INTERNATIONAL STANDARD

ISO/IEC 10181-2

First edition
1996-05-15

Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework

Technologies de l'information — Interconnexion de systèmes ouverts: Cadre général d'authentification

INTERNATIONAL

Reference number
ISO/IEC 10181-2:1996(E)

CONTENTS

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 10181-2 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.811.

ISO/IEC 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*

— *Part 5: Confidentiality*

— *Part 6: Integrity*

— *Part 7: Security audit framework*

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

Introduction

Many applications have requirements for security to protect against threats to the communication of information. Some commonly known threats, together with the security services and mechanisms that can be used to protect against them, are described in ITU Rec. X.800 | ISO 7498-2.

Many Open Systems applications have security requirements which depend upon correctly identifying the principals involved. Such requirements may include the protection of assets and resources against unauthorized access, for which an identity based access control mechanism might be used, and/or the enforcement of accountability by the maintenance of audit logs of relevant events, as well as for accounting and charging purposes.

The process of corroborating an identity is called authentication. This Recommendation | International Standard defines a general framework for the provision of authentication services.

This page intentionally left blank

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SECURITY FRAMEWORKS FOR OPEN SYSTEMS: AUTHENTICATION FRAMEWORK

1 Scope

The series of Recommendations | International Standards on Security Frameworks for Open Systems addresses 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, Open Distributed Processing 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) which 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.

This Recommendation | International Standard:

- defines the basic concepts for authentication;
- identifies the possible classes of authentication mechanisms;
- defines the services for these classes of authentication mechanism;
- identifies functional requirements for protocols to support these classes of authentication mechanism; and
- identifies general management requirements for authentication.

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

1) standards that incorporate the concept of authentication;
2) standards that provide an authentication service;
3) standards that use an authentication service;
4) standards that specify the means to provide authentication within an open system architecture; and
5) standards that specify authentication mechanisms.

[Note that the service in 2), 3) and 4) might include authentication but may have a different primary purpose.]

These standards can use this framework as follows:

* standard types 1), 2), 3), 4) and 5) can use the terminology of this framework;
* standard types 2), 3), 4) and 5) can use the services defined in clause 7 of this framework; and
* standard types 5) can be based on the mechanisms defined in clause 8 of this framework.

As with other security services, authentication can only be provided within the context of a defined security policy for a particular application. The definitions of security policies are outside the scope of this ITU Recommendation | International Standard.

The scope of this Recommendation | International Standard does not include specification of details of the protocol exchanges which need to be performed in order to achieve authentication.

This Recommendation | International Standard does not specify particular mechanisms to support these authentication services. Other standards (such as ISO/IEC 9798) develop specific authentication methods in greater detail. Furthermore, examples of such methods are incorporated into other standards (such as ITU Rec. X.509 | ISO/IEC 9594-8) in order to address specific authentication requirements.

Some of the procedures described in this framework achieve security by the application of cryptographic techniques. This framework is not dependent on the use of a particular cryptographic or other algorithm, although certain classes of authentication mechanisms may depend on particular algorithm properties, e.g. asymmetric properties.

NOTE – Although ISO does not standardize cryptographic algorithms, it does standardize the procedures used to register them in ISO/IEC 9979.

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 Recommendations.

2.1 Identical Recommendations | International Standards

– ITU-T Recommendation X.810[1] | ISO/IEC 10181-1:...[1], *Information technology – Security frameworks for open systems: Overview.*

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.*

2.3 Additional references

– ISO/IEC 9979:1991, *Data cryptographic techniques – Procedures for the registration of cryptographic algorithms.*

– ISO/IEC 10116:1991, *Information technology – Modes of operation for an n-bit block cipher algorithm.*

3 Definitions

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

– audit;
– audit trail;
– authentication information;
– confidentiality;
– cryptography;
– cryptographic checkvalue;
– data origin authentication;
– data integrity;
– decipherment;
– digital signature;
– encipherment;
– key;

---

[1] Presently at the stage of draft.

- key management;
- masquerade;
- password;
- peer-entity authentication;
- security policy.

