INTERNATIONAL STANDARD ISO/IEC 10164-7:1992/Amd.1:1995
TECHNICAL CORRIGENDUM 1

Published 1996-12-15

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

Information technology — Open Systems Interconnection — Systems Management: Security alarm reporting function

AMENDMENT 1: Implementation conformance statement proformas

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Gestion-systèmes: Fonction de rapport d'alarme de sécurité

AMENDEMENT 1: Proformes de déclaration de conformité de mise en œuvre

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to International Standard ISO/IEC 10164-7:1992/Amd.1:1995 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology,* Subcommittee SC 21, *Open systems interconnection, data management and open distributed processing.*

This material is reproduced from ISO documents under International Organization for Standardization (ISO) Copyright License number IHS/ICC/1996. Not for resale. No part of these ISO documents may be reproduced in any form, electronic retrieval system or otherwise, except as allowed in the copyright law of the country of use, or with the prior written consent of ISO (Case postale 56, 1211 Geneva 20, Switzerland, Fax +41 22 734 10 79), IHS or the ISO Licensor's members.

ICS 35.100.70 **Ref. No. ISO/IEC 10164-7:1992/Amd.1:1995/Cor.1:1996(E)**

Descriptors: data processing, information interchange, network interconnection, open systems interconnection, application layer, systems management, management.

© **ISO/IEC 1996**

Printed in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SYSTEMS MANAGEMENT: SECURITY ALARM REPORTING FUNCTION

AMENDMENT 1
Implementation conformance statement proformas

TECHNICAL CORRIGENDUM 1

1) Annex A

In Table A.6 – "PICS Support Summary", *first row referencing* "CCITT Rec. X.730 | ISO/IEC 10164-1, Annex E, SM Application Context", *change the status from* "m" *to* "o" *and add the following note for the corresponding row of this table:*

"NOTE – The supplier of implementation shall indicate the application contexts supported."

2) Subclause A.1.3

Add the following sentence after the line "– Not applicable or out of scope", *and immediately before* "NOTES":

"The value of 'm' in the Status column for the receiving of parameters, of tables of type MCS indicates that there is a minimum requirement for the implementation to be able to receive the parameter. The Additional information column shall be used to state whether the implementation provides support for more than the minimum requirement."

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4851903 0647180 T25

INTERNATIONAL STANDARD

ISO/IEC 10164-7

First edition
1992-05-15

AMENDMENT 1
1995-12-15

Information technology — Open Systems Interconnection — Systems Management: Security alarm reporting function

AMENDMENT 1: Implementation conformance statement proformas

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Gestion-systèmes: Fonction de rapport d'alarme de sécurité

AMENDEMENT 1: Proformes de déclaration de conformité de mise en œuvre

Reference number
ISO/IEC 10164-7:1992/Amd.1:1995(E)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

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 International Standard ISO/IEC 10164-7:1992 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 21, *Open systems interconnection, data management and open distributed processing,* in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.736/Amd.1.

© ISO/IEC 1995
All rights reserved. Unless otherwise specified, 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 publisher.

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

Printed in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4851903 0647182 8T8

Introduction

This amendment includes tables, which document the mandatory and optional management information specific to the Security Alarm Reporting Function. This amendment will be used by Profile specifiers, for example, those developing International Standardized Profiles (ISPs), to specify an explicit subset of capability, which will afford interoperability between implementations. The tables also include a column for equipment vendors to state the capability of their products in terms of the Profiles or base specification. The table structures comply with the Guidelines for Implementation Conformance Statement Proformas specified in ITU-T Recommendation X.724 | ISO/IEC 10165-6.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SYSTEMS MANAGEMENT: SECURITY ALARM REPORTING FUNCTION

AMENDMENT 1
(to Rec. X.736 | ISO/IEC 10164-7)

IMPLEMENTATION CONFORMANCE STATEMENT PROFORMAS

1) *Add the following footnote to the first list item in 2.1:*

"[1] as amended by ITU-T Rec. X.701/Cor.2 | ISO/IEC 10040/Cor.2"

2) *Add the following reference to 2.1:*

"– ITU-T Recommendation X.724 (1993) | ISO/IEC 10165-6:1994, *Information technology – Open Systems Interconnection – Structure of management information: Requirements and guidelines for implementation conformance statement proformas associated with OSI management.*"

3) *Add the following references to 2.2:*

"– CCITT Recommendation X.291 (1992), *OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications – Abstract test suite specification.*

ISO/IEC 9646-2:1991, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 2: Abstract test suite specification.*

– ITU-T Recommendation X.296[3], *OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications – Implementation conformance statements.*

ISO/IEC 9646-7...[3], *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 7: Implementation conformance statements.*"

And then add the following footnote:

[3] Presently at the stage of draft.

4) *Apply the following changes to 3.4:*

Replace "dependent conformance" *with* "managed object conformance statement (MOCS)".

Replace "general conformance" *with* "management information conformance statement (MICS)".

Relabel items e) and f) as g) and h) and insert the following new items:

"e) MICS proforma;

f) MOCS proforma;"

5) *Apply the following change to 3.7:*

Replace "system conformance statement" *with the following:*

"a) PICS proforma;

b) protocol implementation conformance statement;

c) system conformance statement."

6) *Renumber 3.8 as 3.9 and insert the following new subclause:*

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

"3.8 **Implementation conformance statement proforma definitions**

This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.724 | ISO/IEC 10165-6:

a) Managed Relationship Conformance Statement (MRCS);

b) Management Conformance Summary (MCS);

c) Management Information Definition Statement (MIDS) proforma;

d) MCS proforma;

e) MRCS proforma."

7) *Add the following abbreviations to clause 4:*

"ICS Implementation Conformance Statement

MCS Management Conformance Summary

MICS Management Information Conformance Statement

MIDS Management Information Definition Statement

MOCS Managed Object Conformance Statement

MRCS Managed Relationship Conformance Statement

PICS Protocol Implementation Conformance Statement"

8) Replace clause 13 with the following:

"13 Conformance

Implementations claiming to conform to this Recommendation | International Standard shall comply with the conformance requirements as defined in the following subclauses.

13.1 Static conformance

The implementation shall conform to the requirements of this Recommendation | International Standard in the manager role, the agent role, or both roles. A claim of conformance to at least one role shall be made in Table A.1.

If a claim of conformance is made for support in the manager role, the implementation shall support at least one of the notifications or at least one of the management operations specified in this Recommendation | International Standard. The conformance requirements in the manager role for those management operations and notifications are identified in Table A.3 and further tables referenced by Annex A.

If a claim of conformance is made for support in the agent role, the implementation shall support at least one of the notifications specified in this Recommendation | International Standard. The conformance requirements in the agent role are identified in Table A.4 and further tables referenced by Annex A.

The implementation shall support the transfer syntax derived from the encoding rules specified in CCITT Rec. X.209 | ISO/IEC 8825 named {joint-iso-ccitt asn1(1) basicEncoding(1)} for the abstract data types referenced by the definitions for which support is claimed.

NOTE – Prior to the publication of this amendment, this Recommendation | International Standard identified general and dependent conformance classes. A claim of conformance similar to general conformance class can be made by stating support in the manager role, the agent role, or both roles, for the security alarm reporting functional unit in Table A.2. A claim of conformance similar to dependent conformance class can be made by stating support for at least one of the items in Tables A.3 or A.4.

13.2 Dynamic conformance

Implementations claiming to conform to this Recommendation | International Standard shall support the elements of procedure and definitions of semantics corresponding to the definitions for which support is claimed.

13.3 Management implementation conformance statement requirements

Any MCS proforma, MICS proforma, and MOCS proforma which conforms to this Recommendation | International Standard shall be technically identical to the proformas specified in Annexes A, B and C preserving table numbering and the index numbers of items, and differing only in pagination and page headers.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

The supplier of an implementation which is claimed to conform to this Recommendation | International Standard shall complete a copy of the Management Conformance Summary (MCS) provided in Annex A as part of the conformance requirements together with any other ICS proformas referenced as applicable from that MCS. An ICS which conforms to this Recommendation | International Standard shall:

- describe an implementation which conforms to this Recommendation | International Standard;
- have been completed in accordance with the instructions for completion given in ITU-T Rec. X.724 | ISO/IEC 10165-6;
- include the information necessary to uniquely identify both the supplier and the implementation.

Claims of conformance to the management information defined in this Recommendation | International Standard in managed object classes defined elsewhere shall include the requirements of the MIDS proforma in the MOCS for the managed object class."

9) *Add the following annexes:*

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A

MCS proforma[5)]

(This annex forms an integral part of this Recommendation | International Standard)

A.1 Introduction

A.1.1 Purpose and structure

The Management Conformance Summary (MCS) is a statement by a supplier that identifies an implementation and provides information on whether the implementation claims conformance to any of the listed set of documents that specify conformance requirements to OSI management.

The MCS proforma is a document in the form of a questionnaire that when completed by the supplier of an implementation becomes the MCS.

A.1.2 Instructions for completing the MCS proforma to produce a MCS

The supplier of the implementation shall enter an explicit statement in each of the boxes provided. Specific instruction is provided in the text which precedes each table.

A.1.3 Symbols, abbreviations and terms

For all annexes of this Recommendation | International Standard, the following common notations, defined in CCITT Rec. X.291 | ISO/IEC 9646-2 and ITU-T Rec. X.296 | ISO/IEC 9646-7, are used for the Status column:

m Mandatory;

o Optional;

c Conditional;

x Prohibited;

– Not applicable or out of scope.

