INTERNATIONAL STANDARD

ISO/IEC 15816

First edition
2002-02-01

Information technology — Security techniques — Security information objects for access control

Technologies de l'information — Techniques de sécurité — Objets d'informations de sécurité pour le contrôle d'accès

Reference number
ISO/IEC 15816:2002(E)

© ISO/IEC 2002

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2002

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 either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

 © ISO/IEC 2002 – All rights reserved

CONTENTS

Page

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 **SECURITY-CATEGORY** Syntax 19

© ISO/IEC 2002 – All rights reserved

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

The main task of the joint technical committee is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15816 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*, in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.841.

Annex A forms a normative part of of this International Standard. Annex B is for information only.

© ISO/IEC 2002 – All rights reserved

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.

© ISO/IEC 2002 – All rights reserved

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.*