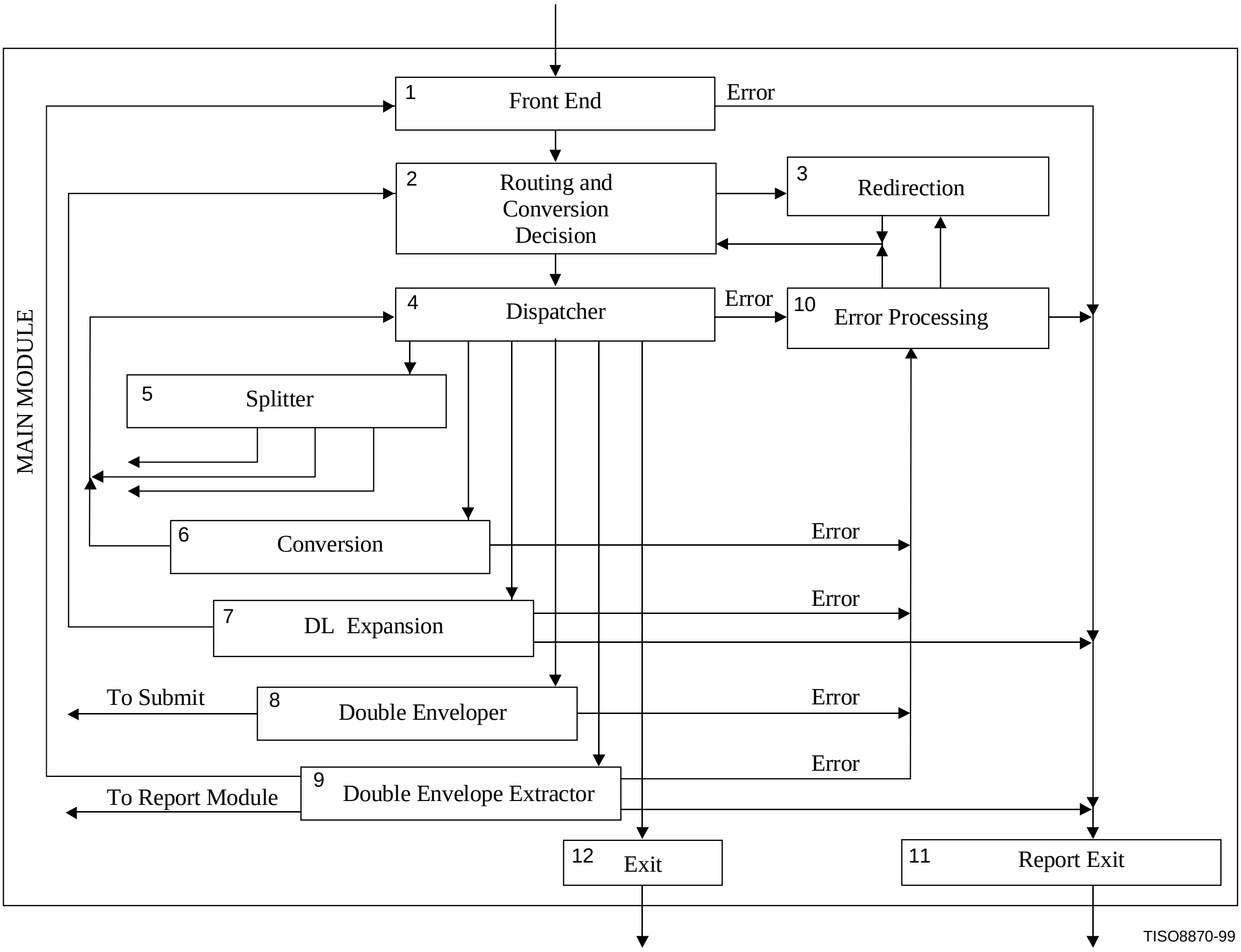
15 Figure 7

Replace Figure 7 by:


IN FROM PROBE-IN, DEFERRED DELIVERY, PROBE, PROBE-DELIVER-TEST
IN FROM
PROBE-OUT
MESSAGE-OUT
MESSAGE DELIVERY
MESSAGE CONTROL PROCEDURE
DISPATCHER
FRONT END
ROUTING AND CONVERSION DECISION
REDIRECTION
SPLITTER
CONVERSION
DISTRIBUTION LIST EXPANSION
DOUBLE ENVELOPER
DOUBLE ENVELOPE EXTRACTOR
ERROR PROCESSING
OUT TO REPORT MODULE
TISO8860-99
OUT TO PROBE-OUT, MESSAGE-OUT, MESSAGE DELIVERY, PROBE-DELIVER-TEST

16 Figure 8

Replace Figure 8 by:



NOTE – Numbers in this figure refer to the numbered steps in the control procedures logic (see 14.3.1.4).

