INTERNATIONAL STANDARD

ISO/IEC 10021-7

Second edition
1997-07-01

AMENDMENT 1
1998-10-15

Information technology — Message Handling Systems (MHS): Interpersonal messaging system

AMENDMENT 1: Security error diagnostic codes

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

AMENDEMENT 1: Codes de diagnostic d'erreur de sécurité

Reference number
ISO/IEC 10021-7:1997/Amd.1:1998(E)

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Amendment 1 to ISO/IEC 10021-7:1997 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 33, *Distributed application services*, in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.420/Amd.1.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

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

AMENDMENT 1
Security error diagnostic codes

1) Annex B

In B.3, *modify the* **SecurityDiagnosticCode ASN.1** *definition as follows:*

```
SecurityDiagnosticCode:: = INTEGER {
        integrity-failure-on-subject-message (0),
        integrity-failure-on-forwarded-message (1),
        moac-failure-on-subject-message (2),
        unsupported-security-policy (3),
        unsupported-algorithm-identifier (4),
        decryption-failed (5),
        token-error (6),
        unable-to-sign-notification (7),
        unable-to-sign-message-receipt (8),
        authentication-failure-on-subject-message (9),
        security-context-failure-message (10),
        message-sequence-failure (11),
        message-security-labelling-failure (12),
        repudiation-failure-of-message (13),
        failure-of-proof-of-message (14),
        signature-key-unobtainable (15),
        decryption-key-unobtainable (16),
        key-failure (17),
        unsupported-request-for-security-service (18),
        inconsistent-request-for-security-service (19),
        ipn-non-repudiation-instead-of-content-proof (20),
        token-decryption-failed (21),
        double-enveloping-message-restoring-failure (22),
        unauthorised-dl-member (23),
        reception-security-failure (24),
        unsuitable-alternate-recipient (25),
        security-services-refusal (26),
        unauthorised-recipient (27),
        unknown-certification-authority-name (28),
        unknown-dl-name (29),
        unknown-originator-name (30),
        unknown-recipient-name (31),
        security-policy-violation (32) }
```

In B.3, *modify the item f) as follows:*

f) *decryption-failed*: The recipient could not decrypt the message content.

In B.3, *add the following text at the end:*

1) *token-decryption-failed*: The recipient could not decrypt the message token.

2) *double-enveloping-message-restoring-failure*: The message contained an inner envelope, but failure of security services on the outer envelope prevented the UA from extracting the inner message for subsequent processing.

3) *unauthorised-dl-member*: The UA has detected that the message has been received via a DL, yet this recipient was prohibited by the security policy from being a member of that DL.

4) *recipient-security-failure*: The message could not be received due to the failure of one of the message security services.

5) *unsuitable-alternate-recipient*: The message was not able to be processed as it has been delivered to an alternate recipient and this recipient is unable to process the security functions.

6) *security-services-refusal***:** The security services cannot be supported.

7) *unauthorised-recipient*: The recipient is not allowed to get the required decryption keys for content confidentiality. The recipient is not authorised to read the message content.

8) *unknown-certification-authority-name*: The message cannot be processed because the certification authority named in a certificate contained within one of the security arguments is not know to the UA, or is not trusted by the UA.

9) *unknown-dl-name*: The security policy requires the UA to perform checks on messages that have been received via DLs, and in this case one of the DLs named in the DL-expansion-history was unknown to the UA.

10) *unknown-originator-name*: The originator MTS-user **O/R name** identifies a user who is not known to the receiving UA, hence the security arguments cannot be validated.

11) *unknown-recipient-name*: The recipient MTS-user **O/R name** identifies a user who is not known to the receiving UA, hence the security arguments cannot be validated.

12) *security-policy-violation:* The security policy is violated.

2) Annex K

Same modification as for **1)** (Annex B).