INTERNATIONAL STANDARD

ISO/IEC 10181-3

First edition
1996-09-15

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

Reference number
ISO/IEC 10181-3:1996(E)

Contents

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

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.*

3 Definitions

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

3.1 This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.800 | ISO 7498-2:

a) access control;

b) access control list;

c) accountability;

d) authentication;

e) authentication information;

f) authorization;

g) capability;

h) identity-based security policy;

i) rule-based security policy;

j) security audit;

k) security label;

l) security policy;

m) security service;

n) sensitivity.

3.2 This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.810 | ISO/IEC 10181-1:

a) secure interaction policy;

b) security certificate;

c) security domain;

d) security domain authority;

e) security information;

f) security policy rules;

g) security token;

h) trust.

3.3 This Recommendation | International Standard makes use of the following term defined in ITU-T Rec. X.200 | ISO/IEC 7498-1:

– real system.

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

3.4.1 **access control certificate**: A security certificate that contains ACI.

3.4.2 **Access Control Decision Information (ADI)**: The portion (possibly all) of the ACI made available to the ADF in making a particular access control decision.

3.4.3 **Access Control Decision Function (ADF)**: A specialized function that makes access control decisions by applying access control policy rules to an access request, ADI (of initiators, targets, access requests, or that retained from prior decisions), and the context in which the access request is made.

3.4.4 **Access Control Enforcement Function (AEF)**: A specialized function that is part of the access path between an initiator and a target on each access request and enforces the decision made by the ADF.

3.4.5 **Access Control Information (ACI)**: Any information used for access control purposes, including contextual information.

3.4.6 **access control policy**: The set of rules that define the conditions under which an access may take place.

3.4.7 **access control policy rules**: Security policy rules concerning the provision of the access control service.

3.4.8 **access control token**: A security token that contains ACI.

3.4.9 **access request**: The operations and operands that form part of an attempted access.

3.4.10 **access request access control decision information; access request ADI**: ADI derived from access request-bound ACI.

3.4.11 **access request access control information; access request ACI**: ACI about an access request.

3.4.12 **access request-bound access control information; access request-bound ACI**: ACI bound to an access request.

3.4.13 **clearance**: Initiator-bound ACI that can be compared with security labels of targets.

3.4.14 contextual information: Information about or derived from the context in which an access request is made (e.g. time of day).

3.4.15 initiator: An entity (e.g. human user or computer-based entity) that attempts to access other entities.

3.4.16 initiator access control decision information; initiator ADI: ADI derived from initiator-bound ACI.

3.4.17 initiator access control information; initiator ACI: ACI about an initiator.

3.4.18 initiator-bound access control information; initiator-bound ACI: ACI bound to an initiator.

3.4.19 operand access control decision information; operand ADI: ADI derived from operand-bound ACI.

3.4.20 operand access control information; operand ACI: ACI about the operands of an access request.

3.4.21 operand-bound access control information; operand-bound ACI: ACI bound to the operands of an access request.

3.4.22 retained ADI: ADI which has been retained by an ADF from earlier access control decisions for use in future access control decisions.

3.4.23 target: An entity to which access may be attempted.

3.4.24 target access control decision information; target ADI: ADI derived from target-bound ACI.

3.4.25 target access control information; target ACI: ACI about a target.

3.4.26 target-bound access control information; target-bound ACI: ACI bound to a target.

4 Abbreviations

ACI	Access Control Information
ADI	Access Control Decision Information
ADF	Access Control Decision Function
AEF	Access Control Enforcement Function
SI	Security Information
SDA	Security Domain Authority

5 General discussion of access control

5.1 Goal of access control

For the purpose of this Security Framework, 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.

The subgoals of this Security Framework are:

- control of access by processes (which may be acting on behalf of humans or other processes) to data, different processes or other computing resources;
- control of access within a security domain or across one or more security domains;
- control of access according to its context; for example, dependent on such factors as time of attempted access, location of the accessor or route of access;
- control of access that is reactive to changes in authorization during access.

5.2 Basic aspects of access control

The following subclauses describe abstract access control functions largely independent of access control policies and system designs. Access control in real systems is concerned with many types of entities, such as:

- physical entities (e.g. real systems);
- logical entities (e.g. OSI layer entities, files, organizations, and enterprises);
- human users.

Access control in real systems can require a complex set of activities. The activities are:

- establishing access control policy representation;
- establishing ACI representations;
- allocating ACI to elements (initiators, targets or access requests);
- binding ACI to elements;
- making ADI available to the ADF;
- performing access control functions;
- modification of ACI (any time after allocating ACI values; includes revocation);
- revocation of ADI.

These activities can be divided into two groups:

- the operational activities (making ADI available to the ADF and performing access control functions);
- and
- the management activities (all the remaining activities).

Some of the activities above may be grouped as a single identifiable activity within a real system. Although some access control activities necessarily precede others, there is often overlap among them and some activities may be performed repeatedly.

