INTERNATIONAL STANDARD

ISO/IEC 10181-6

First edition
1996-09-15

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

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres généraux pour la sécurité des systèmes ouverts: Cadre général d'intégrité

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10181-6:1996
https://standards.iteh.ai/catalog/standards/sist/d384206d-f95d-4f75-91eb-8046c34559dc/iso-iec-10181-6-1996

Reference number
ISO/IEC 10181-6:1996(E)

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10181-6:1996
https://standards.iteh.ai/catalog/standards/sist/d384206d-f95d-4f75-91eb-8046c3559dc/iso-iec-10181-6-1996

© ISO/IEC 1996

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

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

Printed in Switzerland

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10181-6:1996
https://standards.iteh.ai/catalog/standards/sist/d384206d-f95d-4f75-91eb-8046c34559dc/iso-iec-10181-6-1996

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 10181-6 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.815.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO/IEC 10181-6:1996
https://standards.iteh.ai/catalog/standards/sist/d384206d-f95d-4f75-91eb-8046c34559dc/iso-iec-10181-6-1996

- *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 C of this part of ISO/IEC 10181 are for information only.

Introduction

Many open systems applications have security requirements which depend upon the integrity of data. Such requirements may include the protection of data used in the provision of other security services such as authentication, access control, confidentiality, audit and non-repudiation, that, if an attacker could modify them, could reduce or nullify the effectiveness of those services.

The property that data has not been altered or destroyed in an unauthorized manner is called integrity. This Recommendation | International Standard defines a general framework for the provision of integrity services.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10181-6:1996
https://standards.iteh.ai/catalog/standards/sist/d384206d-f95d-4f75-91eb-8046c34559dc/iso-iec-10181-6-1996

This page intentionally left blank

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10181-6:1996
https://standards.iteh.ai/catalog/standards/sist/d384206d-f95d-4f75-91eb-8046c34559dc/iso-iec-10181-6-1996

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

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

1 Scope

The Recommendation | International Standard on Security Frameworks for Open Systems addresses the application of security services in an Open Systems environment, where the term "Open System" 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 may be 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 addresses the integrity of data in information retrieval, transfer, and management:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

1) defines the basic concept of data integrity;
2) identifies possible classes of integrity mechanism;
3) identifies facilities for each class of integrity mechanisms;
4) identifies management required to support the class of integrity mechanism;
5) addresses the interaction of integrity mechanism and the supporting services with other security services and mechanisms.

ISO/IEC 10181-6:1996
https://standards.iteh.ai/catalog/standards/sist/8046c34559dc/iso-iec-10181-6-1996

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

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

Such standards can use this framework as follows:

- standards of type 1), 2), 3), 4) and 5) can use the terminology of this framework;
- standards of type 2), 3), 4) and 5) can use the facilities identified in clause 7;
- standards of type 5) can be based upon the classes of mechanisms identified in clause 8.

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

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

The integrity addressed by this Recommendation | International Standard is that defined by the constancy of a data value. This notion (constancy of a data value) encompasses all instances in which different representations of a data value are deemed equivalent (such as different ASN.1 encodings of the same value). Other forms of invariance are excluded.

The usage of the term data in this Recommendation | International Standard includes all types of data structures (such as sets or collections of data, sequences of data, file-systems and databases).

This framework addresses the provision of integrity to data that are deemed to be write-accessible to potential attackers. Therefore, it focusses on the provision of integrity through mechanisms, both cryptographic and non-cryptographic that do not rely exclusively on regulating access.

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.273 (1994) | ISO/IEC 11577:1995, *Information technology – Open Systems Interconnection – Network layer security protocol.*
- ITU-T Recommendation X.274 (1994) | ISO/IEC 10736:1995, *Information technology – Telecommunications and information exchange between systems – Transport layer security protocol.*
- 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.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework.*

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10181-6:1996
https://standards.iteh.ai/catalog/standards/sist/d384206d-f95d-4f75-91eb-

2.2 Paired Recommendations | International Standards equivalent in technical content

- ITU-T Recommendation X.224 (1993), *Protocol for providing the OSI connection-mode transport service.*

  ISO/IEC 8073:1992, *Information technology – Telecommunications and information exchange between systems – Open Systems Interconnection – Protocol for providing the connection-mode transport service.*
- 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.*

3 Definitions

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

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

a) (N)-connection;

b) (N)-entity;

c) (N)-facility;

d) (N)-layer;

e) (N)-SDU;

f) (N)-service;

g) (N)-user-data.

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

a) access control;

b) connection integrity;

c) data integrity;

d) decipherment;

e) decryption;

f) digital signature;

g) encipherment;

h) encryption;

i) identity-based security policy;

j) integrity;

k) key;

l) routing control;

m) rule-based security policy.

NOTE – Where not otherwise qualified, the term "integrity" in this standard is taken to mean data integrity.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO/IEC 10181-6:1996
https://standards.iteh.ai/catalog/standards/sist/d384206d-f95d-4f75-91eb-8046c34559dc/iso-iec-10181-6-1996

a) digital fingerprint;

b) hash function;

c) one-way function;

d) private key;

e) public key;

f) seal;

g) secret key;

h) trusted third party.

3.4 This Recommendation | International Standard builds on concepts developed in ITU-T Rec. X.811 | ISO/IEC 10181-2 and makes use of the following terms defined in it:

– time variant parameter.

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

3.5.1 **integrity-protected channel**: A communications channel to which an integrity service has been applied.

NOTE – Two forms of integrity services for communication channels are referred to in CCITT Rec. X.800 | ISO 7498-2. These forms (connection and connectionless integrity) are described in annex A.

3.5.2 **integrity-protected environment**: An environment in which unauthorized data alterations (including creation and deletion) are prevented or detectable.

