INTERNATIONAL STANDARD ISO/IEC 10021-5:1996

TECHNICAL CORRIGENDUM 2
TECHNICAL CORRIGENDUM 3

Published 2000-05-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

TECHNICAL CORRIGENDUM 2
TECHNICAL CORRIGENDUM 3

Technologies de l'information — Systèmes de messagerie (MHS): Dépôt de message: Définition de service abstrait

RECTIFICATIF TECHNIQUE 2
RECTIFICATIF TECHNIQUE 3

Technical Corrigenda 2 and 3 to International Standard ISO/IEC 10021-5:1996 were prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

ICS 35.240.20

Ref. No. ISO/IEC 10021-5:1996/Cor.2:2000(E)
ISO/IEC 10021-5:1996/Cor.3:2000(E)

Printed in Switzerland

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – MESSAGE HANDLING SYSTEMS (MHS): MESSAGE STORE: ABSTRACT SERVICE DEFINITION

TECHNICAL CORRIGENDUM 2 AND CORRIGENDUM 3

1 Subclause 6.5.2

Append the following to 6.5.2, bullet b):

This component is disregarded in the case where the auto-action-type supports only a single registration.

In 6.5.2, bullet c), change "(O)" *to* "(C)".

Append the following to 6.5.2, bullet c):

This shall be present if the auto-action-type identifies an auto-action for which a registration parameter is defined, and is absent otherwise.

2 Subclause 7.1.1

In 7.1.1, bullet b) second paragraph third sentence "If strong-authentication ...", *append* "or certificate-selector". *In the fourth sentence replace* "initiator-bind-token and initiator-certificate" *by* "initiator-bind-token, initiator-certificate and certificate-selector". *Insert after the fourth sentence* "The initiator-certificate shall contain the OR-address of the MS-user 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 MS-user.".

3 Subclause 7.1.2

In 7.1.2, in the ASN.1 replace:

```
additional-capabilities [9] MSExtensions OPTIONAL,
```

by:

```
bind-result-extensions [9] MSExtensions OPTIONAL,
```

In 7.1.2, bullet a) second paragraph third sentence "If strong-authentication ...", *append* ", and, optionally, a responder-certificate or certificate-selector". *In the fourth sentence replace* "responder-bind-token is" *by* "responder-bind-token, responder-certificate and certificate-selector are". *Insert after the fourth sentence* "The responder-certificate shall contain the OR-address of the MS 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 MS.".

Replace bullet h) by:

h) **Bind-result-extensions** (C): This parameter allows for future general and content-specific extensions to MS-bind-result. If the MS supports one or more additional capabilities whose specification defines an MS-extension to indicate that capability, the specified extensions shall be present. MS-extensions to indicate additional capabilities defined in this Service Definition are listed in Annex F; further extensions may be defined in future editions of this Service Definition, in content-specific Specifications, or to indicate proprietary capabilities.

4 Subclause 8.1.6

In 8.1.6, replace item d) with the following:

d) **MS-submission-extensions** (O): This component allows for general and content-specific extensions to MS-submission-options. The Specification for a given content-type defines its use of this component. In the absence of the component, no MS-submission-extensions are specified. This Service Definition defines the following extension:

– **Originator-token** (O): This extension is used where the submitted message contains a message-token which contains encrypted-data that has been encrypted such that it cannot subsequently be decrypted by the originator. This extension enables the originator to supply a message-token constructed as if the originator were a recipient of the message, to be stored in the submitted-message entry but not submitted to the MTS. Subsequently, the originator may retrieve this information and use it to recover the original message.

```
originator-token MS-EXTENSION ::= {
      OriginatorToken IDENTIFIED BY id-ext-originator-token}

OriginatorToken ::= MessageToken
      (CONSTRAINED BY {-- Must contain an asymmetric-token with an
                       -- encrypted-data
component --}
```

The **originator-token** contains a *message-token* argument of the Message-submission abstract-operation (see 8.2.1.1.1.26 of ITU-T Rec. X.411 | ISO/IEC 10021-4) which contains an *encrypted-data* component that is encrypted using the public key of the message originator.