This Recommendation | International Standard makes use of the following term defined in ISO/IEC 10116:

- block chaining

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

- digital fingerprint;
- hash function;
- one-way function;
- private key;
- public key;
- seal;
- secret key;
- security authority;
- security certificate;
- security domain;
- security token;
- trust;
- trusted third party.

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

3.1 asymmetric authentication method: A method of authentication, in which not all authentication information is shared by both entities.

3.2 authenticated identity: A distinguishing identifier of a principal that has been assured through authentication.

3.3 authentication: The provision of assurance of the claimed identity of an entity.

3.4 authentication certificate: A security certificate that is guaranteed by an authentication authority and that may be used to assure the identity of an entity.

3.5 authentication exchange: A sequence of one or more transfers of exchange authentication information (AI) for the purposes of performing an authentication.

3.6 authentication information: Information used for authentication purposes.

3.7 authentication initiator: The entity that starts an authentication exchange.

3.8 challenge: A time variant parameter generated by a verifier.

3.9 claim authentication information (claim AI): Information used by a claimant to generate exchange AI needed to authenticate a principal.

3.10 claimant: An entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

3.11 distinguishing identifier: Data that unambiguously distinguishes an entity in the authentication process. This Recommendation | International Standard requires that such an identifier be unambiguous at least within a security domain.

3.12 exchange authentication information (exchange AI): Information exchanged between a claimant and a verifier during the process of authenticating a principal.

3.13 **off-line authentication certificate**: An authentication certificate binding a distinguishing identifier to verification AI, which may be available to all entities.

3.14 **on-line authentication certificate**: An authentication certificate for use in an authentication exchange, obtained directly by the claimant from the authority who guarantees it.

3.15 **principal**: An entity whose identity can be authenticated.

3.16 **symmetric authentication method**: A method of authentication in which both entities share common authentication information.

3.17 **time variant parameter**: A data item used by an entity to verify that a message is not a replay.

3.18 **unique number**: A time variant parameter generated by a claimant.

3.19 **verification authentication information (verification AI)**: Information used by a verifier to verify an identity claimed through exchange AI.

3.20 **verifier**: An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.

4 Abbreviations

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

AI Authentication Information

OSI Open Systems Interconnection

5 General discussion of authentication

5.1 Basic concepts of authentication

Authentication provides assurance of the claimed identity of an entity. Authentication is meaningful only in the context of a relationship between a principal and a verifier. Two important cases are:

- the principal is represented by a claimant which has a specific communications relationship with the verifier (entity authentication); and
- the principal is the source of a data item available to the verifier (data origin authentication).

This Recommendation | International Standard distinguishes between these two forms of authentication.

Entity authentication provides corroboration of the identity of a principal, within the context of a communication relationship. The principal's authenticated identity is assured only when this service is invoked. Assurance of continuity of authentication can be obtained as described in 5.2.7. An example of this is OSI peer-entity authentication as defined in CCITT Rec. X.800 | ISO 7498-2.

Data origin authentication provides corroboration of the identity of the principal that is responsible for a specific data unit.

NOTES

1 When using data origin authentication, it is also necessary to have adequate assurance that the data has not been modified. This may be accomplished by using an integrity service. For example:

a) by using environments in which data cannot be altered;

b) by verifying that the data received matches a digital fingerprint of the data sent;

c) by using a digital signature mechanism; and

d) by using a symmetric cryptographic algorithm.

2 The term communications relationship used in defining entity authentication may be interpreted in a broad way and could refer, for example, to an OSI connection, inter-process communication, or interaction between a user and a terminal.

5.1.1 Identification and authentication

A principal is an entity whose identity can be authenticated. A principal has one or more distinguishing identifiers associated with it. Authentication services can be used by entities to verify purported identities of principals. A principal's identity which has been so verified is called an authenticated identity.

Examples of principals that can be identified and hence authenticated are:

- human users;
- processes;
- real open systems;
- OSI layer entities; and
- enterprises.

Distinguishing identifiers are required to be unambiguous within a given security domain. Distinguishing identifiers distinguish a principal from others in the same domain, in one of two ways:

- at a coarse level of granularity, by virtue of membership in a group of entities considered equivalent for purposes of authentication (in this case the entire group is considered to be one principal and has one distinguishing identifier); or
- at the finest degree of granularity, identifying one and only one entity.

