INTERNATIONAL STANDARD ISO/IEC 10021-7:1997

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): Interpersonal messaging system

TECHNICAL CORRIGENDUM 2
TECHNICAL CORRIGENDUM 3

Technologies de l'information — Systèmes de messagerie (MHS): Système de messagerie entre personnes

RECTIFICATIF TECHNIQUE 2
RECTIFICATIF TECHNIQUE 3

Technical Corrigenda 2 and 3 to International Standard ISO/IEC 10021-7:1997 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 10021-7:1997/Cor.2:2000(E)
ISO/IEC 10021-7:1997/Cor.3:2000(E)

Printed in Switzerland

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – MESSAGE HANDLING SYSTEMS (MHS): INTERPERSONAL MESSAGING SYSTEM

TECHNICAL CORRIGENDUM 2 AND CORRIGENDUM 3

1 Subclause 7.2.6

In 7.2.6 delete "heading" *in the first sentence, and append to the first paragraph:* "It may be present as a Heading field, or alternatively as an equivalent MTS extension that may be present in the per-recipient-message-submission-extensions field of a message-submission envelope and in the message-delivery-extensions field of a message-delivery envelope.". *Insert after the existing ASN.1 productions:*

```
blind-copy-recipients EXTENSION  ::= {
      BlindCopyRecipientsField,
      IDENTIFIED BY standard-extension:41 }
```

Insert at the end of 7.2.6:

NOTE – When submitting through an MS which provides Storage on Submission, the use of the alternative envelope encoding will result in a single submitted-message entry instead of an additional submitted-message entry for each blind copy recipient, which gives greater efficiency of submission, better correspondence between the user's perception of submitting one IPM and the resultant stored entry, and improved correlation of reports and notifications for blind copy recipients with the submitted-message entry. However, if the blind copy recipient's MS or UA conforms to an earlier version of this specification, then use of the alternative envelope encoding will result in the absence of requested notifications and the recipient being aware only implicitly rather than explicitly that he was a blind copy recipient.

2 Subclause 7.2.13

Replace the ASN.1 production for **`ReplyRecipientsSubfield`** *in 7.2.13 by:*

```
ReplyRecipientsSubfield ::= ORDescriptor (WITH COMPONENTS{...,
formal-name PRESENT})
```

3 Subclause 7.4.7

In 7.4.7 bullet b) second sentence "The presence ... is discouraged", *replace* "The presence" *by* "For a delivered message, the presence".

Add a new final paragraph to 7.4.7 (before the Notes):

If the forwarded IPM represents a previously submitted IPM (rather than a delivered IPM) then a simulated delivery-envelope may be constructed to contain message-submission-time; the originator-name and this-recipient-name components of this envelope each contain the OR-address of the IPM's originator.

4 Subclause 7.4.11

In 7.4.11 number the existing Example as Example 1 and insert after it:

EXAMPLE 2 – The extended EITs for the Basic Multilingual Plane of ISO/IEC 10646-1 (16-bit encoding without restrictions on combining characters) are {id-cs-eit-authority 176} for the G0 set, {id-cs-eit-authority 1} for the basic C0 set, and (if required) {id-cs-eit-authority 77} for the C1 set of ISO 6429.

5 Subclause 7.4.12

Delete the last 4 lines of the ASN.1 comment against FileTransferData in 7.4.12.

6 Subclause 7.4.12.7

In 7.4.12.7 second paragraph, second sentence: delete the words "a sequence of Externals to convey".

Delete the 3rd sentence of the 2nd paragraph of clause 7.4.12.7 ("The encoding of each data value in the external is described in 7.4.12"), *and replace by:* "Where the file content comprises more than one data value, each value is placed in a separate External in the FileTransferData".

Delete the last paragraph of clause 7.4.12.7 ("The encoding shall be based...") *and replace by:*

For the purposes of FileTransferData, this Specification places additional restrictions on the encoding of the External ASN.1 type, excluding some of the implementation options permitted by the ASN.1 Basic Encoding Rules in 8.18 of ITU-T Rec. X.690 | ISO/IEC 8825-1:

a) If the data value is a single ASN.1 type, the single-ASN1-type choice shall be used; the options to place a BER-encoding of the data value in the octet-aligned or arbitrary choices are excluded.

b) If the data value comprises an integral number of octets, but is not a single ASN.1 type, the octet-aligned choice shall be used; the option to place octet-aligned data in the arbitrary choice is excluded.

