

---

---

**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*

iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

[ISO/IEC 15816:2002](https://standards.iteh.ai/catalog/standards/iso/6de33e66-5cf3-4485-a9ec-2631619c0eea/iso-iec-15816-2002)

<https://standards.iteh.ai/catalog/standards/iso/6de33e66-5cf3-4485-a9ec-2631619c0eea/iso-iec-15816-2002>



**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.

iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

ISO/IEC 15816:2002

<https://standards.iteh.ai/catalog/standards/iso/6de33e66-5c3b-4485-a9ec-2631619c0eea/iso-iec-15816-2002>

© 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](mailto:copyright@iso.ch)  
Web [www.iso.ch](http://www.iso.ch)

Printed in Switzerland

## 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 <b>SECURITY-CATEGORY</b> Syntax .....	19

<https://standards.iteh.ai/catalog/standards/iso/6de33e66-5cf3-4485-a9ec-2631619c0eea/iso-iec-15816-2002>

## 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.

iTeh Standards  
(<https://standards.itih.ai>)  
Document Preview

ISO/IEC 15816:2002

<https://standards.itih.ai/catalog/standards/iso/6de33e66-5cf3-4485-a9ec-2631619c0eea/iso-iec-15816-2002>

## 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.

# iTeh Standards (<https://standards.iteh.ai>) Document Preview

[ISO/IEC 15816:2002](https://standards.iteh.ai/catalog/standards/iso/6de33e66-5cf3-4485-a9ec-2631619c0eea/iso-iec-15816-2002)

<https://standards.iteh.ai/catalog/standards/iso/6de33e66-5cf3-4485-a9ec-2631619c0eea/iso-iec-15816-2002>



## 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.

<https://standards.iteh.ai/catalog/standards/iso/6de33e66-5cf3-4485-a9ec-2631619c0eea/iso-iec-15816-2002>

### 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 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 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



OID	Object Identifier
RBAC	Rule Based Access Control
SIO	Security Information Object
SPIF	Security Policy Information File

## 5 Conventions

### 5.1 Security Information Object Class Description

An SIO Class comprises:

- a value for a SIO Class identifier;
- a set of one or more data type specifications, one for each component the SIO Class contains; and
- a statement of the semantics associated with use of the SIO Class.

### 5.2 Generic Security Information Object Class Correspondence

A Generic SIO Class is an SIO Class in which the data types for one or more of the components are not fully specified. A Specific SIO Class is an SIO Class in which the data types for all components are fully specified. A generic SIO Class corresponds to a family of specific SIO Classes.

### 5.3 Security Information Object Composition

The specification of each SIO in this Recommendation | International Standard contains the following parts:

- a description of the SIO;
- an explanation of the usage of the SIO;
- a description of the components of the SIO.

The description of the components of the SIO includes the ASN.1 specification and the object identifier of the object class being defined.

<https://standards.iteh.ai/catalog/standards/iso/6de33e66-5c3b-4485-a9ec-2631619c0eea/iso-iec-15816-2002>

## 6 Specification of Security Information Objects

When a new requirement is identified for an SIO, the following steps shall be followed to encourage reuse of existing specifications and to reduce the proliferation of different specifications meeting the same requirements:

- If this Recommendation | International Standard defines an SIO that meets the new requirement, the definition in this Recommendation | International Standard shall be used.
- Components of SIOs defined in this Recommendation | International Standard should be used in the definition of the new SIO if they satisfy part of the new requirement.

Specifications of the SIOs that have been developed to support access control are included in the following subclauses. A complete ASN.1 definition for the Security Information Objects discussed in these subclauses is included as a module in Annex A. This module is identified as follows:

```
id-SIOsAccessControl-MODULE OBJECT IDENTIFIER ::= {
    joint-iso-itu-t sios(24) specification(0) modules(0) accessControl(0)}
```

### 6.1 Confidentiality Label

#### 6.1.1 Introduction

Organizations typically have one or more security policies that provide for the compartmentalization of data into groupings that are to be protected and handled in the same way. The security policy defines the protection to be applied to each compartment.

The aspects of security expressed by a security policy, indicated in a security label, include the following:

- the level of protection to be given to data stored on a system;
- who is authorized to access data, processes or resources;
- security markings required to be shown on any display or print of the material;
- routing and enciphering requirements for data transmitted between systems;
- requirements for protection against unauthorized copying;
- methods for storage of data;
- enciphering algorithms to be used;
- methods of authenticating entities;
- whether operations on the object are to be audited;
- whether preventing repudiation of receipt of an object by recipients is required;
- whether, and whose, digital signatures are required to authenticate the data.

When data is held on an Information Technology (IT) system, or when it is transmitted electronically between systems, the data are labelled to indicate the security compartment to which the data belongs and thus how the data is to be handled for security. The label may be separately identifiable from the protected information but is logically bound to it. The integrity of the labels, and the integrity of their binding to the information, must be assured. This allows IT systems and networks to make security-relevant decisions, such as access control and routing, without the need to access the information that is being protected. The security label may be associated with each data object in an IT system, such as documents, electronic mail messages, display windows, database entries, directory entries and electronic forms. The labels are intended for use when objects are stored, moved around (particularly between systems), and when they are being handled by applications that act on labels, including applications that create new objects from existing ones.

When labelled data is to be passed between different security domains, the domains should agree on a security policy to be applied to that data. If the labels specified by the policy applied within a domain differ from the labels specified by the policy for shared data, then the policy for the shared data shall specify how to translate between the two sets of labels.

Labels alone are not sufficient to ensure the security of information. The security policy that applies to the information needs to be enforced by each organization while the labelled information is within the scope of their control. All the organizations, individuals and IT systems that process an item of information are presumed to know the security policy for that information. Organizations that exchange information need to establish trust in one another to be satisfied that information will be handled according to agreed security policies. This trust is usually established through a formal agreement.

### 6.1.2 ASN.1 Specification of the Label

The confidentiality label is identified as follows:

```
id-ConfidentialityLabel OBJECT IDENTIFIER ::= {
    joint-iso-itu-t sios(24) specification(0) securityLabels(1) confidentiality(0)}

ConfidentialityLabel ::= SET {
    security-policy-identifier      SecurityPolicyIdentifier OPTIONAL,
    security-classification         INTEGER(0..MAX) OPTIONAL,
    privacy-mark                   PrivacyMark OPTIONAL,
    security-categories             SecurityCategories OPTIONAL }
(ALL EXCEPT{-- none; at least one component shall be present --}))

SecurityPolicyIdentifier ::= OBJECT IDENTIFIER

PrivacyMark ::= CHOICE {
    pString      PrintableString (SIZE(1..ub-privacy-mark-length)),
    utf8String   UTF8String (SIZE(1..ub-privacy-mark-length))
}

ub-privacy-mark-length INTEGER ::= 128 -- as defined in ITU-T Rec. X.411 | ISO/IEC 10021-4

SecurityCategories ::= SET SIZE (1..MAX) OF SecurityCategory

SecurityCategory ::= SEQUENCE {
    type [0] SECURITY-CATEGORY.&id ({SecurityCategoriesTable}),
    value  [1] SECURITY-CATEGORY.&Type ({SecurityCategoriesTable} {@type})
}
```