NOTES

1 When storage-on-submission is used, the originator retains a copy of the message in the MS, but is not treated as a recipient in the message submission envelope. This extension provides the originator with the security arguments that are encrypted on a per-recipient basis for the conventional recipients of the message. Note that content-integrity-check does not need to be duplicated here, as it is only a signature, and so the originator is implicitly able to use any of the values provided for the other recipients.

2 If Content Confidentiality is provided using a symmetric encryption algorithm with a content-confidentiality-key (session key) which is itself encrypted such that it requires each recipient's private key to decrypt it, then the message's originator would have no means of decrypting the copy of the message as stored in the MS on submission. This MS-submission-extension enables the MS-user to supply a value with the submitted message, which is stored in the submitted-message entry but is not included in the message submitted to the MTS. This contains the session key for the message, encrypted with the public key of the submitting MS-user. When the MS-user subsequently retrieves the submitted-message, his private key may be used to decrypt the session key, and hence decrypt the message.

3 Where Content Confidentiality is provided by use of a symmetric algorithm, and a method other than the message-token is used to distribute the key, then the originating MS-user must employ a different mechanism to retain the key and so enable subsequent decryption of the stored-message.

4 Where Content Confidentiality is provided directly by use of an asymmetric algorithm, it is unlikely that storage on submission will be useful, except where the key pair is shared between users, including the originating MS-user, who thus has access to both public and private keys.

5 Subclause 8.2.5.1

In 8.2.5.1 and Annex B, in the production for **`Register-MSArgument`**, *replace the lines for old and new credentials by:*

```
    old-credentials          [0]  Credentials (WITH COMPONENTS { simple }),
    new-credentials          [1]  Credentials (WITH COMPONENTS { simple })}
OPTIONAL,
```

6 Subclause 8.2.7. 2

In 8.2.7.2, replace bullet a) with the following, preserving the Note:

a) **Entries-modified** (C): This identifies the entries selected for modification. It is present if the selector component was present in the modify-argument, and at least one entry was selected for modification. It is absent otherwise.

7 Table 2

In Table 2, in the row Message-identifier, in columns submitted-message entry and submitted-probe entry, change "P" *to* "C".

In Table 2, replace the row for "Message-token" by:

Attribute-type name	Presence in:						Support level by MS		Single/ multi-valued	Available for List	Available for Summarize
	delivered-message entry	delivered-report entry	returned-content entry	submitted-message entry*	submitted-probe entry*	draft-message entry*	Stored-message entry-class	Message-log entry-class*			
Message-token*	C	–	–	C	–	C	O	O	S	Y	N

8 Subclause 11.2.34 (renumbered to 11.2.35 by Amendment 1)

In 11.2.34, paragraph 1, after the second sentence insert:

Where Message-submission or Probe-submission fails, the attribute is absent from any entry created in the Message-log entry class. Where Message-submission or Probe-submission succeeds, the attribute is present in any entry created in the Stored-message entry class.

9 Subclause 11.2.40 (renumbered to 11.2.41 by Amendment 1)

Replace the first paragraph of clause 11.2.40 by:

This general attribute contains the *message-token* argument of the Message-delivery abstract-operation or the *originator-token* argument of the Message-submission abstract-operation. When present in submitted-message entries, this attribute contains an *encrypted-data* component that is encrypted using the public key of the message originator rather than that of any recipient. It may be generated by the originator of the message. See 8.2.1.1.1.26 of ITU-T Rec. X.411 | ISO/IEC 10021-4 and 8.1.6.

10 Table 4

In Table 4, replace the row for "Message-token" by:

Attribute-type name	Single /multi valued	Source parameter	Source generated by	Generation rules
Message-token	S	message-token	Md	The attribute-value is the value of the source parameter.
		originator-token	Ms	The attribute-value is the value of the source parameter.