3.5.3 **integrity-protected data**: Data and all relevant attributes within an integrity-protected environment.

3.5.4 **shield**: The conversion of data into integrity-protected data.

3.5.5 **unshield**: The conversion of integrity protected data into the data originally shielded.

3.5.6 **validate**: The checking of integrity-protected data to detect loss of integrity.

4 Abbreviations

PDU Protocol Data Unit

SDU Service Data Unit

SII Shield Integrity Information

MDII Modification Detection Integrity Information

UII Unshield Integrity Information

5 General discussion of integrity

The purpose of the integrity service is to protect the integrity of data and of their relevant attributes which can be compromised in a number of different ways:

1) unauthorized data modification;
2) unauthorized data deletion;
3) unauthorized data creation;
4) unauthorized data insertion;
5) unauthorized data replay.

The integrity service protects against these threats either by means of prevention or by detection with or without recovery. Effective integrity protection may not be possible if the necessary control information (such as keys and SII) is not integrity and/or confidentiality protected; such protection often relies, implicitly or explicitly, on principles different from the ones embodied in the mechanism that protects the data.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The notion of protected environments is explicitly used in this framework so as to capture the idea that integrity protection includes protection against unauthorized creation and/or deletion. Thus, unauthorized data creation/deletion can be seen as unauthorized modifications of some protected environment. Similarly, insertion and replays can be seen as modifications of a structured collection of data (such as a sequence, or a data structure).

ISO/IEC 10181-6:1996
https://standards.iteh.ai/catalog/standards/sist/...

We note that some alterations of data can be seen as having no impact on their integrity. For instance, if an ASN.1 description contains a **SET OF** data type, there is no integrity violation if the members of the data type are reordered. Sophisticated integrity mechanisms may recognize that some transformations of structured data do not compromise the data integrity. Such mechanisms allow transformations of signed or sealed data without necessitating recomputations of the digital signature or seal, respectively.

The objective of the integrity service is to protect against or to detect unauthorized data modifications, including unauthorized data creation and deletion. The provision of the integrity service is accomplished through the following activities:

1) **shield**: the generation of integrity protected data from data;
2) **validate**: the checking of integrity-protected data to detect integrity failure;
3) **unshield**: the regeneration of data from integrity-protected data.

These activities do not necessarily employ cryptographic techniques. When they do use cryptographic techniques, they do not necessarily transform the data. For instance, the **shield** operation may be provided by appending a seal or a digital signature to the data. In this case, after successful **validation**, **unshielding** is performed through seal/digital signature removal.

The integrity service applies to Information Retrieval, Transfer, and Management as follows:

1) For information being transferred in an OSI environment, the integrity service is provided by combining **shielding,** transfer using an (N-1)-facility, and **unshielding** to form the transmission part of an (N)-service.
2) For data storage and retrieval, the integrity service is provided by combining **shielding**&storage and retrieval&**unshielding**.

Both **shielding** and **unshielding** can be provided as parallel operations such that the same data [for example, all the data of an (N)-connection] may consist simultaneously of parts that have not yet been **shielded**, parts that are held as integrity-protected data, and parts that have been **unshielded**.

Integrity mechanisms provide protected environments and hence both the **shield** and **unshield** stages involve the transfer of data between protected environments. Where integrity-protected data is transferred from an environment protected by one integrity mechanism to another the **shield** of the second mechanism should precede the **unshield** of the first in order for the data to be continuously protected.

5.1 Basic concepts

Several types of integrity service can be distinguished depending on what data activity is addressed (creation, deletion, modification, insertion, and/or replay), on whether the prevention or just the detection of a violation is required, and on whether they support data recovery in the event of an integrity violation. The different types of integrity service are described in 5.2.

The mechanisms that can be used as a means to provide these services can be split into broad categories that depend on the level of systematic activity assumed in an attempted integrity violation. These different types of mechanism are described in 5.3.

5.2 Types of integrity services

Integrity services are classified according to the following criteria:

1) By the type of violation they protect against. The types of violation are:
   a) unauthorized data modification;
   b) unauthorized data creation;
   c) unauthorized data deletion;
   d) unauthorized data insertion;
   e) unauthorized data replay;
2) By the type of protection they support. The types of protection are:
   a) prevention of integrity compromise;
   b) detection of integrity compromise;
3) By whether they include recovery mechanisms or not:

   In the former case (with recovery), the **unshield** operation may be able to recover the original data (and possibly signal a recovery action or an error for purposes such as audit) whenever the **validate** operation indicates alteration.

   In the latter (without recovery), the **unshield** operation is unable to recover the original data whenever the **validate** operation indicates alteration.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10181-6:1996
https://standards.iteh.ai/catalog/standards/sist/384206d-f95d-4f75-91eb-8046c34559dc/iso-iec-10181-6-1996

5.3 Types of integrity mechanisms

As a rule, the ability to protect data depends on the medium in use. Some media are, by their very nature, hard to protect (such as removable storage media or communication media) and as a result unauthorized parties can obtain access and engineer data modifications at will. In such media, the purpose of the integrity mechanism is to provide detection of modification and, possibly, restoration of the affected data. The following instances of integrity mechanism are therefore distinguished:

1) Those that prevent access to the medium. Such mechanisms include:
   a) physically isolated, noise free, channels;
   b) routing control;
   c) Access Control.
2) Those that detect unauthorized modifications of data or sequences of data items, including the cases of unauthorized data creation, data deletion, and data replication. Such mechanisms include:
   a) seals;
   b) digital signatures;
   c) data replication (used as a means of combatting other types of violation);
   d) digital fingerprints in conjunction with cryptographic transformations;
   e) message sequence numbers.