A detailed discussion of the notions involved in performing access control functions will be presented first since all the other activities support this one.

5.2.1 Performing access control functions

For the purpose of this subclause, the functions which are fundamental to access control are illustrated in Figures 5-1 and 5-2. Other functions may be necessary for the overall operation of access control. In later discussions, a variety of ways in which these functions may be implemented are presented, including different ways of distributing the access control functions and ACI, and different styles of communication among access control functions in the same or cooperating security domains.

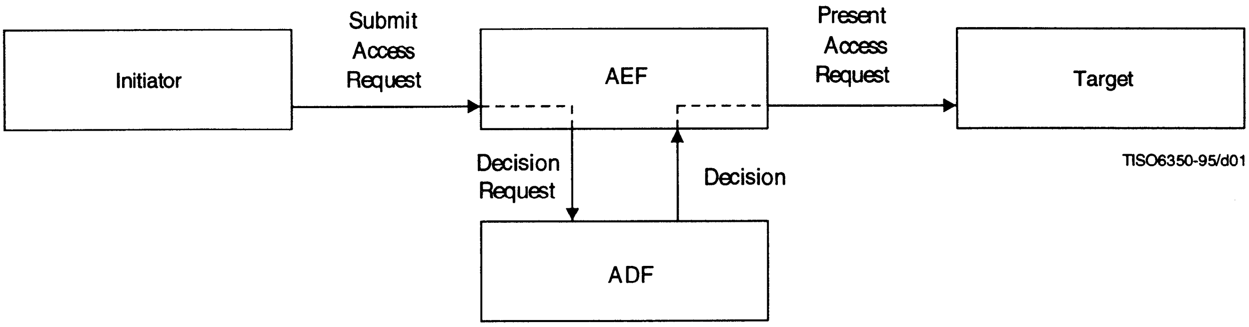

Figure 5-1 – Illustration of fundamental access control functions

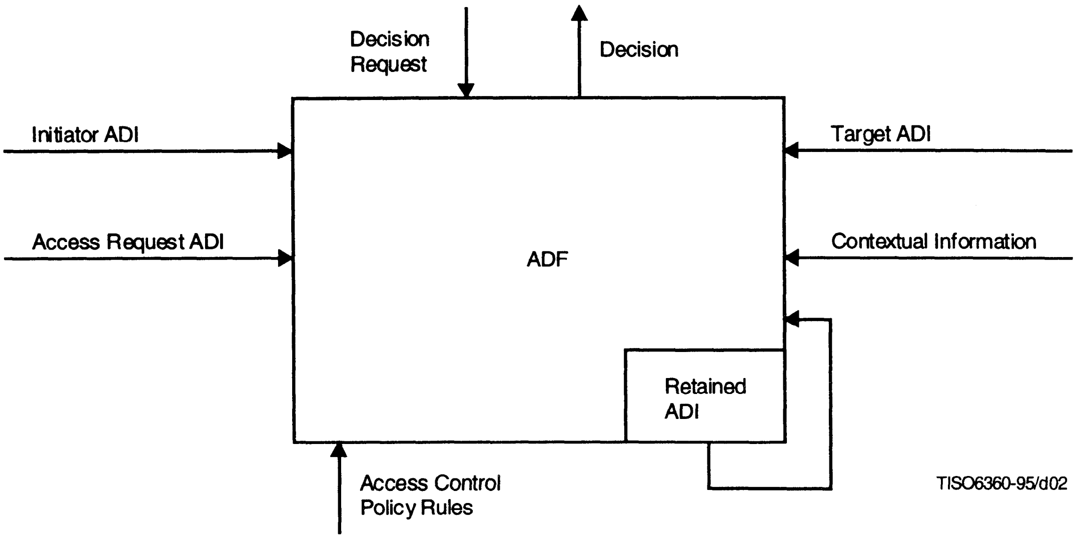

Figure 5-2 – Illustration of ADF

The basic entities and functions involved in access control are the initiator, the Access Control Enforcement function (AEF), the Access Control Decision Function (ADF), and the target.

Initiators represent both the human beings and computer-based entities that access or attempt to access targets. Within a real system, an initiator is represented by a computer-based entity, although the access requests of the computer-based entity on behalf of the initiator may be further limited by the ACI of the computer based-entity.

Targets represent computer-based or communications entities to which access is attempted or that are accessed by initiators. A target may be, for example, an OSI layer entity, a file, or a real system.

An access request represents the operations and operands that form part of an attempted access.

The AEF ensures that only allowable accesses, as determined by the ADF, are performed by the initiator on the target. When the initiator makes a request to perform a particular access on the target, the AEF informs the ADF that a decision is required so that a determination can be made.

In order to perform this decision, the ADF is provided with the access request (as part of the decision request) and the following types of Access Control Decision Information (ADI):

- initiator ADI (ADI derived from the ACI bound to the initiator);
- target ADI (ADI derived from the ACI bound to the target);
- access request ADI (ADI derived from the ACI bound to the access request).

