
**Information technology — Open Systems
Interconnection — Security frameworks for
open systems: Access control framework**

*Technologies de l'information — Interconnexion de systèmes
ouverts (OSI) — Cadres généraux pour la sécurité des systèmes ouverts:
Cadre général de contrôle d'accès*

Contents

	<i>Page</i>
1 Scope	1
2 Normative references	2
2.1 Identical Recommendations International Standards	2
2.2 Paired Recommendations International Standards equivalent in technical content	2
3 Definitions	2
4 Abbreviations	4
5 General discussion of access control	4
5.1 Goal of access control	4
5.2 Basic aspects of access control	5
5.2.1 Performing access control functions	5
5.2.2 Other access control activities	7
5.2.3 ACI forwarding	8
5.3 Distribution of access control components	9
5.3.1 Incoming access control	10
5.3.2 Outgoing access control	10
5.3.3 Interposed access control	10
5.4 Distribution of access control components across multiple security domains	10
5.5 Threats to access control	10
6 Access control policies	11
6.1 Access control policy expression	11
6.1.1 Access control policy categories	11
6.1.2 Groups and roles	11
6.1.3 Security labels	11
6.1.4 Multiple initiator access control policies	12
6.2 Policy management	12
6.2.1 Fixed policies	12
6.2.2 Administratively-imposed policies	12
6.2.3 User-selected policies	12
6.3 Granularity and containment	12
6.4 Inheritance rules	12
6.5 Precedence among access control policy rules	13
6.6 Default access control policy rules	13
6.7 Policy mapping through cooperating security domains	13
7 Access control information and facilities	13
7.1 ACI	13
7.1.1 Initiator ACI	14

© ISO/IEC 1996

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

7.1.2	Target ACI	14
7.1.3	Access request ACI	14
7.1.4	Operand ACI	14
7.1.5	Contextual information	14
7.1.6	Initiator-bound ACI	15
7.1.7	Target-bound ACI	15
7.1.8	Access request-bound ACI	15
7.2	Protection of ACI	15
7.2.1	Access control certificates	15
7.2.2	Access control tokens	16
7.3	Access control facilities	16
7.3.1	Management related facilities	16
7.3.2	Operation related facilities	17
8	Classification of access control mechanisms	19
8.1	Introduction	19
8.2	ACL scheme	20
8.2.1	Basic features	20
8.2.2	ACI	20
8.2.3	Supporting mechanisms	20
8.2.4	Variations of this scheme	21
8.3	Capability scheme	22
8.3.1	Basic features	22
8.3.2	ACI	22
8.3.3	Supporting mechanisms	22
8.3.4	Variation of this scheme – Capabilities without specific operations	22
8.4	Label based scheme	23
8.4.1	Basic features	23
8.4.2	ACI	23
8.4.3	Supporting mechanisms	23
8.4.4	Labeled channels as targets	24
8.5	Context based scheme	24
8.5.1	Basic features	24
8.5.2	ACI	25
8.5.3	Supporting mechanisms	25
8.5.4	Variations of this scheme	25
9	Interaction with other security services and mechanisms	25
9.1	Authentication	25
9.2	Data integrity	25
9.3	Data confidentiality	26
9.4	Audit	26
9.5	Other access-related services	26
Annex A	Exchange of access control certificates among components	27
A.1	Introduction	27
A.2	Forwarding access control certificates	27
A.3	Forwarding multiple access control certificates	27
A.3.1	Example	27
A.3.2	Generalization	28
A.3.3	Simplifications	28
Annex B	Access control in the OSI reference model	29
B.1	General	29
B.2	Use of access control within the OSI layers	29
B.2.1	Use of access control at the network layer	29
B.2.2	Use of access control at the transport layer	29
B.2.3	Use of access control at the application layer	29
Annex C	Non-uniqueness of access control identities	30

Annex D – Distribution of access control components	31
D.1 Aspects considered.....	31
D.2 AEC and ADC locations	31
D.3 Interactions among access control components	32
Annex E – Rule-based versus identity-based policies.....	34
Annex F – A mechanism to support ACI forwarding through an initiator.....	35
Annex G – Access control security service outline.....	36

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 10181-3 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 Recommendation X.812.

