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

Reference number
ISO/IEC 10181-2:1996(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 10181-2 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.

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.*

[1] Presently at the stage of draft.