A data value comprising a single ASN.1 Octet String and a data value comprising octets which are not specified as any ASN.1 type are considered equivalent, and either of the applicable encodings may be used (i.e. the single-ASN1-type choice containing an explicitly tagged Octet String, or the octet-aligned choice containing just the data octets without additional Octet String encoding).

7 Subclause 7.4.16

In 7.4.16 replace the last line of the ASN.1 production for **`ForwardedContentParameters`** *by:*

```
mts-identifier    [2] MessageDeliveryIdentifier OPTIONAL,
submission-proof  [3] SubmissionProof OPTIONAL}
```

In 7.4.16 insert new bullet d):

d) **Submission-proof** (C): The proof-of-submission of the original message together with the associated certificate of the public key of the MTA which generated that proof and the message-submission-envelope, if the content represents a message previously submitted to the MTS.

```
SubmissionProof ::= SET {
      proof-of-submission          [0] ProofOfSubmission,
      originating-MTA-certificate  [1] OriginatingMTACertificate,
      message-submission-envelope      MessageSubmissionEnvelope}
```

In 7.4.16, insert a new penultimate paragraph (after the Notes):

If the original message's delivery envelope contains a message-token which contains encrypted-data then it may be necessary to create a *Forwarded Content Token* (see B.6.2) for each recipient of the forwarding IPM. This is required, for example, when an asymmetric algorithm is used for encrypted-data that contains a content-confidentiality-key.

8 Clause 8

In clause 8, fifth paragraph (starting "The subject recipient specifier"*), append to the first sentence* ", and Blind Copy Recipients envelope field".

9 Subclause 18.2.2

In 18.2.2 first bullet a) insert new bullet iv):

iv) *Blind-copy-recipients* and *Disclosure-of-other-recipients*: If blind copy recipients are specified in the envelope then Disclosure-of-other-recipients shall have the value *disclosure-of-other-recipients-prohibited* (either explicitly or by default), and the Blind Copy Recipients heading field shall be absent within the Content.

In 18.2.2, add a new sentence to the end of the second paragraph of first bullet b):

The This IPM heading field of the IPM shall contain the same value for each instance of such a multiple submission.

In 18.2.2 first bullet b) insert a Note after the second paragraph):

NOTE – An alternative to the multiple submissions required by the Blind Copy Recipients heading field is a single submission with the blind copy recipients encoded in the Blind-copy-recipients per-recipient field in the envelope.

10 Subclause 19.2.1

In 19.2.1, insert the following paragraph before the last paragraph ("Figure 5 illustrates…"):

If the Message-log entry-class is supported, a Message-log entry is created for each Stored-message main-entry. Message-log child-entries are not created.

11 Subclause 19.2.3

In 19.2.3 third set of bullets insert new bullet e):

e) if Submission-proof is present in Parameters then the proof-of-submission, originating-MTA-certificate, and message-submission-envelope general-attribute-types shall be present.

12 Subclause 19.5.2.2

In 19.5.2.2 replace the last paragraph (before Notes) by:

In a Message body part constructed from a stored IPM that represents a delivered-message entry, the Parameters component shall contain delivery-time and delivery-envelope.

In a Message body part constructed from a stored IPM that represents a submitted-message entry, the Parameters component shall not contain delivery-time and shall contain delivery-envelope. This simulated delivery-envelope shall not contain originally-intended-recipient-name, converted-encoded-information-types, nor any extension whose presence is not defined in both a Message Submission envelope and a Message Delivery envelope. The originator-name and this-recipient-name components of this delivery-envelope each contain the OR-address of the IPM's originator.

In a Message body part constructed from a stored IPM that represents a draft-message entry, the Parameters component shall not contain delivery-time or delivery-envelope.

In a Forwarded Content body part constructed from a stored IPM, the Parameters component shall contain delivery-time and delivery-envelope as prescribed above for a Message body part, and shall also contain MTS-identifier except where the stored IPM represents a draft-message entry. In a Forwarded Content body part constructed from a stored IPM that represents a submitted-message entry which has a proof-of-submission and the associated originating-MTA-certificate, the Parameters component shall contain submission-proof.

When the IPMS-MS has assembled the new Body, it shall update the original-encoded-information-types in the message-submission-envelope as necessary, such that the complete message still satisfies the requirements of 20.4.

In 19.5.2.2 insert a new Note:

4. If any of the assembled body parts contain data that has been encrypted with a symmetric encryption algorithm where the session-key for that algorithm is itself encrypted in an associated token, it is the responsibility of the IPMS-MS-user to generate appropriate tokens for each recipient of the forwarding IPM. This does not require the IPMS-MS-user to retrieve or decrypt the encrypted data in these body parts, but just to retrieve, decrypt and re-encrypt the associated tokens.