NOTES

1 'c', 'm', and 'o' are prefixed by "c:" when nested under a conditional or optional item of the same table;

2 'o' may be suffixed by ".N" (where N is a unique number) for selectable options among a set of status values. Support of at least one of the choices (from the items with the same value of N) is required.

For all annexes of this Recommendation | International Standard, the following common notations, defined in CCITT Rec. X.291 | ISO/IEC 9646-2 and ITU-T Rec. X.296 | ISO/IEC 9646-7, are used for the Support column:

Y Implemented;

N Not implemented;

– No answer required;

Ig The item is ignored (i.e. processed syntactically but not semantically).

A.1.4 Table format

Some of the tables in this Recommendation | International Standard have been split because the information is too wide to fit on the page. Where this occurs, the index number of the first block of columns are the index numbers of the corresponding rows of the remaining blocks of columns. A complete table reconstructed from the constituent parts should have the following layout:

Index	First block of columns	Second block of columns	Etc.

In this Recommendation | International Standard the constituent parts of the table appear consecutively, starting with the first block of columns.

---

5) Users of this Recommendation | International Standard may freely reproduce the MCS proforma in this annex so that it can be used for its intended purpose, and may further publish the completed MCS. Instructions for the MCS proforma are specified in ITU-T Rec. X.724 | ISO/IEC 10165-6.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

When a table with sub-rows is too wide to fit on a page, the continuation table(s) have been constructed with index numbers identical to the index numbers in the corresponding rows of the first table, and with sub-index numbers corresponding to the sub-rows within each indexed row. For example, if Table X.1 has 2 rows and the continuation of Table X.1 has 2 sub-rows for each row, the tables are presented as follows:

Table X.1 – Title

					Support		
Index	A	B	C	D	E	F	G
1	a	b	–				
2	a	b	–				

Table X.1 *(concluded)* – Title

Index	Sub-index	H	I	J	K	L
1	1.1	h	i	j		
	1.2	h	i	j		
2	2.1	h	i	j		
	2.2	h	i	j		

A complete table reconstructed from the constituent parts should have the following layout:

					Support								
Index	A	B	C	D	E	F	G	Sub-index	H	I	J	K	L
1	a	b	–					1.1	h	i	j		
								1.2	h	i	j		
2	a	b	–					2.1	h	i	j		
								2.2	h	i	j		

References made to cells within tables shall be interpreted as references within reconstructed tables. In the example, above, the reference X.1/1d corresponds with the blank cell in column G for row with Index 1, and X.1/1.2b corresponds with the blank cell in column L for row with Sub-index 1.2.

A.2 Identification of the implementation

A.2.1 Date of statement

The supplier of the implementation shall enter the date of this statement in the box below. Use the format DD-MM-YYYY.

Date of statement

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.2.2 Identification of the implementation

The supplier of the implementation shall enter information necessary to uniquely identify the implementation and the system(s) in which it may reside, in the box below.

A.2.3 Contact

The supplier of the implementation shall provide information on whom to contact if there are any queries concerning the content of the MCS or any referenced conformance statement, in the box below.

A.3 Identification of the Recommendations I International Standards in which the management information is defined

The supplier of the implementation shall enter the title, reference number and date of the publication of the Recommendations I International Standards which specify the management information to which conformance is claimed, in the box below.

Recommendations I International Standards to which conformance is claimed

A.3.1 Technical corrigenda implemented

The supplier of the implementation shall enter the reference numbers of implemented technical corrigenda which modify the identified Recommendations I International Standards, in the box below.

A.3.2 Amendments implemented

The supplier of the implementation shall state the titles and reference numbers of implemented amendments to the identified Recommendations I International Standards, in the box below.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

A.4 Management conformance summary

The supplier of the implementation shall state the capabilities and features supported and provide a summary of conformance claims to Recommendations I International Standards using the tables in this annex.

The supplier of the implementation shall specify the roles that are supported, in Table A.1.

Table A.1 – Roles

Index	Roles supported	Status	Support	Additional information
1	Manager role support	o.1		
2	Agent role support	o.1		

The supplier of the implementation shall specify support for the systems management functional unit, in Table A.2.

Table A.2 – Systems management functional unit

		Manager		Agent		
Index	Systems management functional unit name	Status	Support	Status	Support	Additional information
1	security alarm reporting functional unit	c1		c2		

c1: if A.1/1a then o else –.

c2: if A.1/2a then o else –.

The supplier of the implementation shall specify support for management information in the manager role, in Table A.3.

Table A.3 – Manager role minimum conformance requirement

Index	Item	Status	Support	Additional information
1	Integrity violation notification	c3		
2	Operational violation notification	c3		
3	Physical violation notification	c3		
4	Security service or mechanism violation notification	c3		
5	Time domain violation notification	c3		
6	Operations on managed objects	c4		

c3: if A.2/1a then m else (if A.1/1a then o.2 else –).

c4: if A.2/1a then m else (if A.1/1a then o.2 else –).

NOTE – Manager role minimum conformance requires support for at least one of the items identified in this table. Support for the functional unit identified in Table A.2 mandates support for some of those items. Conditions c3 and c4 express both of these requirements.

The supplier of the implementation shall specify support for management information in the agent role, in Table A.4.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table A.4 – Agent role minimum conformance requirement

Index	Item	Status	Support	Table reference	Additional information
1	Integrity violation notification	c5			
2	Operational violation notification	c5			
3	Physical violation notification	c5			
4	Security service or mechanism violation notification	c5			
5	Time domain violation notification	c5			
6	Security alarm record managed object class	c6		–	

c5: if A.2/1b then m else (if A.1/2a then o.3 else –).

c6: if A.1/2a and A.5/1a then m else –.

NOTES

1 Condition c6 makes it mandatory, if logging is supported, to support the event log records associated with the notifications supported.

2 The Table reference column in this table is the notification reference of the MOCS supplied by the supplier of the managed object which claims to import the notification from this Recommendation | International Standard.

Table A.5 – Logging of event records

Index		Status	Support	Additional information
1	Does the implementation support logging of event records in agent role?	c7		

c7: if A.1/2a then o else –.

NOTE 1 – Conformance to this Recommendation | International Standard does not require conformance to CCITT Rec. X.735 | ISO/IEC 10164-6.

The supplier of the implementation shall provide information on claims of conformance to any of the Recommendations | International Standards summarized in the Tables A.6 to A.9. For each Recommendation | International Standard that the supplier of the implementation claims conformance to, the corresponding conformance statement(s) shall be completed, or referenced by, the MCS. The supplier of the implementation shall complete the Support, Table numbers and Additional information columns.

In Tables A.6 to A.9, the Status column is used to indicate whether the supplier of the implementation is required to complete the referenced tables or referenced items. Conformance requirements are as specified in the referenced tables or referenced items and are not changed by the value of the MCS Status column. Similarly, the Support column is used by the supplier of the implementation to indicate completion of the referenced tables or referenced items.

Table A.6 – PICS support summary

Index	Identification of the document that includes the PICS proforma	Table numbers of PICS proforma	Description	Constraints and values	Status	Support	Table numbers of PICS	Additional information
1	CCITT Rec. X.730 | ISO/IEC 10164-1	Annex E all tables	SM application context	OBJECT IDENTIFIER	m			

NOTE 2 – Conformance to the MAPDUs defined in this Recommendation | International Standard can be claimed by completing the corresponding tables in the MICS and MOCS annexes of the referenced Recommendations | International Standards.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table A.7 – MOCS support summary

Index	Identification of the document that includes the MOCS proforma	Table numbers of MOCS proforma	Description	Constraints and values	Status	Support	Table numbers of MOCS	Additional information
1	CCITT Rec. X.736 | ISO/IEC 10164-7	Annex C all tables	securityAlarmRecord	–	c8			
c8: if A.4/6a then m else –.								

Table A.8 – MRCS support summary

Index	Identification of the document that includes the MRCS proforma	Table numbers of MRCS proforma	Description	Constraints and values	Status	Support	Table numbers of MRCS	Additional information
1	CCITT Rec. X.735 | ISO/IEC 10164-6	Item D.1/1	logRecord-log name binding	–	c9			
c9: if A.5/1a then o else –.								

Table A.9 – MICS support summary

Index	Identification of the document that includes the MICS proforma	Table numbers of MICS proforma	Description	Constraints and values	Status	Support	Table numbers of MICS	Additional information
1	CCITT Rec. X.736 | ISO/IEC 10164-7	Table B.1	notifications	–	c10			
2	CCITT Rec. X.736 | ISO/IEC 10164-7	Tables B.2 and B.3	management operations	–	c11			
c10: if A.3/1a or A.3/2a or A.3/3a or A.3/4a or A.3/5a then m else –. c11: if A.3/6a then m else –.								

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B

MICS proforma[6)]

(This annex forms an integral part of this Recommendation | International Standard)

B.1 Introduction

The purpose of this MICS proforma is to provide a mechanism for a supplier of an implementation which claims conformance, in the manager role, to management information specified in this Recommendation | International Standard, to provide conformance information in a standard form.