When authentication takes place between different security domains, a distinguishing identifier may not be sufficient to identify unambiguously an entity, as different security domain authorities may use the same distinguishing identifiers. In this case, distinguishing identifiers have to be used in conjunction with an identifier of the security domain in order to provide an unambiguous identifier for the entity.

Examples of typical distinguishing identifiers are:

- directory names (ITU-T Rec. X.509 | ISO/IEC 9594-8);
- network addresses (ITU-T Rec. X.213 | ISO/IEC 8348);
- AP-titles and AE-titles (ITU-T Rec. X.207 | ISO/IEC 9545);
- object identifiers (ITU Rec. X.208 | ISO/IEC 8824);
- names of persons (unambiguous within the context of the domain);
- passport or social security numbers.

5.1.2 Authentication entities

The term claimant is used to describe the entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

The term verifier is used to describe the entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.

An entity involved in mutual authentication (see 5.2.4) will assume both claimant and verifier roles.

The term trusted third party is used to describe a security authority or its agent, trusted by other entities with respect to security-related activities. In the context of this Recommendation | International Standard, a trusted third party is trusted by a claimant and/or a verifier for the purposes of authentication.

NOTE – The claimant or verifier may be refined into multiple functional components, possibly residing in different open systems.

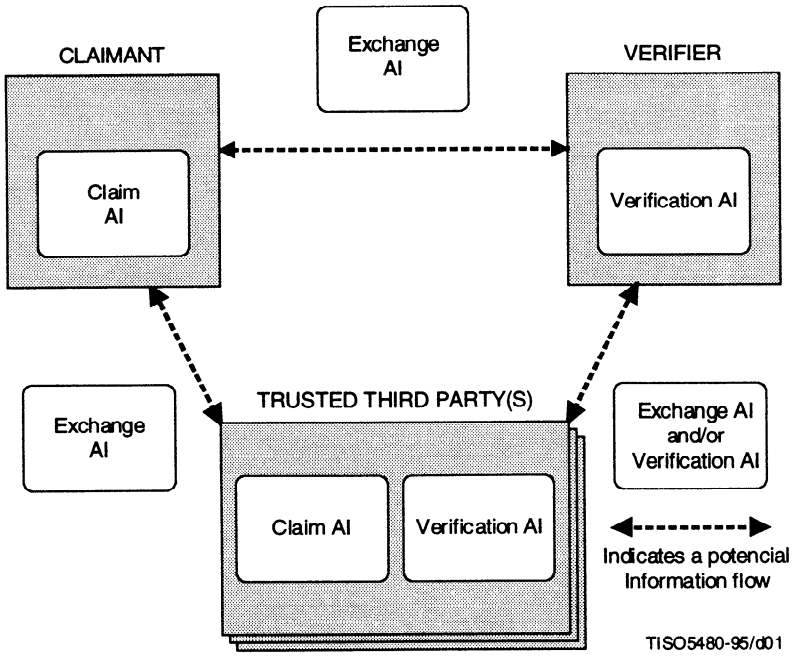
5.1.3 Authentication information

Types of authentication information are:

- exchange authentication information (exchange AI);
- claim authentication information (claim AI);
- verification authentication information (verification AI).

The term authentication exchange is used to describe a sequence of one or more transfers of exchange AI for the purposes of performing an authentication.

Figure 1 illustrates the relationship between claimant, verifier, trusted third party, and the three types of authentication information.



NOTES

1 In some scenarios no trusted third parties may be involved.

2 The verification AI may be that of the principal or that of the trusted third party (see 5.5 for further explanation).

Figure 1 – Illustration of relationship between claimant, verifier trusted third party, and types of authentication information

In some cases, in order to generate exchange AI, a claimant may need to interact with a trusted third party. Similarly, in order to verify exchange AI, a verifier may need to interact with a trusted third party. In these cases the trusted third party may hold verification AI related to a principal.

It is also possible that a trusted third party is used in the transfer of exchange AI.

The entities may also need to hold authentication information to be used in authenticating the trusted third party.

Examples of the three types of authentication information are given in 6.1.

NOTE – Because the term credentials is not always used in a consistent way in other Recommendations | International Standards, this Security Framework does not use this term. The term credentials as defined in ITU Rec. X.800 | ISO 7498-2 could be an example of exchange AI.