11 Clause 13

Append the following to clause 13 (before 13.1):

Table 5 summarizes the registration and log generation capabilities of each of the general-auto-actions in the following respects:

– whether the auto-action may be registered by means of the Register-MS abstract-operation;

– whether multiple registrations are permitted;

– whether a registration parameter is defined for the auto-action;

– whether the execution of the auto-action may cause the generation of an entry in the Auto-action-log.

NOTE – If the register-MS-argument contains a registration-status-request for auto-action-registrations, then all auto-actions currently in effect (whether registered by means of Register-MS or by subscription) are reported in the registered-information argument of register-MS-result.

Table 5 – Summary of general-auto-action registration and logging capabilities

Auto-action-type	Register-MS	Multiple registrations	Registration parameter	Auto-action-log
Auto-alert	Y	Y	Y	Y
Auto-modify	Y	Y	Y	Y
Auto-correlate-reports	N	N	N	N
Auto-delete	Y	N	N	Y

12 Subclause 16.1.1

In 16.1.1, delete item f), renumber existing item c) as d), and insert a new item c):

c} If a security-context is specified for the abstract-association, then the message-security-labels of the selected entries are checked against the security-context. Any entry bearing a message-security-label not permitted by the current security-context is eliminated from the set of selected entries. If no entries remain, the MS returns a Summarize result and the procedure terminates. If the requested operation is barred by the security-policy, the Summarize abstract-operation is abandoned and a security error is indicated.

13 Subclause 16.1.2

In 16.1.2, delete item e), renumber existing items c)-d) as d)-e), and insert a new item c):

c) If a security-context is specified for the abstract-association, then the message-security-labels of the selected entries are checked against the security-context. Any entry bearing a message-security-label not permitted by the current security-context is eliminated from the set of selected entries. If no entries remain, the MS returns a List result and the procedure terminates. If the requested operation is barred by the security-policy, the List abstract-operation is abandoned and a security error is indicated.

14 Subclause 16.1.3

In 16.1.3, delete item f), renumber existing items c)-e) as d)-f), and insert a new item c):

c) If a security-context is specified for the abstract-association and the Fetch argument specifies a specific entry (using the Precise parameter), then the message-security-label of that entry is checked against the security-context. If the entry bears a message-security-label not permitted by the current security-context, then the Fetch abstract-operation is abandoned and a security error is indicated.

If a security-context is specified for the abstract-association and the Fetch argument specifies a set of entries (using the Search parameter), then the message-security-labels of the selected entries are checked against the security-context. Any entry bearing a message-security-label not permitted by the current security-context is eliminated from the set of selected entries. If no entries remain, the MS returns a Fetch result and the procedure terminates. If the requested operation is barred by the security-policy, the Fetch abstract-operation is abandoned and a security error is indicated.

15 Subclause 16.1.4

In 16.1.4, insert the following item c) and renumber items c)-d) as d)-e):

c) If a security-context is specified for the abstract-association and the Delete argument specifies specific entries (using the Sequence-numbers parameter), then the message-security-labels of those entries are checked against the security-context. If any entry bears a message-security-label not permitted by the current security-context, then the Delete abstract-operation is abandoned and a security error is indicated.

If a security-context is specified for the abstract-association and the Delete argument specifies a set of entries (using the Selector parameter), then the message-security-labels of the selected entries are checked against the security-context. Any entry bearing a message-security-label not permitted by the current security-context is eliminated from the set of selected entries. If no entries remain, the MS returns a Delete result and the procedure terminates. If the requested operation is barred by the security-policy, the Delete abstract-operation is abandoned and a security error is indicated.

16 Subclause 16.1.5

In 16.1.5, renumber item d) as item b), replacing "may only permit user-security-labels to be changed" *with* "may permit user-security-labels to be changed only" *and renumber existing items b)-c) as c)-d).*

17 Subclause 16.1.6

In 16.1.6, insert the following item c) and renumber items c)-d) as d)-e):

c) If a security-context is specified for the abstract-association and the Modify argument specifies specific entries (using the Specific-entries parameter), then the message-security-labels of those entries are checked against the security-context. If any entry bears a message-security-label not permitted by the current security-context, then the Modify abstract-operation is abandoned and a security error is indicated.