B.2 Instructions for completing the MICS proforma to produce a MICS

The MICS proforma contained in this annex is comprised of information in tabular form, in accordance with ITU-T Rec. X.724 | ISO/IEC 10165-6. In addition to the general guidance given in ITU-T Rec. X.724 | ISO/IEC 10165-6, the Additional information column shall be used to identify the object classes for which the management operations are supported. The supplier of the implementation shall state which items are supported in the tables below and if necessary, provide additional information.

B.3 Symbols, abbreviations and terms

The following abbreviations are used throughout the MICS proforma:

dmi-att joint-iso-ccitt ms(9) smi(3) part2(2) attribute(7)

dmi-not joint-iso-ccitt ms(9) smi(3) part2(2) notification(10)

The notations used for the Status and Support columns are specified in A.1.3.

B.4 Statement of conformance to the management information

B.4.1 Notifications

The specifier of a manager role implementation that claims to support the notifications specified in this Recommendation | International Standard shall import a copy of Table B.1 and complete it.

Table B.1 – Notification support

					Support		
Index	Notification type template label	Value of object identifier for the notification type	Constraints and values	Status	Confirmed	Non-confirmed	Additional information
1	integrityViolation	{dmi-not 5}	–	c1			
2	operationalViolation	{dmi-not 8}	–	c2			
3	physicalViolation	{dmi-not 9}	–	c3			
4	securityServiceOrMechanism	{dmi-not 13}	–	c4			
5	timeDomainViolation	{dmi-not 55}	–	c5			
c1: if A.3/1a then m else –. c2: if A.3/2a then m else –. c3: if A.3/3a then m else –. c4: if A.3/4a then m else –. c5: if A.3/5a then m else –.							

(continued)

6) Users of this Recommendation | International Standard may freely reproduce the MICS proforma in this annex so that it can be used for its intended purpose, and may further publish the completed MICS.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table B.1 *(continued)* – Notification support

Index	Sub-index	Notification field name label	Value of object identifier for the attribute type associated with the field	Constraints and values	Status	Support	Additional information
1	1.1	securityAlarmCause	{dmi-att 21}	OBJECT IDENTIFIER	m		
	1.2	securityAlarmSeverity	{dmi-att 23}	ENUMERATED 0 to 4	m		
	1.3	securityAlarmDetector	{dmi-att 22}	–	m		
	1.3.1	mechanism	–	OBJECT IDENTIFIER	m		
	1.3.2	object	–	–	m		
	1.3.2.1	distinguishedName	–	–	m		
	1.3.2.2	nonSpecificForm	–	–	m		
	1.3.2.3	localDistinguishedName	–	–	m		
	1.3.3	application	–	OBJECT IDENTIFIER	m		
	1.4	serviceUser	{dmi-att 25}	–	m		
	1.4.1	identifier	–	OBJECT IDENTIFIER	m		
	1.4.2	details	–	–	m		
	1.5	serviceProvider	{dmi-att 24}	–	m		
	1.5.1	identifier	–	OBJECT IDENTIFIER	m		
	1.5.2	details	–	–	m		
	1.6	notificationIdentifier	{dmi-att 16}	INTEGER	m		
	1.7	correlatedNotifications	{dmi-att 12}	–	m		
	1.7.1	correlatedNotifications	–	–	m		
	1.7.2	sourceObjectInst	–	–	m		
	1.7.2.1	distinguishedName	–	–	m		
	1.7.2.2	nonSpecificForm	–	–	m		
	1.7.2.3	localDistinguishedName	–	–	m		
	1.8	additionalText	{dmi-att 7}	–	m		
	1.9	additionalInformation	{dmi-att 6}	required for some objects	m		
2	2.1	securityAlarmCause	{dmi-att 21}	OBJECT IDENTIFIER	m		
	2.2	securityAlarmSeverity	{dmi-att 23}	ENUMERATED 0 to 4	m		
	2.3	securityAlarmDetector	{dmi-att 22}	–	m		
	2.3.1	mechanism	–	OBJECT IDENTIFIER	m		
	2.3.2	object	–	–	m		
	2.3.2.1	distinguishedName	–	–	m		
	2.3.2.2	nonSpecificForm	–	–	m		

(continued)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table B.1 *(continued)* – Notification support

Index	Sub-index	Notification field name label	Value of object identifier for the attribute type associated with the field	Constraints and values	Status	Support	Additional information
2	2.3.2.3	localDistinguishedName	–	–	m		
	2.3.3	application	–	OBJECT IDENTIFIER	m		
	2.4	serviceUser	{dmi-att 25}	–	m		
	2.4.1	identifier	–	OBJECT IDENTIFIER	m		
	2.4.2	details	–	–	m		
	2.5	serviceProvider	{dmi-att 24}	–	m		
	2.5.1	identifier	–	OBJECT IDENTIFIER	m		
	2.5.2	details	–	–	m		
	2.6	notificationIdentifier	{dmi-att 16}	INTEGER	m		
	2.7	correlatedNotifications	{dmi-att 12}	–	m		
	2.7.1	correlatedNotifications	–	–	m		
	2.7.2	sourceObjectInst	–	–	m		
	2.7.2.1	distinguishedName	–	–	m		
	2.7.2.2	nonSpecificForm	–	–	m		
	2.7.2.3	localDistinguishedName	–	–	m		
	2.8	additionalText	{dmi-att 7}	–	m		
	2.9	additionalInformation	{dmi-att 6}	required for some objects	m		
3	3.1	securityAlarmCause	{dmi-att 21}	OBJECT IDENTIFIER	m		
	3.2	securityAlarmSeverity	{dmi-att 23}	ENUMERATED 0 to 4	m		
	3.3	securityAlarmDetector	{dmi-att 22}	–	m		
	3.3.1	mechanism	–	OBJECT IDENTIFIER	m		
	3.3.2	object	–	–	m		
	3.3.2.1	distinguishedName	–	–	m		
	3.3.2.2	nonSpecificForm	–	–	m		
	3.3.2.3	localDistinguishedName	–	–	m		
	3.3.3	application	–	OBJECT IDENTIFIER	m		
	3.4	serviceUser	{dmi-att 25}	–	m		
	3.4.1	identifier	–	OBJECT IDENTIFIER	m		
	3.4.2	details	–	–	m		
	3.5	serviceProvider	{dmi-att 24}	–	m		
	3.5.1	identifier	–	OBJECT IDENTIFIER	m		
	3.5.2	details	–	–	m		

(continued)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table B.1 *(continued)* – Notification support

Index	Sub-index	Notification field name label	Value of object identifier for the attribute type associated with the field	Constraints and values	Status	Support	Additional information
3	3.6	notificationIdentifier	{dmi-att 16}	INTEGER	m		
	3.7	correlatedNotifications	{dmi-att 12}	–	m		
	3.7.1	correlatedNotifications	–	–	m		
	3.7.2	sourceObjectInst	–	–	m		
	3.7.2.1	distinguishedName	–	–	m		
	3.7.2.2	nonSpecificForm	–	–	m		
	3.7.2.3	localDistinguishedName	–	–	m		
	3.8	additionalText	{dmi-att 7}	–	m		
	3.9	additionalInformation	{dmi-att 6}	required for some objects	m		
4	4.1	securityAlarmCause	{dmi-att 21}	OBJECT IDENTIFIER	m		
	4.2	securityAlarmSeverity	{dmi-att 23}	ENUMERATED 0 to 4	m		
	4.3	securityAlarmDetector	{dmi-att 22}	–	m		
	4.3.1	mechanism	–	OBJECT IDENTIFIER	m		
	4.3.2	object	–	–	m		
	4.3.2.1	distinguishedName	–	–	m		
	4.3.2.2	nonSpecificForm	–	–	m		
	4.3.2.3	localDistinguishedName	–	–	m		
	4.3.3	application	–	OBJECT IDENTIFIER	m		
	4.4	serviceUser	{dmi-att 25}	–	m		
	4.4.1	identifier	–	OBJECT IDENTIFIER	m		
	4.4.2	details	–	–	m		
	4.5	serviceProvider	{dmi-att 24}	–	m		
	4.5.1	identifier	–	OBJECT IDENTIFIER	m		
	4.5.2	details	–	–	m		
	4.6	notificationIdentifier	{dmi-att 16}	INTEGER	m		
	4.7	correlatedNotifications	{dmi-att 12}	–	m		
	4.7.1	correlatedNotifications	–	–	m		
	4.7.2	sourceObjectInst	–	–	m		
	4.7.2.1	distinguishedName	–	–	m		
	4.7.2.2	nonSpecificForm	–	–	m		
	4.7.2.3	localDistinguishedName	–	–	m		

(continued)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table B.1 *(concluded)* – Notification support

Index	Sub-index	Notification field name label	Value of object identifier for the attribute type associated with the field	Constraints and values	Status	Support	Additional information
4	4.8	additionalText	{dmi-att 7}	–	m		
	4.9	additionalInformation	{dmi-att 6}	required for some objects	m		
5	5.1	securityAlarmCause	{dmi-att 21}	OBJECT IDENTIFIER	m		
	5.2	securityAlarmSeverity	{dmi-att 23}	ENUMERATED 0 to 4	m		
	5.3	securityAlarmDetector	{dmi-att 22}	–	m		
	5.3.1	mechanism	–	OBJECT IDENTIFIER	m		
	5.3.2	object	–	–	m		
	5.3.2.1	distinguishedName	–	–	m		
	5.3.2.2	nonSpecificForm	–	–	m		
	5.3.2.3	localDistinguishedName	–	–	m		
	5.3.3	application	–	OBJECT IDENTIFIER	m		
	5.4	serviceUser	{dmi-att 25}	–	m		
	5.4.1	identifier	–	OBJECT IDENTIFIER	m		
	5.4.2	details	–	–	m		
	5.5	serviceProvider	{dmi-att 24}	–	m		
	5.5.1	identifier	–	OBJECT IDENTIFIER	m		
	5.5.2	details	–	–	m		
	5.6	notificationIdentifier	{dmi-att 16}	INTEGER	m		
	5.7	correlatedNotifications	{dmi-att 12}	–	m		
	5.7.1	correlatedNotifications	–	–	m		
	5.7.2	sourceObjectInst	–	–	m		
	5.7.2.1	distinguishedName	–	–	m		
	5.7.2.2	nonSpecificForm	–	–	m		
	5.7.2.3	localDistinguishedName	–	–	m		
	5.8	additionalText	{dmi-att 7}	–	m		
	5.9	additionalInformation	{dmi-att 6}	required for some objects	m		

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.4.2 Attributes

The specifier of a manager role implementation that claims to support management operations on the attributes specified in this Recommendation | International Standard shall import a copy of Table B.2 and complete it.