5.2 Aspects of authentication service

5.2.1 Threats to authentication

The goal of authentication is to provide assurance of an identity of a principal. Mechanisms to provide authentication normally must eliminate the threats of masquerade and replay.

Masquerade refers to the pretence by an entity to be a different entity. That is, the entity pretends to be another entity that is related to the verifier in a specific way (e.g. through the origin of data, or through a communications relationship). These types include replay, relay and compromise of claim AI.

A masquerade threat occurs in the context of an activity (e.g. origin of data, a communication relationship) initiated either by the claimant or the verifier. Protection against a masquerade threat to an activity requires the use of an integrity service to bind these data items to an authentication exchange. To counter masquerade-related threats, authentication must be used in conjunction with some form of integrity service, which binds the authenticated identity to the activity.

Replay refers to the repetition of exchange AI, to produce an unauthorized effect. Replay is usually used in combination with other attacks, such as data modification. Not all authentication mechanisms are equally resistant to replay. Replay can be a threat to other security services. Authentication can be used to counter replay since it offers a means to establish the source of the exchanged information.

5.2.2 Authentication forwarding

In some circumstances, a principal may have requirements to act within a system indirectly. In such cases, its representation within the system will have to be created. Moreover, before a representation for a principal can be created within a system, the principal must be authenticated.

When acting on the principal's behalf, the representation will be authenticated in place of the principal's identity. Because the representation acts as if it were the principal, the principal's actions can be carried on within the system without requiring the direct involvement of the principal. See Annex A for an example.

When the principal is a human user, mechanisms can be used which limit the lifetime of the representation to the period of time in which the user is physically present at a particular location.

A claimant, in acting on behalf of a principal, may access another system which creates its own representation of the principal following authentication. The creation of this representation is referred to as authentication forwarding.

The ability to forward authentication in such a manner may be affected by security policy.

5.2.4 Unilateral and mutual authentication

Authentication can be unilateral or mutual. Unilateral authentication provides assurance of the identity of only one principal. Mutual authentication provides assurance of the identities of both principals.

Entity authentication may be either mutual or unilateral. By its very nature, data origin authentication is always unilateral.

5.2.5 Initiation of an authentication exchange

An authentication exchange can be initiated by the claimant or the verifier. The entity which starts the exchange is called the authentication initiator.

5.2.6 Revocation of authentication information

Revocation of authentication information refers to the permanent invalidation of verification AI.

Policy may require the revocation of authentication information in certain situations. The decision to revoke authentication information may be based on detected security violation events, change of policy or other reasons. The revocation of authentication information may or may not imply revocation of existing access, or have other derivative effects.

In addition, the following management-related actions may be taken:

a) recording the event in the audit trail;

b) local reporting of the event;

c) remote reporting of the event; and/or

d) disconnection of a communication relationship.

The specific action to be taken for each event is dependent on the security policy in operation and other factors relating to the status of the communication relationship, e.g. whether or not an update occurred when the principal was logged in and active.

5.2.7 Assurance of continuity of authentication

Entity authentication only provides assurance of an identity at an instant of time. One way of obtaining the assurance of continuity of the authentication is by linking the authentication service with a data integrity service.

An authentication service and an integrity service are said to be linked when the principal is initially authenticated using an authentication service and further data sent on behalf of the principal is bound together with the exchange AI using an integrity service. This ensures that the later information may not be altered by any other entity and therefore must come from the initially authenticated principal. It is important that the integrity service is provided over the whole of the path that the information takes from the principal to the verifier. For example, masquerade is possible if some of the information can be produced by principals other than the one authenticated.

Another way to obtain assurance that the same remote entity is still present at a later time is to perform further authentication exchanges from time to time. However, this does not prevent intrusions during the intervals, hence no assurance of continuity is obtained. For example, the following attack is possible: an intruder, when called upon to do further authentication, allows the valid party to do the authentication actions; after these actions are complete the intruder again takes over.

If the integrity mechanism requires a key, that key may be derived from parameters specified during the authentication exchange. Having thus established that the key is associated with the authenticated principal, its use in the integrity mechanism will serve to link the two services provided as described above.