ISO/IEC 10181 consists of the following parts, under the general title *Information technology — Open Systems Interconnection — Security frameworks for open systems*:

- *Part 1: Overview*
- *Part 2: Authentication framework*
- *Part 3: Access control framework*
- *Part 4: Non-repudiation framework*
- *Part 5: Confidentiality framework*
- *Part 6: Integrity framework*
- *Part 7: Security audit framework*

Annexes A to G of this part of ISO/IEC 10181 are for information only.

Introduction

This Recommendation | International Standard defines a general framework for the provision of access control. The primary goal of access control is to counter the threat of unauthorized operations involving a computer or communications system; these threats are frequently subdivided into classes known as unauthorized use, disclosure, modification, destruction and denial of service.

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

**INFORMATION TECHNOLOGY –
OPEN SYSTEMS INTERCONNECTION –
SECURITY FRAMEWORKS FOR OPEN SYSTEMS:
ACCESS CONTROL FRAMEWORK**

1 Scope

The Security Frameworks are intended to address the application of security services in an Open Systems environment, where the term *Open Systems* is taken to include areas such as Database, Distributed Applications, ODP and OSI. The Security Frameworks are concerned with defining the means of providing protection for systems and objects within systems, and with the interactions between systems. The Security Frameworks are not concerned with the methodology for constructing systems or mechanisms.

The Security Frameworks address both data elements and sequences of operations (but not protocol elements) that are used to obtain specific security services. These security services may apply to the communicating entities of systems as well as to data exchanged between systems, and to data managed by systems.

In the case of Access Control, accesses may either be *to* a system (i.e. to an entity that is the communicating part of a system) or *within* a system. The information items that need to be presented to obtain the access, as well as the sequence of operations to request the access and for notification of the results of the access, are considered to be within the scope of the Security Frameworks. However, any information items and operations that are dependent solely on a particular application and that are strictly concerned with local access within a system are considered to be outside the scope of the Security Frameworks.

Many applications have requirements for security to protect against threats to resources, including information, resulting from the interconnection of Open Systems. Some commonly known threats, together with the security services and mechanisms that can be used to protect against them, in an OSI environment, are described in CCITT Rec. X.800 | ISO 7498-2.

The process of determining which uses of resources within an Open System environment are permitted and, where appropriate, preventing unauthorized access is called access control. This Recommendation | International Standard defines a general framework for the provision of access control services.

This Security Framework:

- a) defines the basic concepts for access control;
- b) demonstrates the manner in which the basic concepts of access control can be specialized to support some commonly recognized access control services and mechanisms;
- c) defines these services and corresponding access control mechanisms;
- d) identifies functional requirements for protocols to support these access control services and mechanisms;
- e) identifies management requirements to support these access control services and mechanisms;
- f) addresses the interaction of access control services and mechanisms with other security services and mechanisms.

As with other security services, access control can be provided only within the context of a defined security policy for a particular application. The definition of access control policies is outside the scope of this Recommendation | International Standard, however, some characteristics of access control policies are discussed.

It is not a matter for this Recommendation | International Standard to specify details of the protocol exchanges which may need to be performed in order to provide access control services.

This Recommendation | International Standard does not specify particular mechanisms to support these access control services nor the details of security management services and protocols.

A number of different types of standard can use this framework including:

- a) standards that incorporate the concept of access control;
- b) standards that specify abstract services that include access control;
- c) standards that specify uses of an access control service;
- d) standards that specify the means of providing access control within an Open System environment; and
- e) standards that specify access control mechanisms.

Such standards can use this framework as follows:

- standard types a, b, c, d, and e can use the terminology of this framework;
- standard types b, c, d, and e can use the facilities defined in clause 7 of this framework; and
- standard type e can be based upon the classes of mechanism defined in clause 8.

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 the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic 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.811(1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.
- ITU-T Recommendation X.880 (1994) | ISO/IEC 13712-1: 1995, *Information technology – Remote Operations: Concepts model 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*.