17 Subclause 14.3.1.4

In 14.3.1.4 insert new steps 8) and 9), and renumber subsequent steps accordingly:

8) The Double-enveloper procedure is called if the routing instruction requires the message to be embedded within an **inner-envelope content-type**.

In the case of a successful return the procedure terminates, as the MTA has no further processing to perform on the original message.

In the case of an unsuccessful return, processing continues at step 10 (Error-handler).

9) The Double-envelope-extractor procedure is called if the routing instruction is to extract the inner envelope from the **content**.

Upon successful return of an extracted message or probe, processing of the extracted message or probe resumes at step 1. Upon successful return of an extracted report, processing of the extracted report continues as specified in 14.4.1. In addition in each case, processing of the report instructions on the original message continues at step 11.

Upon an unsuccessful return, processing continues at step 10 (Error-handler).

18 Subclause 14.3.4.4

In 14.3.4.4 renumber steps 6) and 7) as 7) and 8), and insert new step 6):

6) If the recipient **OR-name** identifies a double-envelope-extractor at this MTA and the **content-type** of the message is **inner-envelope**, then the procedure returns a routing instruction to extract the inner envelope from the **content**. The procedure then terminates.

Insert a new second paragraph in the former step 7) now renumbered 8):

If the security-policy specifies that a double envelope is required for the identified next hop and the **content-type** of the message is not **inner-envelope**, then the procedure returns a routing instruction to embed the current message within the **content** of a new message using the procedure specified in 14.3.13. The procedure then terminates.

19 Subclause 14.3.12.4

In 14.3.12.4 bullet 4) b), append to the second sentence ", and **terminal-type** set to the value *g3-facsimile*".

Insert a new bullet 4) c):

c) telex-delivery: Values of **country-name**, **administration-domain-name**, and optionally **private-domain-name** are configured. The **OR-address** is constructed from the configured components and a **network-address** obtained from the values of the telexNumber and countryCode components of the *telexNumber* Directory attribute, a **terminal-identifier** obtained from the value of the answerback component of the *telexNumber* Directory attribute, and **terminal-type** set to the value *telex*. This is considered to satisfy the **telex-delivery** method.

Insert new subclauses 14.3.13 and 14.3.14, as follows:

14.3.13 Double-enveloper Procedure

This procedure takes a message, probe or report, and places the entire object in the content of a new message which is addressed to a remote double-envelope-extractor, and submitted as a new message which has an inner-envelope content-type.

14.3.13.1 Arguments

1) A message, probe or report which is to be wrapped in an outer-envelope.

2) The **OR-name** of the remote double-envelope-extractor.

3) The **OR-name** of this double-enveloper.

4) The security services to be applied to protect the inner-envelope content and either specific algorithm information or algorithm preferences for these (for content-confidentiality, message-token-encrypted-data, message-token-signed-data, and message-origin-authentication-check).

14.3.13.2 Results

None, as the MTA has no further processing to perform on the original message.

NOTE – There are two output events from this procedure: one is submission of a new message containing the inner-envelope, and the second is a record of sufficient information to enable the double-enveloper to construct a non-delivery report on the original message in the event that it receives a non-delivery report on the new message.

14.3.13.3 Errors

An indication of a security-error if a requested service could not be provided.

NOTE – The occurrence of such a security-error may indicate a configuration error (where a configured algorithm, or the MTA's private-key for it, is unavailable), or an error in the certificate of the double envelope extractor.

14.3.13.4 Procedure Description

The entire MTS-APDU containing the subject message, probe or report, is placed in the content of a new message, whose originator is the **OR-name** of this double-enveloper and whose recipient is the **OR-name** of the remote double-envelope-extractor. The originator-report-request for this recipient is set to report, and the content-type is set to inner-envelope.

If algorithm preferences are specified for the requested security services and the directory-name is present within the **OR-name** of the remote double-envelope-extractor, then that Directory entry is read to obtain its Supported Algorithms and User Certificate attribute. The algorithm highest in the preference order which is supported by both this MTA and by the remote double-envelope-extractor is selected for each requested security service (i.e. content-confidentiality, message-token-encrypted-data, message-token-signed-data, and message-origin-authentication-check). The algorithm-information contains an algorithm-identifier, and, optionally, information to select an appropriate Certificate for that algorithm for the originator or recipient or both (depending on the requirements of the algorithm). Certificate-selector information is required only if the Directory entry may contain more than one Certificate for the identified algorithm. If the directory-name is not present, then the highest preference is selected, and local configuration of the remote double-envelope-extractor's public encryption key will be required.

