INTERNATIONAL STANDARD

ISO/IEC 10181-4

First edition
1997-04-01

Information technology — Open Systems Interconnection — Security frameworks for open systems: Non-repudiation framework

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts: Cadre de non-répudiation

Reference number
ISO/IEC 10181-4:1997(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 10181-4 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.813.

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

— *Part 1: Overwiew*

— *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 and alarms framework*

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

Introduction

The goal of the Non-repudiation service is to collect, maintain, make available and validate irrefutable evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. The Non-repudiation service can be applied in a number of different contexts and situations. The service can apply to the generation of data, the storage of data, or the transmission of data. Non-repudiation involves the generation of evidence that can be used to prove that some kind of event or action has taken place, so that this event or action cannot be repudiated later.

In an OSI environment (see CCITT Rec. X.800 and ISO 7498-2) the Non-repudiation service has two forms:

- Non-repudiation with proof of origin which is used to counter false denial by a sender that the data or its contents has been sent.
- Non-repudiation with proof of delivery which is used to counter false denial by a recipient that the data or its contents (i.e. the information that the data represents) has been received.

Applications which make use of OSI protocols may require other forms of the Non-repudiation service which are specific to particular classes of applications. For example, MHS (ITU-T Rec. X.402 | ISO 10021-2) defines the Non-repudiation of submission service, while the EDI Messaging System (see Recommendation X.435) defines the Non-repudiation of retrieval and Non-repudiation of transfer services.

The concepts in this framework are not limited to OSI communications but may be interpreted more broadly to include such uses as creation and storage of data for later use.

This Recommendation | International Standard defines a general framework for the provision of a Non-repudiation service.

This framework:

- expands upon the concepts of Non-repudiation services described in CCITT Rec. X.800 and ISO 7498-2 and describes how they may be applied to Open Systems;
- describes alternatives for the provision of these services; and
- explains the relationship of these services to other security services.

Non-repudiation services may require:

- adjudicators who will arbitrate disputes that may arise as a result of repudiated events or actions; and
- Trusted Third Parties who will assure the authenticity and integrity of the data to be used for the verification of evidence.

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY — OPEN SYSTEMS INTERCONNECTION — SECURITY FRAMEWORKS FOR OPEN SYSTEMS: NON-REPUDIATION FRAMEWORK

1 Scope

This Recommendation | International Standard 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 of Non-repudiation;
- defines general Non-repudiation services;
- identifies possible mechanisms to provide the Non-repudiation services;
- identifies general management requirements for Non-repudiation services and mechanisms.

As with other security services, Non-repudiation 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 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 Non-repudiation.

This Recommendation | International Standard does not describe in detail the particular mechanisms that can be used to support the Non-repudiation services nor does it give details of the supporting security management services and protocols.

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 or on particular cryptographic techniques (i.e. symmetric or asymmetric) although certain classes of Non-repudiation mechanisms may depend on particular algorithm properties. Indeed it is likely, in practice, that a number of different algorithms will be used. Two entities wishing to use cryptographically-protected data must support the same cryptographic algorithm.

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

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

1) standards that incorporate the concept of Non-repudiation;
2) standards that specify abstract services that include Non-repudiation;
3) standards that specify uses of a Non-repudiation service;
4) standards that specify the means of providing Non-repudiation within an open system architecture; and
5) standards that specify Non-repudiation mechanisms.

Such standards can use this framework as follows:

- standards of type 1), 2), 3), 4) or 5) can use the terminology of this framework;
- standards of type 2), 3), 4) or 5) can use the facilities defined in clause 7; and
- standards of type 5) 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.509 (1993) | ISO/IEC 9594-8:1995, *Information technology – Open Systems Interconnection – The Directory: Authentication framework.*
- ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – 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.*