INTERNATIONAL TELECOMMUNICATION UNION

CCITT X.736

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

DATA COMMUNICATION NETWORKS

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

Recommendation X.736

Geneva, 1992

Foreword

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The CCITT (the International Telegraph and Telephone Consultative Committee) is a permanent organ of the ITU representing some 166 member countries, 68 telecom operating entities, 163 scientific and industrial organizations and 39 international organizations and is the body which sets world telecommunications standards (Recommendations).

The approval of Recommendations by the members of CCITT is covered by the procedure laid down in CCITT Resolution No. 2 (Melbourne, 1988). In addition, the Plenary Assembly of CCITT, which meets every four years, approves Recommendations submitted to it and establishes the study programme for the following period.

In some areas of information technology which fall within CCITT's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC. The text of CCITT Recommendation X.736 was approved on 17 January 1992. The identical text is also published as ISO/IEC International Standard 10164-7.

CCITT NOTE

1) In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication Administration and a recognized private operating agency.

© ITU 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 ITU.

Contents

Information note III

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 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

INFORMATION NOTE

The following table gives a list of X.700 Series Recommendations which were, are being, or will be developed in collaboration with the ISO/IEC. Cross-references to the corresponding ISO/IEC International Standard number and the short title of the Recommendation | International Standard are provided.

CCITT Recommendation ISO/IEC International Standard	Short Title
X.700 | 7498-4	Management Framework
X.701 | 10040	System Management Overview
X.710 | 9595	Common Management Information Service Definition
X.711 | 9596-1	Common Management Information Protocol Specification
X.712 | 9596-2	CMIP PICS
X.720 | 10165-1	Management Information Model
X.721 | 10165-2	Definition of Management Information
X.722 | 10165-4	Guidelines for the Definition of Managed Objects
X.723 | 10165-5	Generic Management Information
X.724 | 10165-6	Guidelines for Implementation Conformance Statement Proformas associated with Management Information
X.730 | 10164-1	Object Management Function
X.731 | 10164-2	State Management Function
X.732 | 10164-3	Attributes for Representing Relationships
X.733 | 10164-4	Alarm Management Function
X.734 | 10164-5	Event Management Function
X.735 | 10164-6	Log Control Function
X.736 | 10164-7	Security Alarm Reporting Function
X.737 | 10164-14	Confidence and Diagnostic Test Classes Function
X.738 | 10164-13	Summarization Function
X.739 | 10164-11	Work Load Monitoring Function
X.740 | 10164-8	Security Audit Trail Function
X.741 | 10164-9	Objects and Attributes for Access Control
X.742 | 10164-10	Accounting Metering Function
X.743 | 10164-xx	Time Management Function
X.744 | 10164-xx	Software Management Function
X.745 | 10164-12	Test Management Function
X.746 | 10164-xx	Scheduling Function
X.747 | 10164-xx	General Relationship Model
X.748 | 10164-xx	Response Time Monitoring Function
X.749 | 10164-xx	Management Domain Management Function
X.749 | 10164-xx	Management Knowledge Management Function
X.750 | 10164-xx	Changeover Function
X.770 | See Note	MOCS and MICS for X.730 | 10164-1
X.771 | See Note	MOCS and MICS for X.731 | 10164-2
X.772 | See Note	MOCS and MICS for X.732 | 10164-3
X.773 | See Note	MOCS and MICS for X.733 | 10164-4
X.774 | See Note	MOCS and MICS for X.734 | 10164-5
X.775 | See Note	MOCS and MICS for X.735 | 10164-6
X.776 | See Note	MOCS and MICS for X.736 | 10164-7
X.780 | See Note	MOCS and MICS for X.740 | 10164-8
xx Part number of the ISO/IEC International Standard number still to be determined Note – ISO/IEC International Standard number still to be determined.	

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.

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.

– 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.

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

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.

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;

- 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.

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.

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.

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.

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.

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)}

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.