The way to derive a key for an integrity service can be specified as part of the parameters specifying which methods and algorithms should be used for the overall authentication exchange.

NOTE – When other security services are used, it is also possible to derive service information from parameters specified during the authentication exchange, e.g. a confidentiality key.

5.2.8 Distribution of authentication components across multiple domains

It is possible for security domains to enter into a relationship such that a claimant in one domain can be authenticated by a verifier in another domain. Multiple security domains may be involved, including:

- the security domain where the initiator resides;
- the security domain where the verifier resides;
- the security domain in which trusted third parties reside.

These domains need not all be distinct.

Before authentication can take place between different security domains, it is necessary to establish a secure interaction policy.

5.3 Principles used in authentication

In general, a particular authentication method will rely upon a chain of assumptions or expectations related to one or more principles.

The principles used include:

a) something known, e.g. a password;

b) something possessed, e.g. a magnetic card or a smart card;

c) some immutable characteristic, e.g. biometric identifiers;

d) accepting that a third entity (trusted third party) has established authentication; and

e) context, e.g. address of principal.

It should be noted that there are inherent weaknesses in all of the principles. For example, the authentication of something possessed is often the authentication of the possessed object rather than the authentication of its holder. In some cases the weaknesses may be overcome by the combination of several principles. For instance, when a smart card (something possessed) is used, the weakness may be overcome by the addition of a PIN (something known) in order to authenticate the user to the card. Moreover, principle e) is particularly weak and is virtually always used in conjunction with another principle.

Note that in d) there are two types of recursion:

- in order to be identified the third entity might itself require to be authenticated; and
- the authentication that the third entity establishes may use a fourth entity, etc.

Analysis of real authentication methods incorporating these principles will indicate the entities that are involved, the principles that are used, and the principals that are authenticated.

5.4 Phases of authentication

The following phases may occur in authentication:

- installation phase;
- change-authentication-information phase;
- distribution phase;
- acquisition phase;

- transfer phase;
- verification phase;
- disable phase;
- re-enable phase;
- de-installation phase.

The phases described here are not necessarily distinct in time, i.e. they may overlap.

Not all of these phases are required for a given authentication scheme. Also, in some cases, the sequencing of the phases may be different from the sequence implied by the following description.

5.4.1 Installation

In the installation phase, the claim AI and the verification AI are defined.

5.4.2 Change-authentication-information

In the change-authentication-information phase, a principal or a manager causes claim AI and verification AI to change (e.g. a password is changed).

5.4.3 Distribution

In the distribution phase verification AI is distributed to an entity (e.g. a claimant or a verifier) for use in verifying exchange AI. For example, in off-linc approaches, entities may obtain authentication certificates, certificate revocation lists and authority revocation lists. The distribution phase may occur before, during or after the transfer phase.

5.4.4 Acquisition

In the acquisition phase a claimant or verifier may obtain information required to generate specific exchange AI for an instance of authentication. Different procedures may acquire exchange AI by interaction with a trusted third party or by message exchange between authenticating entities.

For example, when using an on-line key distribution centre, the claimant or verifier may obtain some information, such as an authentication certificate (see 6.1.3), from the key distribution centre to enable authentication with the other entity.

5.4.5 Transfer

In the transfer phase, exchange AI is transferred between claimant and verifier.

5.4.6 Verification

In the verification phase, the exchange AI is checked against the verification AI. In this phase, an entity which is unable to verify the exchange AI itself may contact a trusted third party which will perform the verification of the exchange AI. In this case, the trusted third party will send back a positive or negative response.

5.4.7 Disable

In the disable phase, a state is established whereby a principal that previously could be authenticated is temporarily unable to be authenticated.

5.4.8 Re-enable

In the re-enable phase, the state established in a disable phase is terminated.

5.4.9 De-installation

In the de-installation phase, a principal is removed from the population of principals.

5.5 Trusted Third Party Involvement

Authentication mechanisms can be characterized by the number of trusted third parties involved.

5.5.1 Authentication without Trusted Third Party Involvement

In the simplest situation neither the claimant nor the verifier is supported by any other entity in the generation and verification of exchange AI. In this case, the verification AI for the principal must be already installed in the verifier.