The content is encrypted using the selected (or configured) content-confidentiality-algorithm which may be an asymmetric algorithm, or if this is a symmetric algorithm then a random content-confidentiality-key is generated and used to encrypt the content, and a message-token created with this key encrypted using the selected (or configured) message-token-encryption-algorithm (which must be an asymmetric algorithm) and signed using the selected (or configured) message-token-signature-algorithm (which must be a signature algorithm). The public key that is used with the asymmetric encryption algorithm is found by using the algorithm-identifier and recipient-certificate-selector to select an appropriate Certificate from the Directory entry.

If message-origin-authentication is specified, then a message-origin-authentication-check is computed containing a signature of the encrypted content using the selected (or configured) algorithm together with the private key of this MTA corresponding to its Certificate identified by originator-certificate-selector.

The new message containing the inner-envelope is submitted, and a record is made of its message-submission-identifier together with sufficient information to enable the double-enveloper to construct a non-delivery report on the original message in the event that it receives a non-delivery report on the new message.

14.3.14 Double-envelope-extractor Procedure

This procedure takes a message which has an inner-envelope content-type and extracts from its content a message, probe or report which the MTA then processes as if it had been transferred normally.

14.3.14.1 Arguments

A message which has an inner-envelope content-type.

14.3.14.2 Results

A message, probe or report.

14.3.14.3 Errors

An indication of a security-error if verification of a security argument failed.

In response to a probe, or to a message with a content-type other than inner-envelope, a report generation instruction unable-to-transfer unrecognised-OR-name.

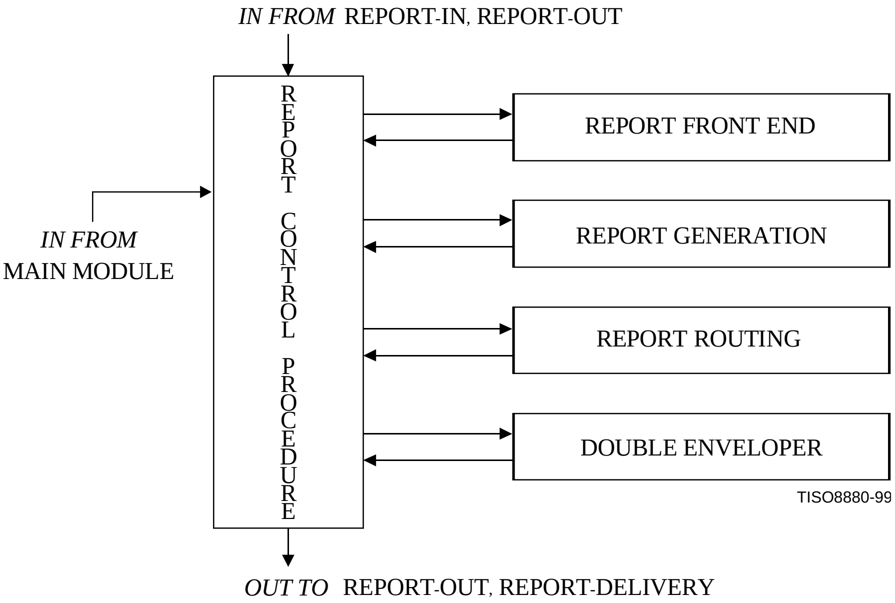
14.3.14.4 Procedure Description

The message-delivery procedure (see 14.7.1) is followed (as appropriate), including generation of a report instruction where requested.

If message-origin-authentication-check is present, then this is verified. The content is decrypted, and the message, probe or report is extracted and passed to the front-end (or report-front-end) procedure.