The other inputs to the ADF are the access control policy rules (from the ADF's security domain authority), and any contextual information needed to interpret the ADI or policy. Examples of contextual information include the location of the initiator, the time of access, or the particular communications path in use.

Based on these inputs, and possibly from ADI retained from prior decisions, the ADF arrives at a decision to allow or deny the initiator's attempted access to the target. The decision is conveyed to the AEF which then either allows the access request to pass to the target or takes other appropriate actions.

In many situations, successive access requests by an initiator on a target are related. A typical example is in an application that opens a connection to a peer target application process and then attempts to perform several accesses using the same (retained) ADI. For some succeeding access requests communicated over the connection, additional ADI may need to be provided to the ADF for it to allow the access request. In other situations, a security policy may demand that certain related access requests between one or more initiators and one or more targets are subject to restrictions. In such cases, the ADF may use retained ADI from prior decisions involving multiple initiators and targets to make the decision on a particular access request.

For the purposes of this subclause, an access request involves a single interaction by an initiator with a target, if permitted by the AEF. Although some access requests between an initiator and a target are purely independent of others, it is often the case that two entities enter into a set of related access requests such as a query-response paradigm. In such cases, the initiator and target roles are assumed by the entities as necessary, either simultaneously or alternately, and the access control functions are carried out for each access request, possibly by separate AEF components, ADF components and access control policies.

5.2.2 Other access control activities

5.2.2.1 Establishing access control policy representations

Access control policies commonly are stated in natural languages as broad principles; for example: only managers of at least a certain rank are allowed to examine salary information of employees. The conversion of these principles into rules is an engineering design activity that necessarily precedes the other access control activities and is not within the scope of this Security Framework. An overview of access control policy concepts is given in clause 6.

5.2.2.2 Establishing ACI representations

In this activity, choices are made for the representation of ACI within real systems (data structures) and for exchange between real systems (syntaxes). A broad range of possible representations is discussed in this Security Framework. ACI representations must be able to support the requirements of specific access control policies. Some ACI representations may be appropriate both for use within and between real systems. Different ACI representations may be used for different purposes and among particular elements.

The chosen ACI representations can be considered as templates for the assignment of particular ACI values for elements in a security domain (as discussed in the next subclause). One aspect of establishing ACI representations is the determination of the types and ranges of the ACI values that may be assigned to elements in a security domain (but not which types can be assigned to specific elements).

Representation of ACI exchanged between real systems for access control management purposes or for ACI exchanges among entities and access control functions are candidates for OSI standardization. How ACI is represented within real systems or for presentation to a local ADF are not matters for OSI standardization. Protecting the exchange of ACI is discussed in 7.2. For OSI applications (and, possibly, others), it is appropriate to consider ACI representations as attributes which consist of attribute type-attribute value pairs.

5.2.2.3 Allocating ACI to initiators and targets

In this activity, the specific attribute types and attribute values of ACI assigned to an element are designated by an SDA, its agents, or other entities (e.g. resource owners). These entities may specify or modify ACI allocations in accordance with the security domain policy. ACI allocated by an entity may be limited by the ACI that has been bound to it by another entity. The allocation of ACI to elements is a continuing activity as new elements are added to a security domain.

NOTE – The administrative act of granting "access rights" is sometimes referred to as authorization. This meaning is included in the allocation of ACI to initiators or targets.

ACI can be either information about a single entity or information about a relationship among entities. The ACI allocated to an initiator may be purely about that initiator, or it may be about relationships between that initiator and particular targets, or about relationships between that initiator and possible contexts. Thus, the ACI allocated to an initiator may include initiator ACI, target ACI, or contextual information. Similarly, ACI allocated to a target may include target ACI, initiator ACI (about one or more initiators), or contextual information.

In actual operation, ACI must be bound to an element (see 5.2.2.4) so that an ADF that uses ADI derived from the bound ACI has confidence in that information. Thus, although the allocation of ACI to elements is a prerequisite to constructing bound ACI, only ACI that is bound to an element is actually present in real open systems.

5.2.2.4 Binding ACI to initiators, targets and access requests

Binding ACI to an element (i.e. an initiator, target or access request) creates a secure linkage between an element and the ACI allocated to that element. The binding provides assurance to access control functions and other elements both that the ACI is indeed assigned to the particular element and that no modification has occurred since the binding was made. Binding is achieved by using an integrity service. Several binding mechanisms are possible, including some that are dependent on the location of the element and the ACI, while others may depend on some cryptographic signing or sealing process. The integrity of the binding of ACI to elements needs to be protected within initiator and target systems (e.g. by relying upon operating system functions such as file protection and process separation) and, also, in the exchange of ACI. Since there may be several possible representations of an element's ACI (both within systems and between systems), different binding mechanisms may be used for the same ACI. Under some security policies, the confidentiality of ACI also needs to be maintained.