Table B.2 – Attribute support

				Set by create		Get	
Index	Attribute template label	Value of object identifier for the attribute	Constraints and values	Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	–		o.4	
2	nameBinding	{dmi-att 63}	–	–		o.4	
3	packages	{dmi-att 66}	–	–		o.4	
4	allomorphs	{dmi-att 50}	–	–		o.4	
5	logRecordId	{dmi-att 3}	–	–		o.4	
6	loggingTime	{dmi-att 59}	–	–		o.4	
7	managedObjectClass	{dmi-att 60}	–	–		o.4	
8	managedObjectInstance	{dmi-att 61}	–	–		o.4	
9	eventType	{dmi-att 14}	–	–		o.4	
10	eventTime	{dmi-att 13}	–	–		o.4	
11	notificationIdentifier	{dmi-att 16}	–	–		o.4	
12	correlatedNotifications	{dmi-att 12}	–	–		o.4	
13	additionalText	{dmi-att 7}	–	–		o.4	
14	additionalInformation	{dmi-att 6}	–	–		o.4	
15	securityAlarmCause	{dmi-att 21}	–	–		o.4	
16	securityAlarmSeverity	{dmi-att 23}	–	–		o.4	
17	securityAlarmDetector	{dmi-att 22}	–	–		o.4	
18	serviceUser	{dmi-att 25}	–	–		o.4	
19	serviceProvider	{dmi-att 24}	–	–		o.4	

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table B.2 *(concluded)* – Attribute support

	Replace		Add		Remove		Set to default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	–		–		–		–		
2	–		–		–		–		
3	–		–		–		–		
4	–		–		–		–		
5	–		–		–		–		
6	–		–		–		–		
7	–		–		–		–		
8	–		–		–		–		
9	–		–		–		–		
10	–		–		–		–		
11	–		–		–		–		
12	–		–		–		–		
13	–		–		–		–		
14	–		–		–		–		
15	–		–		–		–		
16	–		–		–		–		
17	–		–		–		–		
18	–		–		–		–		
19	–		–		–		–		

B.4.3 Create and delete management operations

The specifier of a manager role implementation that claims to support the create or delete management operations on the managed objects specified in this Recommendation | International Standard shall import a copy of Table B.3 and complete it.

Table B.3 – Create and delete support

Index	Operation	Constraints and values	Status	Support	Additional information
1	Create support	–	x		
1.1	Create with reference object	–	–		
2	Delete support	securityAlarmRecord managed object	o.4		

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Annex C

MOCS proforma[7)]

(This annex forms an integral part of this Recommendation | International Standard)

C.1 Introduction

The purpose of this MOCS proforma is to provide a mechanism for a supplier of an implementation which claims conformance to a managed object class, to provide conformance information in a standard form.

C.2 Instructions for completing the MOCS proforma to produce a MOCS

The MOCS proforma contained in this annex is comprised of information in tabular form, in accordance with ITU-T Rec. X.724 | ISO/IEC 10165-6. The supplier of the implementation shall state which items are supported in the tables below and if necessary, provide additional information.

C.3 Symbols, abbreviations and terms

The following abbreviations are used throughout the MOCS proforma:

dmi-att	joint-iso-ccitt ms(9) smi(3) part2(2) attribute(7)
dmi-moc	joint-iso-ccitt ms(9) smi(3) part2(2) managedObjectClass(3)
dmi-nb	joint-iso-ccitt ms(9) smi(3) part2(2) nameBinding(6)
dmi-not	joint-iso-ccitt ms(9) smi(3) part2(2) notification(10)
dmi-pkg	joint-iso-ccitt ms(9) smi(3) part2(2) package(4)

The notations used for the Status and Support columns are specified in A.1.3.

The following conditional expression is commonly used throughout this MOCS proforma:

c1 if C.3/3a or C.3/6a or C.3/7a or C.3/8a or C.3/9a or C.3/10a, then m else –.

C.4 Security alarm record managed object class

C.4.1 Statement of conformance to the managed object class

The supplier of the implementation shall state whether or not all mandatory features of the security alarm report record managed object class are supported, and if the actual class supported is the same as the managed object class to which conformance is claimed, in Table C.1.

Table C.1 – Managed object class support

Index	Managed object class template label	Value of object identifier for the managed object class	Does the implementation support all mandatory features? (Y/N)	Is the actual class the same as the managed object class to which conformance is claimed? (Y/N)
1	securityAlarmReportRecord	{dmi-moc 11}		

7) Users of this Recommendation | International Standard may freely reproduce the MOCS proforma in this annex so that it can be used for its intended purpose, and may further publish the completed MOCS. Instructions for completing the MOCS proforma are specified in ITU-T Rec. X.724 | ISO/IEC 10165-6. Instructions for the MOCS proforma are specified in ITU-T Rec. X.724 | ISO/IEC 10165-6.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

If the answer to the actual class question in the managed object class support table is "N", the supplier of the implementation shall supply the actual class support details, in Table C.2.

Table C.2 – Actual class support

Index	Actual managed object class template label	Value of object identifier for the managed object class	Additional information
1			

C.4.2 Packages

See Table C.3.

Table C.3 – Package support

Index	Package template label	Value of object identifier for the package	Constraints and values	Status	Support	Additional information
1	topPackage	–	–	m		
2	packagesPackage	{dmi-pkg 16}	–	c1		
3	allomorphicPackage	{dmi-pkg 17}	–	c2		
4	logRecordPackage	–	–	m		
5	eventLogRecordPackage	–	–	m		
6	eventTimePackage	{dmi-pkg 11}	–	o		
7	notificationIdentifierPackage	{dmi-pkg 24}	–	o		
8	correlatedNotificationsPackage	{dmi-pkg 23}	–	o		
9	additionalTextPackage	{dmi-pkg 19}	–	o		
10	additionalInformationPackage	{dmi-pkg 18}	–	o		
11	securityAlarmRecordPackage	–	–	m		
c2: if C.1/1b then – else m.						

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

C.4.3 Attributes

See Table C.4.

Table C.4 – Attribute support

Index	Attribute template label	Value of object identifier for the attribute	Constraints and values	Set by create		Get	
				Status	Support	Status	Support
1	objectClass	{dmi-att 65}	–	x		m	
2	nameBinding	{dmi-att 63}	–	x		m	
3	packages	{dmi-att 66}	–	x		c1	
4	allomorphs	{dmi-att 50}	–	x		c3	
5	logRecordId	{dmi-att 3}	–	x		m	
6	loggingTime	{dmi-att 59}	–	x		m	
7	managedObjectClass	{dmi-att 60}	–	x		m	
8	managedObjectInstance	{dmi-att 61}	–	x		m	
9	eventType	{dmi-att 14}	–	x		m	
10	eventTime	{dmi-att 13}	–	x		c4	
11	notificationIdentifier	{dmi-att 16}	–	x		c5	
12	correlatedNotifications	{dmi-att 12}	–	x		c6	
13	additionalText	{dmi-att 7}	–	x		c7	
14	additionalInformation	{dmi-att 6}	–	x		c8	
15	securityAlarmCause	{dmi-att 21}	–	x		m	
16	securityAlarmSeverity	{dmi-att 23}	–	x		m	
17	securityAlarmDetector	{dmi-att 22}	–	x		m	
18	serviceUser	{dmi-att 25}	–	x		m	
19	serviceProvider	{dmi-att 24}	–	x		m	

c3: if C.3/3a then m else –.
c4: if C.3/6a then m else –.
c5: if C.3/7a then m else –.
c6: if C.3/8a then m else –.
c7: if C.3/9a then m else –.
c8: if C.3/10a then m else –.

(continued)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table C.4 *(concluded)* – Attribute support

	Replace		Add		Remove		Set to default		
Index	Status	Support	Status	Support	Status	Support	Status	Support	Additional information
1	x		–		–		–		
2	x		–		–		–		
3	x		x		x		–		
4	x		x		x		–		
5	x		–		–		–		
6	x		–		–		–		
7	x		–		–		–		
8	x		–		–		–		
9	x		–		–		–		
10	x		–		–		–		
11	x		–		–		–		
12	x		x		x		–		
13	x		–		–		–		
14	x		x		x		–		
15	x		–		–		–		
16	x		–		–		–		
17	x		–		–		–		
18	x		–		–		–		
19	x		–		–		–		

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex D

MIDS (notification) proforma[8)]

(This annex forms an integral part of this Recommendation I International Standard)

D.1 Symbols, abbreviations and terms

The following abbreviations are used throughout this MIDS proforma:

dmi-att joint-iso-ccitt ms(9) smi(3) part2(2) attribute(7)

dmi-not joint-iso-ccitt ms(9) smi(3) part2(2) notification(10)

The notations used for the Status and Support columns are specified in A.1.3.