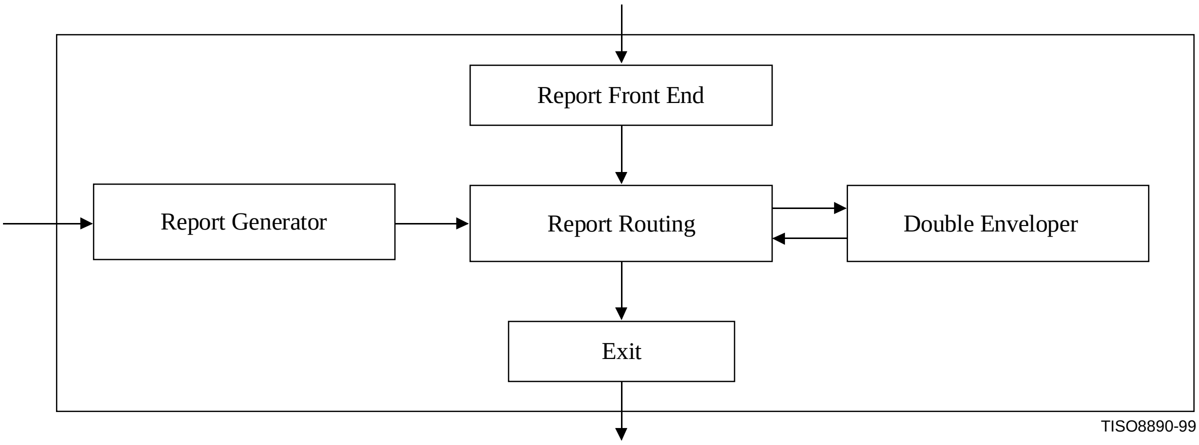
20 Figure 10

Replace Figure 10 by:



21 Figure 11

Replace Figure 11 by:



22 Subclause 14.4.4.4

In 14.4.4.4, insert a new second paragraph in step 1) a):

If the security-policy specifies that a double envelope is required for the identified next hop, then the procedure returns an instruction to embed the report within the **content** of a new message using the procedure specified in 14.3.13. The procedure then terminates.

In 14.4.4.4, insert a new step 1) e):

e) If the **report-destination-name** identifies a double-enveloper at this MTA, then the procedure in 14.4.5 applies, and the procedure terminates. Any resultant new report is processed from the start of this procedure.

Insert new subclause 14.4.5, as follows:

14.4.5 Double-enveloper Procedure

This procedure takes a report on a message (created by this MTA) which had an inner-envelope content-type, and if it is a non-delivery report then it substitutes a non-delivery report on the message that was in the inner-envelope.

14.4.5.1 Arguments

A report.

14.4.5.2 Results

Another report if the argument is a non-delivery report, or none otherwise.

14.4.5.3 Errors

None.

14.4.5.4 Procedure Description

If the report is a non-delivery report, then the record of submitted double-enveloped messages is read to obtain the information necessary to create a non-delivery report on the inner-envelope message. This new non-delivery report replaces the non-delivery report on the outer-envelope.

If the report is a delivery report, then no further transfer of it is required.

In either case, the record of submitted double-enveloped messages is augmented with information about the delivery or non-delivery report. The MTA may implement an additional procedure, activated by expiry of a timer, to generate a non-delivery report on the inner-envelope message if no delivery report has been received on the outer-envelope message.

23 Subclause 14.5.1.4

In 14.5.1.4 insert the following paragraphs after the first sentence of bullet 2):

If the **initiator-credentials** contain **strong-credentials**, the signature of the initiator-bind-token is verified using the public key from the MTS-user's **certificate** for the identified signature algorithm. The MTS-user's **certificate** may be included in initiator-credentials in the Bind argument, or identified by a **certificate-selector** and, if not already available to the MTA, obtained from the MTS-user's User Certificate attribute in the Directory. The validity of the **certificate** and its certification-path are also verified. Additionally, the Directory name from the subject field of that Certificate is verified to be that of the MTS-user. The **OR-name** in the subject-alternative-name field of that Certificate is verified to correspond to the **OR-name** of the MTS-user, and to correspond to the **OR-name** present in the initiator-name field of Bind. The mta-name and global-domain-identifier within initiator-bind-token are verified as being those of this MTA. The Time in the token is compared with the current time to ensure that the validity period of the token acceptable to this MTA has not expired.

The responder-bind-token is generated by using the same signature algorithm (unless a preferred alternative is known to be supported by the MTS-user) and this MTA's private key to sign a token which comprises the algorithm-identifier for the signature algorithm, the **OR-name** of the MTS-user, the current time, and a random number as the bind-token-signed-data. This responder-bind-token together with either the **certificate-selector** or the **certificate** (and the additional certificates which provide its certification-path) for this MTA's public key for this algorithm form the responder-credentials in the Bind result.