13 Subclause 19.5.2.4

Insert new clause 19.5.2.5:

19.5.2.5 Originator-forwarded-content-token

This MS-submission-extension is used where the submitted message contains a *Forwarded Content Token* (see B.6.2) that has been encrypted such that it cannot subsequently be decrypted by the originator. This extension enables the originator to supply a *Forwarded Content 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 Forwarded Content body part.

```
originator-forwarded-content-token MS-EXTENSION ::= {
      ForwardedContentToken IDENTIFIED BY
            id-mst-originator-forwarded-content-token}
```

14 Table 3

Add the following to MS attributes definitions to Table 3:

Attribute	V	Support			P				L	S
		Sm	DI	SI	IPM	NRN	RN	ON		
F										
Forwarded Content Token	S	O	O	O	C	—	—	—	Y	N
Forwarding Token	S	O	—	—	C	—	—	—	Y	N

15 Subclause 19.6.2.4

In 19.6.2.4, insert after the production for blind-copy-recipients:

NOTE – If the blind-copy-recipients envelope field is present then the heading field of the same name is absent, and this attribute has instead subfields of the envelope field as its values.

16 Subclause 19.6.2.5

Insert new subclause19.6.2.6:

19.6.2.6 Envelope Extensions

Some attributes bear the names of extensions that are logically part of the IPM, but to facilitate efficient processing are envelope extensions, and have as their values the values of those extensions or a part thereof.

```
forwarded-content-token  ATTRIBUTE ::= {
     WITH ATTRIBUTE-SYNTAX   ForwardedContentToken,
     NUMERATION              single-valued,
     ID                      id-hat-forwarded-content-token }

forwarding-token  ATTRIBUTE ::= {
     WITH ATTRIBUTE-SYNTAX   MessageToken,
     NUMERATION              single-valued,
     ID                      id-hat-forwarding-token }
```

An IPMS-MS that supports the Forwarded Content Token attribute shall maintain it for an information object that it holds (and the Message-log entry for such an object) if that object is a message whose content is an IPM whose Body contains a Forwarded Content. An IPMS-MS that supports the Forwarding Token attribute shall maintain it for an information object that it holds if, and only if, that object is a child-entry which represents a Forwarded Content body part, where that content originally had an associated message-token containing encrypted-data.

17 Subclause 19.6.5

In 19.6.5, append to the second paragraph:

With the exception of AC Forwarded IPMs, all other Correlation attributes defined in this clause are applicable only to main entries.

18 Subclause 19.6.5.1.7

In 19.6.5.1.7 first sentence replace "attribute contains the sequence-number" *by* "attribute, which is multi-valued, contains the sequence-numbers of each instance", *and in the final sentence replace* "the entry" *by* "each entry". *In the* **NUMERATION** *line of the ASN.1 production replace* **"single"** *by* **"multi"**.

19 Subclause 19.6.5.1.9

In 19.6.5.1.9 first sentence replace "attribute contains the sequence-number" *by* "attribute, which is multi-valued, contains the sequence-numbers of each instance", *and in the final sentence replace* "the entry" *by* "each entry". *In the* **NUMERATION** *line of the ASN.1 production replace* **"single"** *by* **"multi"**.

20 Subclause 19.6.6

*In 19.6.6, insert into "***IPMSAttributeTable***" after "-- 1994 extension additions --" in the correct alphabetic sequence:*

```
forwarded-content-token | forwarding-token |
```

21 Table 5

In Table 5, in the Generation rules column in the row for Blind Copy Recipients, insert "Envelope field, if present, otherwise of the" *before* "Heading field".

Add the following rows to Table 5 in the correct alphabetic sequence:

Attribute-type name	Single/ multi valued	Source	Generation rules
Forwarded Content Token	S	IPM	For a delivered-message main-entry the attribute-value is the value of the Delivery Envelope parameter of the same name. For a submitted-message main-entry the attribute-value is the value of the Originator-forwarded-content-token MS-submission-extension. For a child-entry the attribute-value is the appropriate **`message-or-content-body-part`** component from this attribute-value in its parent-entry.
Forwarding Token	S	IPM	This attribute may only be present in a child-entry which represents a Forwarded Content body part, where that content originally had an associated message-token containing encrypted-data. The attribute-value is the value of the Forwarding-token component of the Forwarded Content Token which is associated with this Forwarded Content body part.