D.2 Notifications

The specifier of a managed object class that claims to support the notifications specified by CCITT Rec. X.736 I ISO/IEC 10164-7 shall import a copy of this annex and complete it according to the instructions specified in ITU-T Rec. X.724 I ISO/IEC 10165-6.

Table D.1 – Notification support

					Support		
Index	Notification type template label	Value of object identifier for the notification type	Constraints and values	Status	Confirmed	Non-confirmed	Additional information
1	integrityViolation	{dmi-not 5}	–				
2	operationalViolation	{dmi-not 8}	–				
3	physicalViolation	{dmi-not 9}	–				
4	securityServiceOrMechanism	{dmi-not 13}	–				
5	timeDomainViolation	{dmi-not 55}	–				

(continued)

8) Users of this Recommendation I International Standard may freely reproduce the MIDS proforma in this annex so that it can be used for its intended purpose, and may further publish the completed MIDS. Instructions for completing the MIDS proforma are specified in ITU-T Rec. X.724 I ISO/IEC 10165-6.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table D.1 *(continued)* – Notification support

Index	Sub-index	Notification field name label	Value of object identifier for the attribute type associated with the field	Constraints and values	Status	Support	Additional information
1	1.1	securityAlarmCause	{dmi-att 21}	OBJECT IDENTIFIER	m		
	1.2	securityAlarmSeverity	{dmi-att 23}	ENUMERATED 0 to 4	m		
	1.3	securityAlarmDetector	{dmi-att 22}	–	m		
	1.3.1	mechanism	–	OBJECT IDENTIFIER	o.5		
	1.3.2	object	–	–	o.5		
	1.3.2.1	distinguishedName	–	–	c:o.6		
	1.3.2.2	nonSpecificForm	–	–	c:o.6		
	1.3.2.3	localDistinguishedName	–	–	c:o.6		
	1.3.3	application	–	OBJECT IDENTIFIER	o.5		
	1.4	serviceUser	{dmi-att 25}	–	m		
	1.4.1	identifier	–	OBJECT IDENTIFIER	m		
	1.4.2	details	–	–	m		
	1.5	serviceProvider	{dmi-att 24}	–	m		
	1.5.1	identifier	–	OBJECT IDENTIFIER	m		
	1.5.2	details	–	–	m		
	1.6	notificationIdentifier	{dmi-att 16}	INTEGER	c1		
	1.7	correlatedNotifications	{dmi-att 12}	–	o		
	1.7.1	correlatedNotifications	–	–	c:m		
	1.7.2	sourceObjectInst	–	–	c:o		
	1.7.2.1	distinguishedName	–	–	c:o.6		
	1.7.2.2	nonSpecificForm	–	–	c:o.6		
	1.7.2.3	localDistinguishedName	–	–	c:o.6		
	1.8	additionalText	{dmi-att 7}	–	o		
	1.9	additionalInformation	{dmi-att 6}	required for some objects	o		
2	2.1	securityAlarmCause	{dmi-att 21}	OBJECT IDENTIFIER	m		
	2.2	securityAlarmSeverity	{dmi-att 23}	ENUMERATED 0 to 4	m		
	2.3	securityAlarmDetector	{dmi-att 22}	–	m		
	2.3.1	mechanism	–	OBJECT IDENTIFIER	o.7		
	2.3.2	object	–	–	o.7		
	2.3.2.1	distinguishedName	–	–	c:o.8		

c1: if D.1/1.7a then m else o.

(continued)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table D.1 *(continued)* – Notification support

Index	Sub-index	Notification field name label	Value of object identifier for the attribute type associated with the field	Constraints and values	Status	Support	Additional information
2	2.3.2.2	nonSpecificForm	–	–	c:o.8		
	2.3.2.3	localDistinguishedName	–	–	c:o.8		
	2.3.3	application	–	OBJECT IDENTIFIER	o.7		
	2.4	serviceUser	{dmi-att 25}	–	m		
	2.4.1	identifier	–	OBJECT IDENTIFIER	m		
	2.4.2	details	–	–	m		
	2.5	serviceProvider	{dmi-att 24}	–	m		
	2.5.1	identifier	–	OBJECT IDENTIFIER	m		
	2.5.2	details	–	–	m		
	2.6	notificationIdentifier	{dmi-att 16}	INTEGER	c2		
	2.7	correlatedNotifications	{dmi-att 12}	–	o		
	2.7.1	correlatedNotifications	–	–	c:m		
	2.7.2	sourceObjectInst	–	–	c:o		
	2.7.2.1	distinguishedName	–	–	c:o.9		
	2.7.2.2	nonSpecificForm	–	–	c:o.9		
	2.7.2.3	localDistinguishedName	–	–	c:o.9		
	2.8	additionalText	{dmi-att 7}	–	o		
	2.9	additionalInformation	{dmi-att 6}	required for some objects	o		
3	3.1	securityAlarmCause	{dmi-att 21}	OBJECT IDENTIFIER	m		
	3.2	securityAlarmSeverity	{dmi-att 23}	ENUMERATED 0 to 4	m		
	3.3	securityAlarmDetector	{dmi-att 22}	–	m		
	3.3.1	mechanism	–	OBJECT IDENTIFIER	o.10		
	3.3.2	object	–	–	o.10		
	3.3.2.1	distinguishedName	–	–	c:o.11		
	3.3.2.2	nonSpecificForm	–	–	c:o.11		
	3.3.2.3	localDistinguishedName	–	–	c:o.11		
	3.3.3	application	–	OBJECT IDENTIFIER	o.10		
	3.4	serviceUser	{dmi-att 25}	–	m		
	3.4.1	identifier	–	OBJECT IDENTIFIER	m		
c2: if D.1/2.7a then m else o.							

(continued)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table D.1 *(continued)* – Notification support

Index	Sub-index	Notification field name label	Value of object identifier for the attribute type associated with the field	Constraints and values	Status	Support	Additional information
3	3.4.2	details	–	–	m		
	3.5	serviceProvider	{dmi-att 24}	–	m		
	3.5.1	identifier	–	OBJECT IDENTIFIER	m		
	3.5.2	details	–	–	m		
	3.6	notificationIdentifier	{dmi-att 16}	INTEGER	c3		
	3.7	correlatedNotifications	{dmi-att 12}	–	o		
	3.7.1	correlatedNotifications	–	–	c:m		
	3.7.2	sourceObjectInst	–	–	c:o		
	3.7.2.1	distinguishedName	–	–	c:o.12		
	3.7.2.2	nonSpecificForm	–	–	c:o.12		
	3.7.2.3	localDistinguishedName	–	–	c:o.12		
	3.8	additionalText	{dmi-att 7}	–	o		
	3.9	additionalInformation	{dmi-att 6}	required for some objects	o		
4	4.1	securityAlarmCause	{dmi-att 21}	OBJECT IDENTIFIER	m		
	4.2	securityAlarmSeverity	{dmi-att 23}	ENUMERATED 0 to 4	m		
	4.3	securityAlarmDetector	{dmi-att 22}	–	m		
	4.3.1	mechanism	–	OBJECT IDENTIFIER	o.13		
	4.3.2	object	–	–	o.13		
	4.3.2.1	distinguishedName	–	–	c:o.14		
	4.3.2.2	nonSpecificForm	–	–	c:o.14		
	4.3.2.3	localDistinguishedName	–	–	c:o.14		
	4.3.3	application	–	OBJECT IDENTIFIER	o.13		
	4.4	serviceUser	{dmi-att 25}	–	m		
	4.4.1	identifier	–	OBJECT IDENTIFIER	m		
	4.4.2	details	–	–	m		
	4.5	serviceProvider	{dmi-att 24}	–	m		
	4.5.1	identifier	–	OBJECT IDENTIFIER	m		
	4.5.2	details	–	–	m		
	4.6	notificationIdentifier	{dmi-att 16}	INTEGER	c4		
	4.7	correlatedNotifications	{dmi-att 12}	–	o		

c3: if D.1/3.7a then m else o.

c4: if D.1/4.7a then m else o.

