INTERNATIONAL STANDARD

ISO/IEC 10181-1

First edition
1996-08-01

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

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadre pour la sécurité dans les systèmes ouverts: Présentation

Reference number
ISO/IEC 10181-1:1996(E)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

CONTENTS

		Page
1	Scope	1
2	Normative references	1
	2.1 Identical Recommendations | International Standards	1
	2.2 Paired Recommendations | International Standards equivalent in technical content	1
3	Definitions	2
	3.1 Basic Reference Model definitions	2
	3.2 Security architecture definitions	2
	3.3 Additional definitions	2
4	Abbreviations	4
5	Notation	4
6	Organization	4
	6.1 Part 1 – Overview	4
	6.2 Part 2 – Authentication	4
	6.3 Part 3 – Access control	5
	6.4 Part 4 – Non-repudiation	5
	6.5 Part 5 – Confidentiality	5
	6.6 Part 6 – Integrity	6
	6.7 Part 7 – Security audit and alarms	6
	6.8 Key management	6
7	Common concepts	6
	7.1 Security information	7
	7.2 Security domain	7
	7.2.1 Security policy and security policy rules	7
	7.2.2 Security domain authority	8
	7.2.3 Inter-relationships among security domains	8
	7.2.4 Establishment of secure interaction rules	9
	7.2.5 Inter-domain security information transfer	9
	7.3 Security policy considerations for specific security services	9
	7.4 Trusted entities	9
	7.5 Trust	10
	7.6 Trusted third parties	10
8	Generic security information	10
	8.1 Security labels	10
	8.2 Cryptographic checkvalues	11
	8.3 Security certificates	11
	8.3.1 Introduction to security certificates	11
	8.3.2 Verification and chaining of security certificates	12
	8.3.3 Revocation of security certificates	12
	8.3.4 Re-use of security certificates	12
	8.3.5 Security certificate structure	12
	8.4 Security tokens	13

© 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 micro-film, without permission in writing from the publisher.

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

Printed in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

9 Generic security facilities 13
9.1 Management related facilities 13
9.1.1 Install SI 13
9.1.2 Deinstall SI 13
9.1.3 Change SI 13
9.1.4 Validate SI 14
9.1.5 Invalidate SI 14
9.1.6 Disable/Re-enable security service 14
9.1.7 Enrol 14
9.1.8 Un-enrol 14
9.1.9 Distribute SI 14
9.1.10 List SI 14
9.2 Operational related facilities 14
9.2.1 Identify trusted security authorities 14
9.2.2 Identify secure interaction rules 14
9.2.3 Acquire SI 14
9.2.4 Generate SI 14
9.2.5 Verify SI 15
10 Interactions between security mechanisms 15
11 Denial of service and availability 15
12 Other requirements 16
Annex A – Some examples of protection mechanisms for security certificates 17
A.1 Protection using an OSI communications security service 17
A.2 Protection using a parameter within the security certificate 17
A.2.1 The authentication method 17
A.2.2 The secret key method 17
A.2.3 The public key method 18
A.2.4 The one-way function method 18
A.3 Protection of the internal and external parameters while in transit 18
A.3.1 Transfer of internal parameters to the issuing security authority 18
A.3.2 Transfer of external parameters among entities 18
A.4 Use of security certificates by single entities or by groups of entities 19
A.5 Linking a security certificate with accesses 19
Annex B – Bibliography 20

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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 10181-1 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.810.

ISO/IEC 10181 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 framework*

— *Part 5: Confidentiality framework*

— *Part 6: Integrity framework*

— *Part 7: Security audit and alarms framework*

Annexes A and B of this part of ISO/IEC 10181 are for information only.

--`,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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 CCITT Rec. X.800 | ISO 7498-2.

This Recommendation | International Standard defines the framework within which security services for open systems are specified.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

This page intentionally left blank

--`,,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SECURITY FRAMEWORKS FOR OPEN SYSTEMS: OVERVIEW

1 Scope

The security frameworks address 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, ODP 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.

The security frameworks provide the basis for further standardization, providing consistent terminology and definitions of generic abstract service interfaces for specific security requirements. They also categorize the mechanisms that can be used to achieve those requirements.