22 Subclause 19.9.1.1

In 19.9.1.1, item a), append the following paragraph after the Note:

If the delivered message contains an IPM whose This IPM heading field matches a subfield of the Replied-to IPM heading field of a stored IPM, then the sequence-number of each such stored IPM is recorded in the AC Replying IPMs attribute of the present entry. In addition, the AC Replied-to IPM attribute of each such stored IPM is updated to reference the present entry.

In 19.9.1.1, item b), append the following paragraph after the Note:

If the delivered message contains an IPM whose This IPM heading field is identical with that of a (previously delivered) stored IPM, then the value of the delivered IPM's AC Submitted Reply Status attribute and that of the corresponding attribute of the stored IPM shall be made identical, the higher value taking precedence.

In 19.9.1.1, item d), append the following second paragraph:

If the delivered message contains an IPM whose This IPM heading field matches a subfield of the Related IPMs heading field of a stored IPM, then the AC Related IPMs attribute of each such stored IPM is updated to record the sequence-number of the delivered IPM. In addition the AC Relating IPMs attribute of the delivered IPM is updated to record the sequence-numbers of the stored IPMs.

In 19.9.1.1, item e), append the following second paragraph:

If the delivered message contains an IPM whose This IPM heading field matches a subfield of the Obsoleted IPMs heading field of a stored IPM, then the AC Obsoleted IPMs attribute of each such stored IPM is updated to record the sequence-number of the delivered IPM. In addition the AC Obsoleting IPMs attribute of the delivered IPM is updated to record the sequence-numbers of the stored IPMs.

In 19.9.1.1 item f) first sentence replace "an entry corresponding" *by* "all entries which may correspond", *and in the second sentence replace* "the subject IPM entry is" *by* "any such entries are" *and append to that sentence* "on each such entry in turn".

23 Subclause 19.9.1.2

In 19.9.1.2, in item a) replace "steps (b) to (h)" *by* "steps (b) to (i)".

In 19.9.1.2, item e) 2), replace items (i) and (ii) with the following:

(i) If the Subject field or Sensitivity field is absent from the forwarding-heading, each assumes the value (if any) present in the delivered Heading.

(ii) The Importance field assumes the higher of the values present in the forwarding-heading and delivered Heading.

In 19.9.1.2, item e) 2), insert the following new item (vii):

(vii) If the delivered object is an IPN, then the notification-requests component of each recipient-specifier present in Primary, Copy, Blind Copy, and Circulation List Recipients is deleted.

In 19.9.1.2 replace item e) 3) (iii) by:

(iii) The original-encoded-information-types argument shall be the union of those values specified in the same argument of forwarding-envelope, and one of following dependent on the body part type for the forwarded object selected in item e) 1):

Message	– the encoded-information-types specified in the delivered Envelope (from the converted-encoded-information-types argument, if present, or original-encoded-information-types otherwise);
Forwarded Content	– the encoded-information-type for the Forwarded Content body part specified in 7.4.16;
Notification	– no additional encoded-information-types;
Report	– no additional encoded-information-types.

In 19.9.1.2, item e) 3), insert the following new item (iv):

(iv) If the delivered object is a Report, then for each recipient-name specified in the Envelope under construction, the originator-report-request is given the value no-report.

In 19.9.1.2, delete existing item i), rename existing item h) as i), and insert a new item h):

h) If the submission is successful, the IPMS-MS verifies the following:

1) that an NRN reporting non-receipt of the delivered object has not already been submitted;

2) that the registered IPM-auto-forward-options do not specify preserve-retrieval-status;

3) that the delivered object is an IPM whose originator requested an NRN by means of the notification-requests component of the subject recipient specifier.

If these conditions are fulfilled, then the IPMS-MS shall submit an NRN. The IPMS-MS draws the NRN's Auto-forward Comment field from the registered NRN-comment, if present. Other fields of the NRN are constructed as specified in 18.5.3.4. The IPMS-MS stages a performance of the MS-message-submission abstract-operation with the NRN and the registered submission-options as its arguments, and the procedure defined in 19.9.2 is followed.

In 19.9.1.2, replace item j) with the following:

j) Once all registered IPM auto-forward-registration-parameters have been processed, the procedure continues as follows.

If at least one of the IPM auto-forward auto-actions is performed successfully, and at least one of the registered IPM-auto-forward-registration-parameters whose criteria were satisfied by the delivered object did not request preserve-retrieval-status, then the delivered object's MS retrieval-status is set to *processed*. This change in retrieval-status does not cause the performance of the IPM auto-acknowledgement auto-action.

k) If at least one of the IPM auto-forward auto-actions is performed successfully, and all of the registered IPM-auto-forward-registration-parameters whose criteria were satisfied by the delivered object requested delete-delivered-object, then the IPMS-MS shall delete the delivered object.