(continued)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table D.1 *(concluded)* – Notification support

Index	Sub-index	Notification field name label	Value of object identifier for the attribute type associated with the field	Constraints and values	Status	Support	Additional information
4	4.7.1	correlatedNotifications	–	–	c:m		
	4.7.2	sourceObjectInst	–	–	c:o		
	4.7.2.1	distinguishedName	–	–	c:o.15		
	4.7.2.2	nonSpecificForm	–	–	c:o.15		
	4.7.2.3	localDistinguishedName	–	–	c:o.15		
	4.8	additionalText	{dmi-att 7}	–	o		
	4.9	additionalInformation	{dmi-att 6}	required for some objects	o		
5	5.1	securityAlarmCause	{dmi-att 21}	OBJECT IDENTIFIER	m		
	5.2	securityAlarmSeverity	{dmi-att 23}	ENUMERATED 0 to 4	m		
	5.3	securityAlarmDetector	{dmi-att 22}	–	m		
	5.3.1	mechanism	–	OBJECT IDENTIFIER	o.16		
	5.3.2	object	–	–	o.16		
	5.3.2.1	distinguishedName	–	–	c:o.17		
	5.3.2.2	nonSpecificForm	–	–	c:o.17		
	5.3.2.3	localDistinguishedName	–	–	c:o.17		
	5.3.3	application	–	OBJECT IDENTIFIER	o.16		
	5.4	serviceUser	{dmi-att 25}	–	m		
	5.4.1	identifier	–	OBJECT IDENTIFIER	m		
	5.4.2	details	–	–	m		
	5.5	serviceProvider	{dmi-att 24}	–	m		
	5.5.1	identifier	–	OBJECT IDENTIFIER	m		
	5.5.2	details	–	–	m		
	5.6	notificationIdentifier	{dmi-att 16}	INTEGER	c5		
	5.7	correlatedNotifications	{dmi-att 12}	–	o		
	5.7.1	correlatedNotifications	–	–	c:m		
	5.7.2	sourceObjectInst	–	–	c:o		
	5.7.2.1	distinguishedName	–	–	c:o.18		
	5.7.2.2	nonSpecificForm	–	–	c:o.18		
	5.7.2.3	localDistinguishedName	–	–	c:o.18		
	5.8	additionalText	{dmi-att 7}	–	o		
	5.9	additionalInformation	{dmi-att 6}	required for some objects	o		

c5: if D.1/5.7a then m else o.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

4851903 0647208 934

© ISO/IEC

ICS 35.100.70

Descriptors: data processing, information interchange, network interconnection, open systems interconnection, application layer, management, implementation.

Price based on 25 pages

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

10164 PT*7 92 ■ 4851903 0505695 2 ■

INTERNATIONAL STANDARD

ISO/IEC 10164-7

First edition
1992-05-15

Information technology — Open Systems Interconnection — Systems Management: Security alarm reporting function

Technologies de l'information — Interconnexion de systèmes ouverts — Gestion-système: Fonction de compte rendu d'alarme de sécurité



Reference number
ISO/IEC 10164-7:1992(E)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Contents

Page

Foreword ... iii

Introduction ... iv

1 Scope ... 1

2 Normative references ... 2
2.1 Identical CCITT Recommendations | International Standards ... 2
2.2 Paired CCITT Recommendations | International Standards equivalent in technical content ... 2
2.3 Additional references ... 3

3 Definitions ... 3
3.1 Basic reference model definitions ... 3
3.2 Security architecture definitions ... 3
3.3 Management framework definitions ... 3
3.4 Systems management overview definitions ... 3
3.5 Event report management function definitions ... 4
3.6 Service conventions definitions ... 4
3.7 OSI conformance testing definitions ... 4
3.8 Additional definitions ... 4

4 Abbreviations ... 4

5 Conventions ... 4

6 Requirements ... 5

7 Model ... 5

8 Generic definitions ... 5
8.1 Generic notifications ... 5
8.2 Managed object ... 8
8.3 Imported generic definitions ... 8
8.4 Compliance ... 8

9 Service definition ... 8
9.1 Introduction ... 8
9.2 Security alarm reporting service ... 8

10 Functional units ... 9

11 Protocol ... 9
11.1 Elements of procedure ... 9
11.2 Abstract syntax ... 10
11.3 Negotiation of the security alarm reporting functional unit ... 12

12 Relationships with other functions ... 12

13 Conformance ... 12
13.1 General conformance class requirements ... 12
13.2 Dependent conformance class requirements ... 13

© ISO/IEC 1992

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 publisher.

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

Printed in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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.

International Standard ISO/IEC 10164-7 was prepared by the Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in collaboration with the CCITT. The identical text is published as CCITT Recommendation X.736.

ISO/IEC 10164 consists of the following parts, under the general title *Information technology - Open Systems Interconnection - Systems Management:*

— Part 1: *Object management function*

— Part 2: *State management function*

— Part 3: *Attributes for representing relationships*

— Part 4: *Alarm reporting function*

— Part 5: *Event report management function*

— Part 6: *Log control function*

— Part 7: *Security alarm reporting function*

— Part 8: *Security audit trail function*

— Part 9: *Objects and attributes for access control*

— Part 10: *Accounting meter function*

— Part 11: *Workload monitoring function*

— Part 12: *Test management function*

— Part 13: *Summarization function*

— Part 14: *Confidence and diagnostic test categories*

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Introduction

ISO/IEC 10164 is a multipart standard developed according to ISO 7498 and ISO/IEC 7498-4. ISO/IEC 10164 is related to the following International Standards

— ISO/IEC 9595 : 1990, *Information technology — Open Systems Interconnection — Common management information service definition*;

— ISO/IEC 9596 : 1990, *Information technology — Open Systems Interconnection — Common management information protocol*;

— ISO/IEC 10040 : 1992, *Information technology — Open Systems Interconnection — Systems management overview*;

— ISO/IEC 10165 : 1992, *Information technology — Open Systems Interconnection — Structure of management information.*

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

INTERNATIONAL STANDARD

CCITT RECOMMENDATION

Information technology — Open Systems Interconnection — Systems Management: Security alarm reporting function

1 Scope

This Recommendation | International Standard defines the security alarm reporting function. The security alarm reporting function is a systems management function which may be used by an application process in a centralized or decentralized management environment to exchange information for the purpose of systems management, as defined by CCITT Rec. X.700 | ISO/IEC 7498-4. This Recommendation | International Standard is positioned in the application layer of CCITT Rec. X.200 | ISO 7498 and is defined according to the model provided by ISO/IEC 9545. The role of systems management functions is described by CCITT Rec. X.701 | ISO/IEC 10040. The security alarm notifications defined by this systems management function provide information regarding operational condition and quality of service, pertaining to security.

Security-related events are of relevance to the provision of security. The security policy determines the actions to be undertaken whenever a security-related event has occured. The security policy may, for example, specify that a security alarm report be generated, a record of the event be made in a security audit trail, a threshold counter be incremented, the event be ignored, or a combination of these actions be taken. This Recommendation | International Standard is only concerned with security alarm reporting.

This Recommendation | International Standard

- establishes user requirements for the service definition needed to support the security alarm reporting function;
- defines the service provided by the security alarm reporting function;
- specifies the protocol that is necessary in order to provide the service;
- defines the relationship between the service and management notifications;
- defines relationships with other systems management functions;
- specifies conformance requirements.

This Recommendation | International Standard does not

- define the nature of any implementation intended to provide the security alarm reporting function;
- specify the manner in which management is accomplished by the user of the security alarm reporting function;
- define the nature of any interactions which result in the use of the security alarm reporting function;
- specify the services necessary for the establishment, normal and abnormal release of a management association;
- define any other notifications, defined by other Recommendations | International Standards, which may be of interest to a security administrator.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2 Normative references

The following CCITT Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent editions of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The CCITT Secretariat maintains a list of the currently valid CCITT Recommendations.

2.1 Identical CCITT Recommendations | International Standards

— CCITT Recommendation X.701 (1992) | ISO/IEC 10040 : 1992, *Information technology - Open Systems Interconnection - Systems management overview.*

— CCITT Recommendation X.721 (1992) | ISO/IEC 10165-2 : 1992, *Information technology - Open Systems Interconnection - Structure of management information: Definition of management information.*

— CCITT Recommendation X.722 (1992) | ISO/IEC 10165-4 : 1992, *Information technology - Open Systems Interconnection - Structure of management information: Guidelines for the definition of managed objects.*

— CCITT Recommendation X.733 (1992) | ISO/IEC 10164-4 : 1992, *Information technology - Open Systems Interconnection - Systems Management: Alarm reporting function.*

— CCITT Recommendation X.734[1)] | ISO/IEC 10164-5 : 1992, *Information technology - Open Systems Interconnection - Systems Management: Event report management function.*

— CCITT Recommendation X.735[1)] | ISO/IEC 10164-6 : 1992, *Information technology - Open Systems Interconnection - Systems Management: Log control function.*

2.2 Paired CCITT Recommendations | International Standards equivalent in technical content

— CCITT Recommendation X.200 (1988), *Reference model of Open Systems Interconnection for CCITT applications.*

ISO 7498 : 1984, *Information processing systems - Open Systems Interconnection - Basic Reference Model.*

— CCITT Recommendation X.208 (1988), *Specification of abstract syntax notation one (ASN.1).*

ISO/IEC 8824 : 1990, *Information technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1).*

— CCITT Recommendation X.209 (1988), *Specification of Basic Encoding Rules for abstract syntax notation.*

ISO/IEC 8825 : 1990, *Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

— CCITT Recommendation X.210 (1988), *Open Systems Interconnection layer service definition conventions.*

ISO/TR 8509 : 1987, *Information processing systems - Open Systems Interconnection - Service conventions.*

— CCITT Recommendation X.290 (1992), *OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications - General concepts.*

ISO/IEC 9646-1 : 1991, *Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 1: General concepts.*

— CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

ISO 7498-2 : 1988, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.*

---

1) Presently at state of draft Recommendation.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

— CCITT Recommendation X.700[1], *Management framework definition for Open Systems Interconnection for CCITT applications.*

ISO/IEC 7498-4 : 1989, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 4: Management framework.*

— CCITT Recommendation X.710 (1991), *Common management information service definition for CCITT applications.*

ISO/IEC 9595 : 1991, *Information technology - Open Systems Interconnection - Common management information service definition.*

2.3 Additional references

— ISO/IEC 9545 : 1989, *Information technology - Open Systems Interconnection - Application Layer structure.*

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

3.1 Basic reference model definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.200 | ISO 7498:

open system

3.2 Security architecture definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.800 | ISO 7498-2:

a) authentication;

b) confidentiality;

c) integrity;

d) non-repudiation;

e) security policy;

f) security service.