If a security-context is specified for the abstract-association and the Modify argument specifies a set of entries (using the Selector parameter), then the message-security-labels of the selected entries are checked against the security-context. Any entry bearing a message-security-label not permitted by the current security-context is eliminated from the set of selected entries. If no entries remain, the MS returns a Modify result and the procedure terminates. If the requested operation is barred by the security-policy, the Modify abstract-operation is abandoned and a security error is indicated.

18 Subclause 16.1.7

In 16.1.7, delete item (d), renumber existing items (a)-(c) as (b)-(d), and insert the following item (a):

a) If a security-context is specified for the abstract-association, then the message-security-labels of the delivered message or report are checked against the security-context. If the entry bears a message-security-label not permitted by the current security-context, or other security restrictions apply, the action taken shall be defined by the security-policy in force.

19 Subclause 16.2.1

In 16.2.1, move existing bullet j) to become a new bullet a) and renumber a)-i) accordingly. Replace bullets e) and f) [here renumbered f) and g)] with the following:

f) The MS invokes the Message-submission abstract-operation over its abstract-association with the MTS, and creates an entry in the Submission-log entry-class (if subscribed to by the MS-user). If the submission-options parameter (or its registered default) requests the creation of an entry in the Submission entry-class, then that entry is created at the same time. The mandatory and optional attribute-types for submitted-message entries of the Submission and Submission-log entry-classes are indicated in Table 2. If the submission-options parameter contain an originator-token parameter, then the MS shall create a message-token attribute in the Submission and Submission-log entry-classes containing that value.

g) If the Message-submission is successful, and the Auto-correlate reports auto-action is subscribed to by the MS-user, then the MS generates the correlation attributes indicated in 13.3. If the Message-submission is unsuccessful, the MS deletes the newly created entry in the Submission entry-class and attaches an MS-submission-error to the Submission-log entry to record the error.

20 Subclause 16.2.2

In 16.2.2, move existing bullet h) to become a new bullet a) and renumber a)-g) accordingly. Replace bullets c) and d) [here renumbered d) and e)] with the following:

d) The MS invokes the Probe-submission abstract-operation over its abstract-association with the MTS, and creates an entry in the Submission-log entry-class (if subscribed to by the MS-user). If the submission-options parameter (or its registered default) requests the creation of an entry in the Submission entry-class, then that entry is created at the same time. The mandatory and optional attribute-types for submitted-probe entries of the Submission and Submission-log entry-classes are indicated in Table 2.

g) If the Probe-submission is successful, and the Auto-correlate reports auto-action is subscribed to by the MS-user, then the MS generates the correlation attributes indicated in 13.3. If the Probe-submission is unsuccessful, the MS deletes the newly created entry in the Submission entry-class and attaches an MS-submission-error to the Submission-log entry to record the error.

21 Annex A

*In Annex A (as modified by Technical Corrigendum 1), insert the following after the line beginning "**id-ext-modify-retrieval-status**":*

```
id-ext-originator-token   ID ::= {id-ext 3}
```

22 Annex B

*Add "**MessageToken,**" to the imports from MTSAbstractService (data-types).*

*Add "**id-ext-originator-token,**" to the imports from MSObjectIdentifiers on the second page.*

In the ASN.1 for **MSBindResult** *on the fifth page replace:*

```
additional-capabilities [9] MSExtensions OPTIONAL,
```

by:

```
bind-result-extensions [9] MSExtensions OPTIONAL,
```

Insert the following after the production for MSSubmissionOptions on the seventh page:

```
originator-token MS-EXTENSION ::= {
      OriginatorToken IDENTIFIED BY id-ext-originator-token}

OriginatorToken ::= MessageToken
      (CONSTRAINED BY {-- Must contain an asymmetric-token with an encrypted-data component --} )
```