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

		Page
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
	3.1 Basic Reference Model definitions	2
	3.2 Security Architecture definitions	2
	3.3 Security Frameworks Overview definitions	3
	3.4 Additional definitions	3
4	Abbreviations	4
5	General discussion of Non-repudiation	4
	5.1 Basic concepts of Non-repudiation	4
	5.2 Roles of a Trusted Third Party	5
	5.3 Phases of Non-repudiation	5
	5.4 Some forms of Non-repudiation services	7
	5.5 Examples of OSI Non-repudiation evidence	8
6	Non-repudiation policies	8
7	Information and facilities	9
	7.1 Information	9
	7.2 Non-repudiation facilities	10
8	Non-repudiation mechanisms	12
	8.1 Non-repudiation using a TTP security token (secure envelope)	12
	8.2 Non-repudiation using security tokens and tamper-resistant modules	13
	8.3 Non-repudiation using a digital signature	13
	8.4 Non-repudiation using Time Stamping	13
	8.5 Non-repudiation using an in-line Trusted Third Party	14
	8.6 Non-repudiation using a Notary	14
	8.7 Threats to Non-repudiation	14

9 Interactions with other security services and mechanisms 16
9.1 Authentication 16
9.2 Access Control 16
9.3 Confidentiality 16
9.4 Integrity 16
9.5 Audit 16
Annex A – Non-repudiation in OSI Basic Reference Model 17
Annex B – Non-repudiation Facilities Outline 18
Annex C – Non-repudiation in store and forward systems 19
Annex D – Recovery in a Non-repudiation service 20
Annex E – Interaction with the Directory 22
Annex F – Bibliography 23

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.

This page intentionally left blank

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.*

3 Definitions

3.1 Basic Reference Model definitions

This Recommendation | International Standard builds on concepts developed in ITU-T Rec. X.200 | ISO/IEC 7498-1 and makes use of the following term defined in it:

(N)-entity.

3.2 Security Architecture definitions

This Recommendation | International Standard builds on the concepts developed in CCITT Rec. X.800 and ISO 7498-2 and makes use of the following terms defined in it:

- access control;
- audit (also security audit);
- authentication;
- channel;
- cryptographic checkvalue;
- cryptography;
- data integrity (also integrity);
- data origin authentication;
- decipherment;

- digital signature (also signature);
- encipherment;
- key;
- key management;
- notarization;
- repudiation;
- security audit trail (also audit trail, log);
- threat.

3.3 Security Frameworks Overview definitions

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

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

3.4 Additional definitions

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

3.4.1 compromised evidence: Evidence that was, at one time, satisfactory but which no longer has the confidence of the Trusted Third Party or adjudicator.

3.4.2 counter-signature: A digital signature appended to a data unit which has already been signed by a different entity (e.g. a TTP).

3.4.3 evidence: Information that, either by itself or when used in conjunction with other information, may be used to resolve a dispute.

3.4.4 evidence generator: An entity that produces Non-repudiation evidence.

NOTE – This entity may be the Non-repudiation service requester, the originator, the recipient or multiple parties working in conjunction (e.g. a signer and co-signer).

3.4.5 evidence subject: The entity whose involvement in an event or action is established by evidence.

3.4.6 evidence user: An entity that uses Non-repudiation evidence.

3.4.7 evidence verifier: An entity that verifies Non-repudiation evidence.

3.4.8 message authentication code: A cryptographic checkvalue that is used to provide data origin authentication and data integrity.

3.4.9 Non-repudiation service requester: An entity that requests that Non-repudiation evidence be generated for a particular event or action.

3.4.10 notary: A Trusted Third Party with whom data is registered so that later assurance of the accuracy of the characteristics of the data can be provided.

3.4.11 originator: In the context of data transfer, an entity that originates the data in an action that is subject to a Non-repudiation service.

3.4.12 recipient: In the context of data transfer, an entity that receives the data in an action that is subject to a Non-repudiation service.

NOTE – In the logical model of Non-repudiation, other entities may be considered. E.g. the owner is the entity that makes an original message and a transfer agent is the entity that transfers the message; in this context, entities are modeled as originators or recipients.

4 Abbreviations

OSI Open Systems Interconnection

CA Certification Authority

TTP Trusted Third Party

MAC Message Authentication Code

5 General discussion of Non-repudiation

5.1 Basic concepts of Non-repudiation

The Non-repudiation service involves the generation, verification and recording of evidence, and the subsequent retrieval and re-verification of this evidence in order to resolve disputes. Disputes cannot be resolved unless the evidence has been previously recorded.