3.3 Management framework definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.700 | ISO/IEC 7498-4:

managed object

3.4 Systems management overview definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.701 | ISO/IEC 10040:

a) agent role;

b) dependent conformance;

c) general conformance;

d) manager role;

---

[1] Presently at state of draft Recommendation.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

e) notification;

f) systems management functional unit.

3.5 Event report management function definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.734 | ISO/IEC 10164-5:

discriminator

3.6 Service conventions definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.210 | ISO/TR 8509:

a) service-user;

b) service-provider.

3.7 OSI conformance testing definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.290 | ISO/IEC 9646-1:

system conformance statement

3.8 Additional definitions

3.8.1 **security alarm**: A security-related event that has been identified by a security policy as a potential breach of security;

3.8.2 **security-related event**: An event which is considered to have relevance to security.

4 Abbreviations

ASN.1	Abstract Syntax Notation One
CMIS	Common Management Information Services
Conf	Confirmation
Ind	Indication
MAPDU	Management Application Protocol Data Unit
OSI	Open Systems Interconnection
Req	Request
Rsp	Response
SMAPM	Systems Management Application Protocol Machine

5 Conventions

This Recommendation | International Standard defines services for the security alarm reporting function using the descriptive conventions defined in CCITT Rec. X.210 | ISO/TR 8509. In clause 9, the definition of each service includes a table that lists the parameters of its primitives. For a given primitive, the presence of each parameter is described by one of the following values

M the parameter is mandatory

(=) the value of the parameter is equal to the value of the parameter in the column to the left

U the use of the parameter is a service-user option

— the parameter is not present in the interaction described by the primitive concerned

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

C the parameter is conditional. The condition(s) are defined by the text which describes the parameter

P subject to the constraints imposed on the parameter by CCITT Rec. X.710 | ISO/IEC 9595

NOTE — The parameters that are marked "P" in Table 2 of this Recommendation | International Standard are mapped directly onto the corresponding parameters of the CMIS service primitive, without changing the semantics or syntax of the parameters. The remaining parameters are used to construct an MAPDU.

6 Requirements

The security management user needs to be alerted whenever an event indicating an attack or potential attack on system security has been detected. A security attack may be detected by a security service, a security mechanism, or another process.

A security alarm notification may be generated by either of the communicating end users, or by any intermediate system or process between the end users. The security alarm report shall identify the cause of the security alarm, the source of the detection of the security-related event, the appropriate end users, and of the perceived severity of any misoperation, attack or breach of security, as specified by the security policy.

This Recommendation | International Standard describes the use of services and techniques to satisfy these requirements.

7 Model

The model for security alarm reporting is defined in CCITT Rec. X.734 | ISO/IEC 10164-5. The information may be logged in accordance with CCITT Rec. X.735 | ISO/IEC 10164-6.

8 Generic definitions

8.1 Generic notifications

This Recommendation | International Standard defines a set of generic security alarm notifications and their applicable parameters and semantics.

The set of generic notifications, parameters and semantics defined by this Recommendation | International Standard provide the detail for the following parameters of the M-EVENT-REPORT service as defined by CCITT Rec. X.710 | ISO/IEC 9595

— event type;

— event information;

— event reply.

All notifications are potential entries in a systems management log and this Recommendation | International Standard defines a managed object class for this purpose. CCITT Rec. X.721 | ISO/IEC 10165-2 defines a generic log record object class from which all entries are derived, the additional information being specified by the event information and event reply parameters.

8.1.1 Event type

This parameter defines the type of the security alarm report. The following event types are defined in this Recommendation | International Standard

— integrity violation: an indication that information may have been illegally modified, inserted or deleted;

— operational violation: an indication that the provision of the requested service was not possible due to the unavailability, malfunction or incorrect invocation of the service;

— physical violation: an indication that a physical resource has been violated in a way that suggests a security attack;

— security service or mechanism violation: an indication that a security attack has been detected by a security service or mechanism;

— time domain violation: an indication that an event has occurred at an unexpected or prohibited time.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.1.2 Event information

The following parameters constitute the notification specific event information.

8.1.2.1 Security alarm cause

This parameter defines further qualification as to the probable cause of the security alarm. The value of this parameter in combination with the value of event type, determines which parameters constitute the balance of the security alarm event report, and what the possible values of those parameters may be.

Security alarm cause values for notifications shall be indicated in the behaviour clause of the object class definition. This Recommendation | International Standard defines, for use within the systems management application context defined in CCITT Rec. X.701 | ISO/IEC 10040, security alarm causes that have wide applicability across managed object classes. These values are registered in CCITT Rec. X.721 | ISO/IEC 10165-2. The syntax of security alarm causes shall be the ASN.1 type object identifier. Additional security alarm causes, for use within the systems management application context defined in CCITT Rec. X.701 | ISO/IEC 10040, may be added to this Recommendation | International Standard and registered using the registration procedures defined for ASN.1 object identifier values in CCITT Rec. X.208 | ISO/IEC 8824.

Other security alarm causes, for use within the systems management application context defined in CCITT Rec. X.701 | ISO/IEC 10040, may be defined outside of this Recommendation | International Standard and registered using the registration procedures defined for ASN.1 object identifier values in CCITT Rec. X.208 | ISO/IEC 8824.

Table 1 identifies the security alarm causes for the event types specified in this Recommendation | International Standard.

Table 1 — Security alarm causes

Event type	Security alarm causes
integrity violation	duplicate information information missing information modification detected information out of sequence unexpected information
operational violation	denial of service out of service procedural error unspecified reason
physical violation	cable tamper intrusion detection unspecified reason
security service or mechanism violation	authentication failure breach of confidentiality non-repudiation failure unauthorized access attempt unspecified reason
time domain violation	delayed information key expired out of hours activity

This Recommendation | International Standard defines the following security alarm causes

- authentication failure: an indication that an attempt to authenticate a user was unsuccessful;
- breach of confidentiality: an indication that information may have been read by an unauthorized user;
- cable tamper: an indication that a physical violation of a communications medium has occurred;
- delayed information: an indication that information has been received later than expected;

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

- denial of service: an indication that a valid request for service has been prevented or disallowed;
- duplicate information: an indication that an item of information has been received more than once, and therefore may be a replay attack;
- information missing: an indication that expected information has not been received;
- information modification detected: an indication, for example by a data integrity mechanism, that information has been modified;
- information out of sequence: an indication that information has been received in an incorrect sequence;
- intrusion detection: an indication that either the site on which the identified equipment is located may have been illegally entered, or the equipment itself has been violated;
- key expired: an indication that an out of date encipherment key has been presented or used;
- non-repudiation failure: an indication that communication has been prevented or halted due to the failure or unavailability of a non-repudiation service;
- out of hours activity: an indication that resource utilization has occurred at an unexpected time;
- out of service: an indication that a valid request for service could not be satisfied due to the unavailability of the service provider;
- procedural error: an indication that an incorrect procedure has been used in invoking a service;
- unauthorized access attempt: an indication that an access control mechanism has detected an illegal attempt to access a resource;
- unexpected information: an indication that information that was not expected has been received;
- unspecified reason: an indication that an unspecified security-related event has occurred.

The managed object class definer should choose the most specific security alarm cause applicable.

8.1.2.2 Security alarm severity

This parameter defines the significance of the security alarm as perceived by the managed object. The following levels of severity are defined

- indeterminate: a security attack has been detected. The integrity of the system is unknown;
- critical: a breach of security has occurred that has compromised the system. The system may no longer be assumed to be operating correctly in support of the security policy. Critical severity may involve the modification of security information without the correct authorization, leakage of information vital to the security of the system (such as passwords, private encryption keys etc), or breaches of physical security;
- major: a breach of security has been detected and significant information or mechanisms have been compromised;
- minor: a breach of security has been detected and less significant information or mechanisms have been compromised;
- warning: a security attack has been detected. The security of the system is not believed to be compromised.

8.1.2.3 Security alarm detector

This parameter identifies the detector of the security alarm.

8.1.2.4 Service user

This parameter identifies the service-user whose request for service led to the generation of the security alarm.

8.1.2.5 Service provider

This parameter identifies the intended service-provider of the service that led to the generation of the security alarm.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.1.3 Event reply

This Recommendation | International Standard does not specify management information to be used in the event reply parameter.

8.2 Managed object

A security alarm record is a managed object class derived from the event log record object class defined in CCITT Rec. X.721 | ISO/IEC 10165-2. The security alarm record object class represents information stored in logs resulting from security alarm notifications.

8.3 Imported generic definitions

The following parameters are also utilized. These parameters are defined by CCITT Rec. X.733 | ISO/IEC 10164-4.

- additional information;
- additional text;
- correlated notifications;
- notification identifier.

8.4 Compliance

Managed object class definitions support the functions defined in this Recommendation | International Standard by incorporating the specification of the notifications through reference to the notification templates defined in CCITT Rec. X.721 | ISO/IEC 10165-2. The reference mechanism is defined in CCITT Rec. X.722 | ISO/IEC 10165-4.