24 Subclause 19.9.2

In clause 19.9.2, replace the last sentence before bullet c) by:

This procedure is described for the case where an entry is created in the Submission-log (or Submission) entry-class; if the submission options and subscription details are such that no entry is created, the maintenance of the AC Submitted IPN Status and AC Submitted Reply Status attributes shall be performed as described in steps c) and e), but the remaining steps are not applicable.

In 19.9.2, append the following:

i) If the submitted message contains an IPM, and the submission-options parameter of the MS-message-submission argument contains an originator-forwarded-content-token parameter, then the IPMS-MS shall create a forwarded-content-token attribute in the Submission and Submission-log entry-classes containing that value.

25 Subclause 20.1

In clause 20.1, add to the end of the sentence: ", and the additional encoding rules specified in 7.4.12.7"

26 Subclause A.2

Replace the ASN.1 production for `Language` *in A.2 by:*

```
Language ::= PrintableString (SIZE (2|5))
```

27 Subclause B.1

Delete the fourth paragraph of B.1: "At most one of content-non-repudiation and content-proof shall be requested. At most one of ipn-non-repudiation and ipn-proof shall be requested".

28 Subclause B.4.2.2

Delete the second sentence in B.4.2.2.

29 Subclause B.4.2.2.1

Replace B.4.2.2.1 by:

If more than one value is present in Recipient Security Request and the UA supports more than one of the requests, then the following precedence rules shall apply:

a) the content-non-repudiation procedures (see B.4.2.2.2) shall be the only procedures invoked when the request is present and supported, otherwise

b) the ipn-non-repudiation procedures (see B.4.2.2.4) shall be the only procedures invoked when ipn-non-repudiation together with either or both content-proof or ipn-proof are requested and supported, otherwise

c) the content-proof procedures (see B.4.2.2.3) shall be the only procedures invoked when both content-proof and ipn-proof are requested and supported.

When both ipn-non-repudiation and content-proof are requested and supported, the UA shall in addition to the ipn-non-repudiation procedures also generate a Security Diagnostic Code with the value *ipn-non-repudiation-provided-instead-of-content-proof*.

If more than one value is present in Recipient Security Request but the UA supports only one of the requests, then the procedure for the supported request shall apply.

30 Subclause B.6.1

Insert new subclause B.6.2:

B.6.2 Forwarded Content Token

The **Forwarded Content Token** MTS extension, which may be present in the per-recipient-message-submission-extensions field of a message-submission envelope and in the message-delivery-extensions field of a message-delivery envelope, enables an IPM's originator to convey one or more message-tokens (containing encrypted-data) to each of the IPM's recipients. Each Token enables a recipient to verify the security properties of a Forwarded Content body part contained either directly in the Body of the IPM or recursively within a Message or another Forwarded Content body part. The Forwarded Content Token shall be present only if the IPM contains (directly or recursively) at least one Forwarded Content body part (see 7.4.16) where that original message's envelope contains a message-token (see 8.2.1.1.1.26 of ITU-T Rec. X.411 | ISO/IEC 10021-4) which itself contains encrypted-data. The Forwarded Content Token contains a message-token for each such Forwarded Content body part contained (directly or recursively) in the forwarding IPM. The Forwarded Content Token is created by the originator of the forwarding IPM after decrypting the encrypted-data of the forwarded message's message-token (or of its Forwarded Content Token) to contain message-tokens with encrypted-data components encrypted appropriately for each recipient of the forwarding IPM.

```
forwarded-content-token EXTENSION ::= {
     ForwardedContentToken,
     RECOMMENDED CRITICALITY {for-delivery},
     IDENTIFIED BY standard-extension:44 }

ForwardedContentToken ::= SET OF SET {
     body-part-number            BodyPartNumber,
     body-part-choice            CHOICE {
          forwarding-token                MessageToken,
          message-or-content-body-part    ForwardedContentToken } }
```

A Forwarded Content Token has the following components:

a) **Body-part-number** (M): Identifies one of the body parts in this IPM, numbered starting at '1', which is a Message (or Encrypted Message) or Forwarded Content (or Encrypted Forwarded Content) body part.

NOTE – A body-part-number may occur twice in a Forwarded Content Token only if a Forwarded Content body part containing encrypted content itself contains a Forwarded Content body part containing encrypted content.