The purpose of the Non-repudiation service described in this framework is to provide evidence about a particular event or action. Non-repudiation services may be requested by entities other than those involved in the event or action. Examples of actions which may be protected with a Non-repudiation service are:

- sending an X.400 message;
- inserting a record in a database; and
- invoking a remote operation.

When messages are involved, to provide proof of origin, the identity of the originator and the integrity of the data must be confirmed. To provide proof of delivery, the identity of the recipient, and the integrity of the data must be confirmed. In some cases, evidence concerning the context (e.g. date, time, location of the originator/recipient) may also be required.

The service provides the following facilities which can be used in the event of an attempted repudiation:

- generation of evidence;
- recording of evidence;
- verification of generated evidence;
- retrieval and re-verification of the evidence.

Disputes may be settled between parties directly through inspection of the evidence. However, a dispute may have to be resolved by an adjudicator who evaluates the evidence and determines whether or not the disputed action or event occurred. Adjudication can only be provided effectively if the parties to the dispute accept the authority of the adjudicator. For the evidence provided to be accepted by the adjudicator, it must usually be assured by one or more Trusted Third Parties. The adjudicator can optionally be the Trusted Third Party that assures the evidence. Non-repudiation mechanisms use a number of types of Trusted Third Parties and forms of evidence.

5.2 Roles of a Trusted Third Party

One or more Trusted Third Parties may be involved in the Non-repudiation service.

Trusted Third Parties which support Non-repudiation without being actively involved in each use of the service are known as Off-line Trusted Third Parties. A TTP which is actively involved in the generation or verification of evidence is known as an On-line TTP. An On-line TTP which acts as an intermediary in all interactions is known as an In-line TTP.

A Trusted Third Party may be required to record and/or gather evidence as well as being required to vouch for the validity of the evidence. There may be a number of Trusted Third Parties involved acting in various roles (e.g. Notary, Time Stamping, Monitoring, Key Certification, Signature Generation, Signature Verification, and Delivery Authority roles). A single Trusted Third Party may act in one or more of these roles.

In an Evidence Generation role, a TTP cooperates with a Non-repudiation service requester to generate evidence.

In an Evidence Recording role, a TTP records evidence that can later be retrieved by an evidence user or an adjudicator.

In a Time Stamping role, a TTP is trusted to provide evidence which includes the time when the time stamping request was received.

In a Monitoring role, a TTP monitors the action or the event and is trusted to provide evidence about what was monitored.

In a Key Certification role, a TTP provides Non-repudiation certificates related to an evidence generator in order to assure the validity of a public key to be used for Non-repudiation purposes.

In a Key Distribution role, a TTP provides keys to the evidence generators and/or the evidence verifiers. It may also place constraints on the use of the keys, in particular when symmetrical techniques are used.

In a Signature Generation role, a TTP is trusted to provide evidence in the form of a digital signature on behalf of the evidence subject.

In an Evidence Verification role, a TTP verifies evidence at the request of an entity.

In a Signature Verification role, a TTP is trusted by the evidence user to verify evidence in the form of a digital signature.

NOTE – The Signature Generation role is a particular case of the Evidence Generation role. The Signature verification role is a particular case of the evidence verification role.

In a Notary role, a TTP provides assurance about the properties of the data (such as its integrity, origin, time or destination) that are communicated between two or more entities and that have been previously registered with the TTP.

