



INTERNATIONAL STANDARD ISO/IEC 10021-4:1997

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): Message transfer system: Abstract service definition and procedures

TECHNICAL CORRIGENDUM 2

TECHNICAL CORRIGENDUM 3

*Technologies de l'information — Systèmes de messagerie (MHS): Système de transfert de messages: Définition et
procédures du service abstrait*

RECTIFICATIF TECHNIQUE 2

RECTIFICATIF TECHNIQUE 3

Technical Corrigenda 2 and 3 to International Standard ISO/IEC 10021-4:1997 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

© ISO/IEC 2000 – All rights reserved

Printed in Switzerland

Ref. No. ISO/IEC 10021-4:1997/Cor.2:2000(E)

ISO/IEC 10021-4:1997/Cor.3:2000(E)



Documents

Document Sharing Hub

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 8.1.1.1.2

*In 8.1.1.1.2 fifth paragraph "If strong-authentication ...", append "or **certificate-selector**".*

*In 8.1.1.1.2 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) }

```