



INTERNATIONAL TELECOMMUNICATION UNION

**ITU-T**

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

**X.420**

**Amendment 1**

(08/97)

SERIES X: DATA NETWORKS AND OPEN SYSTEM  
COMMUNICATION

Message Handling Systems

---

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

**Amendment 1: Security error diagnostic codes**

ITU-T Recommendation X.420 – Amendment 1

(Previously CCITT Recommendation)

---

ITU-T X-SERIES RECOMMENDATIONS  
DATA NETWORKS AND OPEN SYSTEM COMMUNICATION

PUBLIC DATA NETWORKS	X.1–X.199
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 SYSTEM INTERCONNECTION	X.200–X.299
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	X.300–X.399
General	X.300–X.349
Satellite data transmission systems	X.350–X.399
<b>MESSAGE HANDLING SYSTEMS</b>	<b>X.400–X.499</b>
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
Networking	X.600–X.629
Efficiency	X.630–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	X.700–X.799
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	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
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.*

**INTERNATIONAL STANDARD 10021-7**

**ITU-T RECOMMENDATION X.420**

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

**AMENDMENT 1  
Security error diagnostic codes**

**Summary**

This amendment defines an extended set of ASN.1 integer values for IPM security error diagnostic codes.

**Source**

The ITU-T Recommendation X.420, Amendment 1 was approved on the 9th August 1997. The identical text is also published as ISO/IEC International Standard 10021-7.

## 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 expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

## 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 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.

© ITU 1998

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.

## CONTENTS

	<i>Page</i>
1) Annex B .....	1
2) Annex K .....	2



## INTERNATIONAL STANDARD

## ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – MESSAGE HANDLING SYSTEMS (MHS):  
INTERPERSONAL MESSAGING SYSTEMAMENDMENT 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 known 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).

## 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
<b>Series X</b>	<b>Data networks and open system communication</b>
Series Z	Programming languages