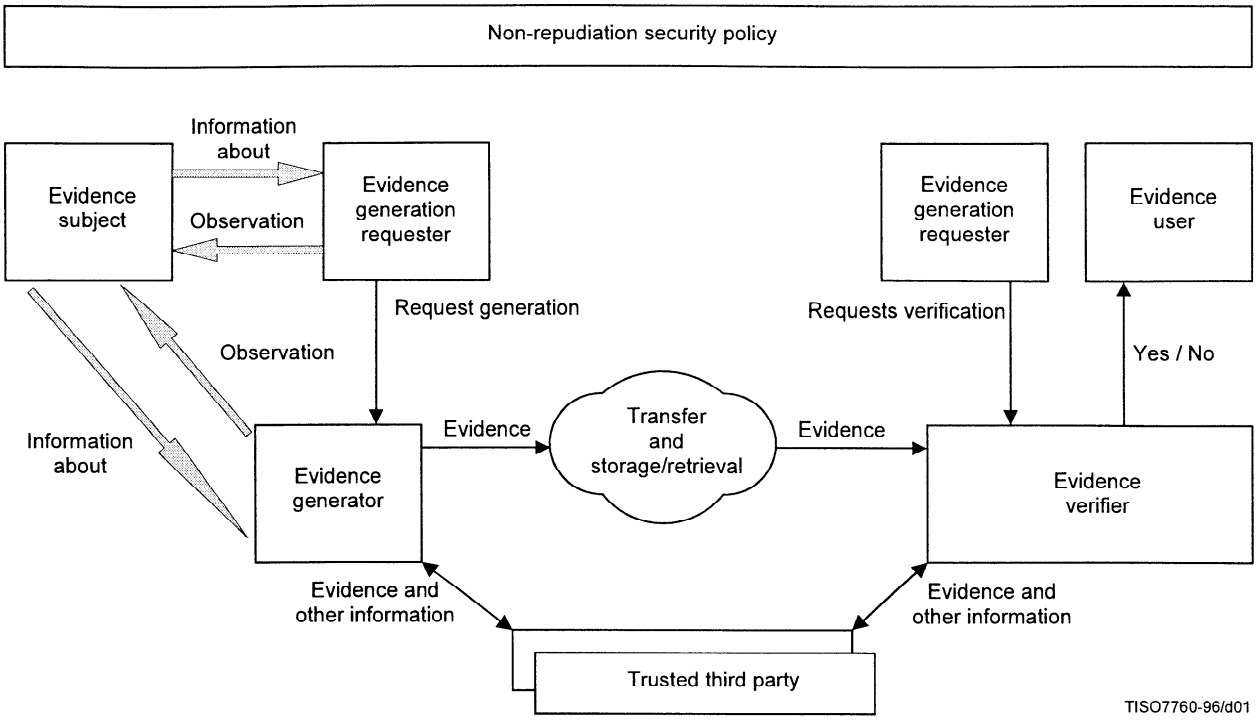
In a Delivery Authority role, a TTP interacts with the intended recipient of data and attempts to release the data to the recipient. It then provides evidence that the data was delivered, that the data was not delivered, or that delivery was attempted but that no confirmation of receipt was received. In the last case, the evidence user cannot determine whether the data was received by the intended recipient or not.

5.3 Phases of Non-repudiation

Non-repudiation is composed of four distinct phases:

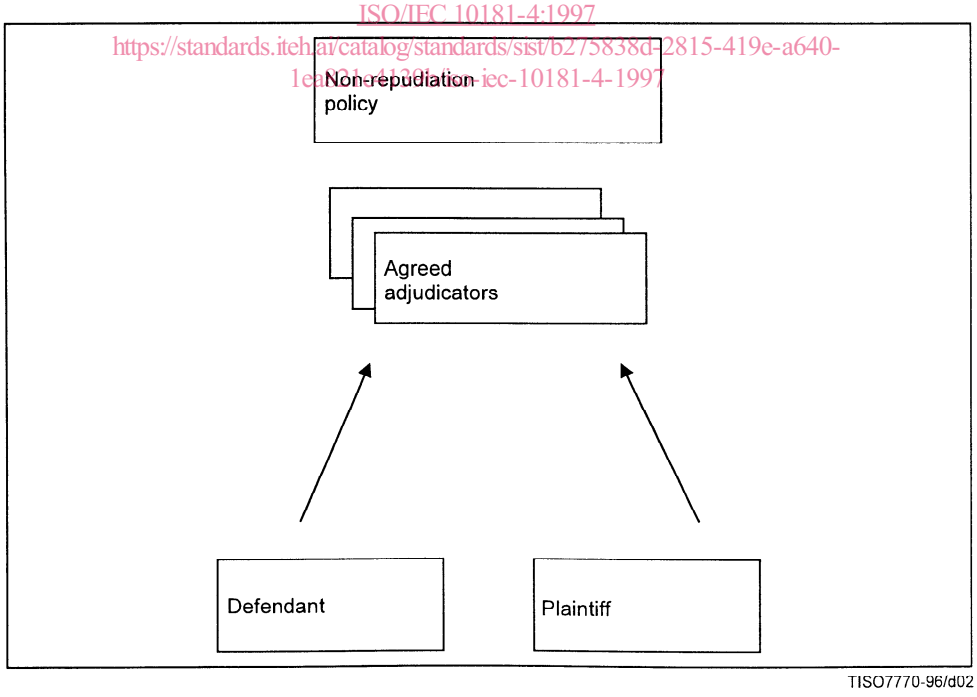
- evidence generation;
- evidence transfer, storage and retrieval;
- evidence verification; and
- dispute resolution.

Figure 1 illustrates the first three phases; Figure 2 illustrates the fourth phase.



NOTE – This figure is illustrative, not definitive.

Figure 1 – Entities involved in the generation, transfer, storage/retrieval and verification phases



NOTE – This figure is illustrative, not definitive.

Figure 2 – Dispute Resolution phase of a Non-repudiation process