A managed object class definition importing one or more of the security alarm notifications defined in this Recommendation | International Standard is required for each instance of a security alarm report to select the security alarm type and security alarm cause that most closely reflects the real event that leads to the managed object issuing the notification. The managed object class definition is also required to specify the security alarm generator, service-user, service-provider, and shall also specify in the behaviour clause, how the security alarm severity parameter is to be specified.

The definition of the managed object class shall, for each imported notification, specify in the behaviour clause which of the optional and conditional parameters are to be utilized, the conditions for their use, and their values. It is permissible to state that the use of a parameter remains optional.

9 Service definition

9.1 Introduction

This Recommendation | International Standard defines one service. Security alarm notifications provide the ability to report security attacks, security service and mechanism misoperations or other security-related events. The parameters convey the information relevant to the security alarm.

9.2 Security alarm reporting service

The security alarm reporting service uses the parameters defined in clause 8 of this Recommendation | International Standard in addition to the general M-EVENT-REPORT service parameters defined in CCITT Rec. X.710 | ISO/IEC 9595.

Table 2 lists the parameters for the security alarm reporting service.

The Event time, Correlated notifications, and Notification identifier parameters may be assigned by the managed object that emits the notification or by the managed system.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 2 — Security alarm reporting parameters

Parameter name	Req/Ind	Rsp/Conf
Invoke identifier	P	P
Mode	P	—
Managed object class	P	P
Managed object instance	P	P
Event type	M	C(=)
Event time	P	—
Event information		
Security alarm cause	M	—
Security alarm severity	M	—
Security alarm detector	M	—
Service user	M	—
Service provider	M	—
Notification identifier	U	—
Correlated notifications	U	—
Additional text	U	—
Additional information	U	—
Current time	—	P
Event reply	—	—
Errors	—	P

10 Functional units

The security alarm reporting function constitutes a single systems management functional unit.

11 Protocol

11.1 Elements of procedure

11.1.1 Agent role

11.1.1.1 Invocation

The security alarm reporting procedures are initiated by the security alarm reporting request primitive. On receipt of a security alarm reporting request primitive, the SMAPM shall construct an MAPDU and issue a CMIS M-EVENT-REPORT request service primitive with parameters derived from the security alarm reporting request primitive. In the non-confirmed mode, the procedure in 11.1.1.2 does not apply.

11.1.1.2 Receipt of response

On receipt of a CMIS M-EVENT-REPORT confirm service primitive containing an MAPDU responding to a security alarm reporting notification, the SMAPM shall issue a security alarm reporting confirmation primitive to the security alarm reporting service user with parameters derived from the CMIS M-EVENT-REPORT confirm service primitive, thus completing the security alarm reporting procedure.

NOTE — The SMAPM shall ignore all errors in the received MAPDU. The security alarm reporting service user may ignore such errors, or abort the association as a consequence of such errors.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

11.1.2 Manager role

11.1.2.1 Receipt of request

On receipt of a CMIS M-EVENT-REPORT indication service primitive containing an MAPDU requesting the security alarm reporting service, the SMAPM shall, if the MAPDU is well formed, issue a security alarm reporting indication primitive to the security alarm reporting service user with parameters derived from the CMIS M-EVENT-REPORT indication service primitive. Otherwise, the SMAPM shall in the confirmed mode construct an appropriate MAPDU containing notification of the error, and shall issue a CMIS M-EVENT-REPORT response service primitive with an error parameter present. In the non-confirmed mode, the procedure in 11.1.2.2 does not apply.

11.1.2.2 Response

In the confirmed mode, the SMAPM shall accept a security alarm reporting response primitive and shall construct an MAPDU confirming the notification and issue a CMIS M-EVENT-REPORT response service primitive with the parameters derived from the security alarm reporting response primitive.

11.2 Abstract syntax

11.2.1 Managed objects

This Recommendation | International Standard references the following support object, the abstract syntax of which is specified in CCITT Rec. X.721 | ISO/IEC 10165-2.

— securityAlarmReportRecord.

11.2.2 Attributes

Table 3 identifies the relationship between the parameters defined in 8.1.2 of this Recommendation | International Standard and the attribute type specifications in CCITT Rec. X.721 | ISO/IEC 10165-2.

Table 3 — Attributes

Parameter	Attribute name
Security alarm cause	securityAlarmCause
Security alarm severity	securityAlarmSeverity
Security alarm detector	securityAlarmDetector
Service user	serviceUser
Service provider	serviceProvider

11.2.3 Attribute groups

There are no attribute groups defined by this systems management function.

11.2.4 Actions

There are no specific actions defined by this systems management function.

11.2.5 Notifications

Table 4 identifies the relationship between the notifications defined in 8.1.1 of this Recommendation | International Standard and the notification type specifications in CCITT Rec. X.721 | ISO/IEC 10165-2.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 4 — Notifications

Security alarm type	Notification type
integrity violation	integrityViolation
operational violation	operationalViolation
physical violation	physicalViolation
security service or mechanism violation	securityServiceOrMechanismViolation
time domain violation	timeDomainViolation

The abstract syntax referenced by the notification type specifications is carried in the MAPDU.

11.2.6 Security alarm causes

Table 5 identifies the relationship between the security alarm causes defined in 8.1.2.1 of this Recommendation | International Standard and the ASN.1 value references defined in CCITT Rec. X.721 | ISO/IEC 10165-2.

Table 5 — Security alarm causes

Security alarm cause	ASN.1 value reference
authentication failure	authenticationFailure
breach of confidentiality	breachOfConfidentiality
cable tamper	cableTamper
delayed information	delayedInformation
denial of service	denialOfService
duplicate information	duplicateInformation
information missing	informationMissing
information modification detected	informationModificationDetected
information out of sequence	informationOutOfSequence
intrusion detection	intrusionDetection
key expired	keyExpired
non-repudiation failure	nonRepudiationFailure
out of hours activity	outOfHoursActivity
out of service	outOfService
procedural error	proceduralError
unauthorized access attempt	unauthorizedAccessAttempt
unexpected information	unexpectedInformation
unspecified reason	unspecifiedReason

11.2.7 Security alarm severity values

Table 6 identifies the relationship between the values defined for the security alarm severity parameter in 8.1.2.2 of this Recommendation | International Standard and the ASN.1 value references defined in CCITT Rec. X.721 | ISO/IEC 10165-2.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 6 — Security alarm severity values

Security alarm severity	ASN.1 value reference
indeterminate	indeterminate
critical	critical
major	major
minor	minor
warning	warning

11.3 Negotiation of security alarm reporting functional unit

This Recommendation | International Standard assigns the object identifier

{joint-iso-ccitt ms(9) function(2) part7(7) functionalUnitPackage(1)}

as a value of the ASN.1 type FunctionalUnitPackageId defined in CCITT Rec. X.701 | ISO/IEC 10040 to use for negotiating the following functional unit

0 security alarm reporting functional unit

where the number identifies the bit position assigned to the functional unit, and the name references the functional unit as defined in clause 10.

Within the Systems management application context, the mechanism for negotiating the security alarm reporting functional unit is described by CCITT Rec. X.701 | ISO/IEC 10040.

NOTE — The requirement to negotiate functional units is specified by the application context.

12 Relationships with other functions

Control of the security alarm reporting service is provided by mechanisms specified in CCITT Rec. X.734 | ISO/IEC 10164-5. The security alarm reporting service may exist independently of the control mechanisms of CCITT Rec. X.734 | ISO/IEC 10164-5.

13 Conformance

There are two conformance classes: general conformance class and dependent conformance class. A system claiming to implement the elements of procedure for the systems management services defined in this Recommendation | International Standard shall comply with the requirements for either the general or the dependent conformance class as defined in the following subclauses. The supplier of the implementation shall state the class to which conformance is claimed.

13.1 General conformance class requirements

A system claiming general conformance to this Recommendation | International Standard shall support this systems management function for all managed object classes that import management information defined by this Recommendation | International Standard.

13.1.1 Static conformance

The system shall

a) support the role of manager or agent or both, with respect to the security alarm reporting functional unit;

b) support the transfer syntax derived from the encoding rules specified in CCITT Rec. X.209 | ISO/IEC 8825 and named

{joint-iso-ccitt asn1(1) basic encoding(1)}

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

for the purpose of generating and interpreting the MAPDUs, defined by the abstract data types referenced in 11.2.5.

13.1.2 Dynamic conformance

The system shall, in the role(s) for which conformance is claimed, support the elements of procedure defined in this Recommendation | International Standard for the security alarm reporting service.

13.2 Dependent conformance class requirements

13.2.1 Static conformance

The system shall

a) supply a system conformance statement which identifies the standardized use of this systems management function;

b) support the transfer syntax derived from the encoding rules specified in CCITT Rec. X.209 | ISO/IEC 8825 and named

{joint-iso-ccitt asn1(1) basic encoding(1)}

for the purpose of generating and interpreting the MAPDUs, defined by the abstract data types referenced in 11.2.5, as required by a standardized use of this systems management function.

13.2.2 Dynamic conformance

The system shall support the elements of procedure defined in this Recommendation | International Standard as required by a standardized use of this systems management function.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

UDC 681.3:691.39

Descriptors: data processing, information interchange, network interconnection, open systems interconnection, application layer, management.

Price based on 13 pages

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale