



INTERNATIONAL TELECOMMUNICATION UNION

**ITU-T**

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

**X.841**  
(10/2000)

**SERIES X: DATA NETWORKS AND OPEN SYSTEM  
COMMUNICATIONS**

**Security**

---

**Information technology – Security techniques –  
Security information objects for access control**

**ITU-T Recommendation X.841**

(Formerly CCITT Recommendation)

**ITU-T X-SERIES RECOMMENDATIONS**  
**DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS**

|                                               |                    |
|-----------------------------------------------|--------------------|
| <b>PUBLIC DATA NETWORKS</b>                   |                    |
| Services and facilities                       | X.1–X.19           |
| Interfaces                                    | X.20–X.49          |
| Transmission, signalling and switching        | X.50–X.89          |
| Network aspects                               | X.90–X.149         |
| Maintenance                                   | X.150–X.179        |
| Administrative arrangements                   | X.180–X.199        |
| <b>OPEN SYSTEMS INTERCONNECTION</b>           |                    |
| Model and notation                            | X.200–X.209        |
| Service definitions                           | X.210–X.219        |
| Connection-mode protocol specifications       | X.220–X.229        |
| Connectionless-mode protocol specifications   | X.230–X.239        |
| PICS proformas                                | X.240–X.259        |
| Protocol Identification                       | X.260–X.269        |
| Security Protocols                            | X.270–X.279        |
| Layer Managed Objects                         | X.280–X.289        |
| Conformance testing                           | X.290–X.299        |
| <b>INTERWORKING BETWEEN NETWORKS</b>          |                    |
| General                                       | X.300–X.349        |
| Satellite data transmission systems           | X.350–X.369        |
| IP-based networks                             | X.370–X.399        |
| <b>MESSAGE HANDLING SYSTEMS</b>               | X.400–X.499        |
| <b>DIRECTORY</b>                              | X.500–X.599        |
| <b>OSI NETWORKING AND SYSTEM ASPECTS</b>      |                    |
| Networking                                    | X.600–X.629        |
| Efficiency                                    | X.630–X.639        |
| Quality of service                            | X.640–X.649        |
| Naming, Addressing and Registration           | X.650–X.679        |
| Abstract Syntax Notation One (ASN.1)          | X.680–X.699        |
| <b>OSI MANAGEMENT</b>                         |                    |
| Systems Management framework and architecture | X.700–X.709        |
| Management Communication Service and Protocol | X.710–X.719        |
| Structure of Management Information           | X.720–X.729        |
| Management functions and ODMA functions       | X.730–X.799        |
| <b>SECURITY</b>                               | <b>X.800–X.849</b> |
| <b>OSI APPLICATIONS</b>                       |                    |
| Commitment, Concurrency and Recovery          | X.850–X.859        |
| Transaction processing                        | X.860–X.879        |
| Remote operations                             | X.880–X.899        |
| <b>OPEN DISTRIBUTED PROCESSING</b>            | X.900–X.999        |

*For further details, please refer to the list of ITU-T Recommendations.*

**INTERNATIONAL STANDARD 15816**

**ITU-T RECOMMENDATION X.841**

**INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – SECURITY  
INFORMATION OBJECTS FOR ACCESS CONTROL**

**Summary**

This Recommendation | International Standard provides object definitions that are commonly needed in security standards to avoid multiple and different definitions of the same functionality. Precision in these definitions is achieved by use of the Abstract Syntax Notation One (ASN.1).

This Recommendation | International Standard covers only static aspects of Security Information Objects (SIOs).

**Source**

ITU-T Recommendation X.841 was prepared by ITU-T Study Group 7 (1997-2000) and approved by the World Telecommunication Standardization Assembly (Montreal, 27 Septembre – 6 October 2000). An identical text is also published as ISO/IEC 15816.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

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

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

© ITU 2001

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 ITU.

# CONTENTS

|                                                                                            | <i>Page</i> |
|--------------------------------------------------------------------------------------------|-------------|
| 1 Scope .....                                                                              | 1           |
| 2 Normative references .....                                                               | 1           |
| 2.1 Identical Recommendations   International Standards .....                              | 1           |
| 2.2 Paired Recommendations   International Standards equivalent in technical content ..... | 2           |
| 3 Definitions .....                                                                        | 2           |
| 4 Abbreviations .....                                                                      | 2           |
| 5 Conventions .....                                                                        | 3           |
| 5.1 Security Information Object Class Description .....                                    | 3           |
| 5.2 Generic Security Information Object Class Correspondence .....                         | 3           |
| 5.3 Security Information Object Composition .....                                          | 3           |
| 6 Specification of Security Information Objects .....                                      | 3           |
| 6.1 Confidentiality Label .....                                                            | 3           |
| 6.1.1 Introduction .....                                                                   | 3           |
| 6.1.2 ASN.1 Specification of the Label .....                                               | 4           |
| 6.1.3 Binding Methods for Confidentiality Labels .....                                     | 5           |
| 6.2 Security Policy Information File .....                                                 | 5           |
| 6.2.1 Introduction .....                                                                   | 5           |
| 6.2.2 ASN.1 Specification of the Security Policy Information File .....                    | 6           |
| 6.3 Clearance Attribute .....                                                              | 9           |
| 6.3.1 Introduction .....                                                                   | 9           |
| 6.3.2 Definition of clearance attribute .....                                              | 10          |
| 7 Security Information Object Interaction .....                                            | 10          |
| 7.1 SIO Class Structure Comparison .....                                                   | 10          |
| 7.2 Security Information Object Interaction for Access Control .....                       | 10          |
| Annex A – Security Information Objects for Access Control in ASN.1 .....                   | 13          |
| Annex B – Expansion of the <b>SECURITY-CATEGORY</b> Syntax .....                           | 19          |

## Introduction

This Recommendation | International Standard on Security Information Objects (SIOs) for Access Control provides object definitions that are commonly needed in more than one security standard such that multiple and different definitions of the same functionality may be avoided. Precision in these definitions is achieved by use of the Abstract Syntax Notation One (ASN.1) defined in ITU-T Rec. X.680 (1997) | ISO/IEC 8824-1:1998, and ITU-T Rec. X.681 (1997) | ISO/IEC 8824-2:1998.

The aim of security management is to ensure that assets, including information, are protected appropriately and cost effectively. In order to protect proprietary interests and Intellectual Property Rights, organizations need to control the handling of their information. Severe damage or embarrassment can be caused to either the originator or holder of sensitive information, for example, if it is released to those not authorized to receive it (a breach of confidentiality), or if it is modified in any way (a breach of integrity). Each organization needs to ensure that it protects its own information and assets adequately in all forms during its storage, processing and transmission between and within organizations over both private and public networks. Organizations must be satisfied that their assets will be protected properly when they are held or processed by others if business is to be conducted more widely.

The motivation for development of SIOs for Access Control is the achievement of the flexibility and interoperability in security management that accrues from the use of common structures for similar functions. Standardization of security labels and alternative methods for access control have been pursued in this Recommendation | International Standard.

## INTERNATIONAL STANDARD

## ITU-T RECOMMENDATION

# INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – SECURITY INFORMATION OBJECTS FOR ACCESS CONTROL

## 1 Scope

The scope of this Recommendation | International Standard is:

- a) the definition of guidelines for specifying the abstract syntax of generic and specific Security Information Objects (SIOs) for Access Control;
- b) the specification of generic SIOs for Access Control;
- c) the specification of specific SIOs for Access Control.

The scope of this Recommendation | International Standard covers only the "statics" of SIOs through syntactic definitions in terms of ASN.1 descriptions and additional semantic explanations. It does not cover the "dynamics" of SIOs, for example rules relating to their creation and deletion. The dynamics of SIOs are a local implementation issue.

## 2 Normative references

The following 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 edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of ITU maintains a list of currently valid ITU-T Recommendations.

### 2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.411 (1999) | ISO/IEC 10021-4, *Information technology – Message Handling Systems (MHS): Message transfer system: Abstract service definition and procedures.*
- ITU-T Recommendation X.500 (2001) | ISO/IEC 9594-1:2001, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services.*
- ITU-T Recommendation X.501 (2001) | ISO/IEC 9594-2:2001, *Information technology – Open Systems Interconnection – The Directory: Models.*
- ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*
- ITU-T Recommendation X.680 (1997) | ISO/IEC 8824-1:1998, *Information technology – Abstract syntax notation one (ASN.1): Specification of basic notation.*
- ITU-T Recommendation X.681 (1997) | ISO/IEC 8824-2:1998, *Information technology – Abstract syntax notation one (ASN.1): Information object specification.*
- ITU-T Recommendation X.682 (1997) | ISO/IEC 8824-3:1998, *Information technology – Abstract syntax notation one (ASN.1): Constraint specification.*
- ITU-T Recommendation X.683 (1997) | ISO/IEC 8824-4:1998, *Information technology – Abstract syntax notation one (ASN.1): Parameterization of ASN.1 specifications.*
- ITU-T Recommendation X.690 (1997) | ISO/IEC 8825-1:1998, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).*

- 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.*
- ITU-T Recommendation X.741 (1995) | ISO/IEC 10164-9:1995, *Information technology – Open Systems Interconnection – Systems Management: Objects and attributes for access control.*
- ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model.*
- ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview.*
- ITU-T Recommendation X.830 (1995) | ISO/IEC 11586-1:1996, *Information technology – Open Systems Interconnection – Generic upper layers security: Overview, models and notation.*

## 2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*  
ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

## 3 Definitions

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

- 3.1 Compartmentalization:** As defined in ISO/IEC DIS 2382-8.
- 3.2 Generic SIO Class:** An SIO Class in which the data types for one or more of the components are not fully specified.
- 3.3 Information Object:** As defined in ITU-T Rec. X.681 | ISO/IEC 8824-2.
- 3.4 Information Object Class:** As defined in ITU-T Rec. X.681 | ISO/IEC 8824-2.
- 3.5 Object Identifier (OID):** As defined in ITU-T Rec. X.680 | ISO/IEC 8824-1.
- 3.6 Seal:** As defined in ITU-T Rec. X.810 | ISO/IEC 10181-1.
- 3.7 Security Authority:** The entity accountable for the administration of a security policy within a security domain.
- 3.8 Security Domain:** A collection of users and systems subject to a common security policy.
- 3.9 Security Information Object:** An instance of an SIO Class.
- 3.10 Security Information Object Class:** An Information Object Class that has been tailored for security use.
- 3.11 Security Label:** As defined in CCITT Rec. X.800 and ISO/IEC 7498-2.
- 3.12 Security Policy:** As defined in ISO/IEC DIS 2382-8.
- 3.13 Security Policy Information File:** A construct that conveys domain-specific security policy information.
- 3.14 Specific SIO Class:** An SIO Class in which the data types for all components are fully specified.

## 4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

|       |                              |
|-------|------------------------------|
| ASN.1 | Abstract Syntax Notation One |
| EE    | End Entity                   |
| IT    | Information Technology       |