24 Subclause 14.5.3.4

In 14.5.3.4 append the following paragraph to bullet 1):

If the **initiator-credentials** is to contain **strong-credentials**, the MTA selects a signature algorithm which is supported by the MTS-user, and uses this algorithm to sign an initiator-bind-token comprising the algorithm-identifier for this algorithm, the **OR-name** of the MTS-user, the current time, and a random number as the bind-token-signed-data. This initiator-bind-token together with either the **certificate-selector** or the **certificate** (and the additional certificates which provide its certification-path) for this MTA's public key for this algorithm form the initiator-credentials in the Bind argument.

In 14.5.3.4 insert the following paragraph after the second sentence of bullet 3):

When the Bind result is received, the signature of the responder-bind-token is verified using the public key from the MTS-user's **certificate** for the identified signature algorithm. (This might be a different signature algorithm to the one used to sign the initiator-bind-token.) The MTS-user's **certificate** may be included in the Bind result, or identified by a **certificate-selector** and, if not already available to the MTA, obtained from the MTS-user's User Certificate attribute in the Directory. The validity of the **certificate** and its certification-path are also verified. Additionally, the Directory name from the subject field of that **certificate** is verified to be that of the MTS-user (i.e. that the responding MTS-user is the intended target of the Bind). The **OR-name** in the subject-alternative-name field of that **certificate** is verified to correspond to the **OR-name** of the MTS-user, and to correspond to the **OR-name** present in the responder-name field of Bind result. The mta-name and global-domain-identifier within responder-bind-token are verified as being those of this MTA. The Time in the token is compared with the current time to ensure that the validity period of the token acceptable to this MTA has not expired.

25 Subclause 14.9.1.4

In 14.9.1.4 insert the following paragraphs after the first sentence of bullet 2):

If the **initiator-credentials** contain **strong-credentials**, the signature of the initiator-bind-token is verified using the public key from the initiating MTA's **certificate** for the identified signature algorithm. The initiating MTA's **certificate** may be included in initiator-credentials in the Bind argument, or identified by a **certificate-selector** and, if not already available to the MTA, obtained from the initiating MTA's User Certificate attribute in the Directory. The validity of the **certificate** and its certification-path are also verified. Additionally, the Directory name from the subject field of that Certificate is verified to be that of the initiating MTA. The mta-name in the subject-alternative-name field of that Certificate is verified to correspond to the calling MTA's MTA Name and Global Domain Identifier, and to correspond to the mta-name present in the initiator-name field of Bind. The mta-name and global-domain-identifier within initiator-bind-token are verified as being those of this MTA. The Time in the token is compared with the current time to ensure that the validity period of the token acceptable to this MTA has not expired.

The responder-bind-token is generated by using the same signature algorithm (unless a preferred alternative is known to be supported by the initiator) and this MTA's private key to sign a token which comprises the algorithm-identifier for the signature algorithm, the mta-name and global domain identifier of the initiating MTA, the current time, and a random number as the bind-token-signed-data. This responder-bind-token together with either the **certificate-selector** or the **certificate** (and the additional certificates which provide its certification-path) for this MTA's public key for this algorithm form the responder-credentials in the Bind result.

26 Subclause 14.9.3.4

In 14.9.3.4 append the following paragraph to bullet 1):

If the **initiator-credentials** is to contain **strong-credentials**, the MTA selects a signature algorithm which is supported by the target MTA, and uses this algorithm to sign an initiator-bind-token comprising the algorithm-identifier for this algorithm, the mta-name and global domain identifier of the target MTA, the current time, and a random number as the bind-token-signed-data. This initiator-bind-token together with either the **certificate-selector** or the **certificate** (and the additional certificates which provide its certification-path) for this MTA's public key for this algorithm form the initiator-credentials in the Bind argument.

In 14.9.3.4 insert the following paragraph after the second sentence of bullet 3):

When the Bind result is received, the signature of the responder-bind-token is verified using the public key from the responding MTA's **certificate** for the identified signature algorithm. (This might be a different signature algorithm to the one used to sign the initiator-bind-token.) The responding MTA's **certificate** may be included in the Bind result, or identified by a **certificate-selector** and, if not already available to the MTA, obtained from the responding MTA's User Certificate attribute in the Directory. The validity of the **certificate** and its certification-path are also verified. Additionally, the Directory name from the subject field of that **certificate** is verified to be that of the target MTA (i.e. that the responding MTA is the intended target of the Bind). The mta-name in the subject-alternative-name field of that **certificate** is verified to correspond to the target MTA's MTA Name and Global Domain Identifier, and to correspond to the mta-name present in the responder-name field of Bind result. The mta-name and global-domain-identifier within responder-bind-token are verified as being those of this MTA. The Time in the token is compared with the current time to ensure that the validity period of the token acceptable to this MTA has not expired.