One security service frequently depends on other security services, making it difficult to isolate one part of security from the others. The security frameworks address particular security services, describe the range of mechanisms that can be used to provide the security services, and identify interdependancies between the services and the mechanisms. The description of these mechanisms may involve a reliance on a different security service, and it is in this way that the security frameworks describe the reliance of one security service on another.

This part of the security frameworks:

- describes the organization of the security frameworks;
- defines security concepts which are required in more than one part of the security frameworks;
- describes the inter-relationship of the services and mechanisms identified in other parts of the frameworks.

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 indicated 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 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.*

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.*

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3 Definitions

The following definitions are used either in the overview or are common to two or more of the subsequent parts of the security frameworks.

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

3.1 Basic Reference Model definitions

This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.200 | ISO/IEC 7498-1:

- (N)-layer;
- (N)-entity;
- (N)-protocol-data-unit;
- application process;
- real open system;
- real system.

3.2 Security architecture definitions

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

- access control;
- availability;
- ciphertext;
- cryptographic checkvalue;
- decipherment;
- denial of service;
- digital signature;
- encipherment;
- insider threat;
- key;
- key management;
- plaintext;
- outsider threat;
- security audit;
- security label;
- security policy;
- sensitivity;
- threat.

3.3 Additional definitions

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

3.3.1 asymmetric cryptographic algorithm: An algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ.

NOTE – With some asymmetric cryptographic algorithms, decipherment of ciphertext or the generation of a digital signature requires the use of more than one private key.

3.3.2 certification authority: An entity that is trusted (in the context of a security policy) to create security certificates containing one or more classes of security-relevant data.

3.3.3 conditionally trusted entity: An entity that is trusted in the context of a security policy, but which cannot violate the security policy without being detected.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.3.4 cryptographic chaining: A mode of use of a cryptographic algorithm in which the transformation performed by the algorithm depends on the values of previous inputs or outputs.

3.3.5 digital fingerprint: A characteristic of a data item, such as a cryptographic checkvalue or the result of performing a one-way hash function on the data, that is sufficiently peculiar to the data item that it is computationally infeasible to find another data item that will possess the same characteristics.

3.3.6 distinguishing identifier: Data that uniquely identifies an entity.

3.3.7 hash function: A (mathematical) function that maps values from a (possibly very) large set of values into a smaller range of values.

3.3.8 one-way function: A (mathematical) function that is easy to compute but, when knowing a result, it is computationally infeasible to find any of the values that may have been supplied to obtain it.

3.3.9 one-way hash function: A (mathematical) function that is both a one-way function and a hash function.

3.3.10 private key: A key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity).

3.3.11 public key: A key that is used with an asymmetric cryptographic algorithm and that can be made publicly available.

3.3.12 revocation certificate: A security certificate issued by a security authority to indicate that a particular security certificate has been revoked.

3.3.13 revocation list certificate: A security certificate that identifies a list of security certificates that have been revoked.

3.3.14 seal: A cryptographic checkvalue that supports integrity but does not protect against forgery by the recipient (i.e. it does not provide non-repudiation). When a seal is associated with a data element, that data element is said to be *sealed.*

NOTE – Although a seal does not by itself provide non-repudiation, some non-repudiation mechanisms make use of the integrity service provided by seals, e.g. to protect communications with trusted third parties.

3.3.15 secret key: A key that is used with a symmetric cryptographic algorithm. Possession of a secret key is restricted (usually to two entities).

3.3.16 security administrator: A person who is responsible for the definition or enforcement of one or more parts of a security policy.

3.3.17 security authority: An entity that is responsible for the definition, implementation or enforcement of security policy.

3.3.18 security certificate: A set of security-relevant data issued by a security authority or trusted third party, together with security information which is used to provide the integrity and data origin authentication services for the data.

NOTE – All certificates are deemed to be security certificates (see the relevant definitions in ISO 7498-2). The term *security certificate* is adopted in order to avoid terminology conflicts with ITU-T Rec. X.509 | ISO/IEC 9594-8 (i.e. the directory authentication standard).

3.3.19 security certificate chain: An ordered sequence of security certificates, in which the first security certificate contains security-relevant information, and each subsequent security certificate contains security information which can be used in the verification of previous security certificates.

3.3.20 security domain: A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain.

3.3.21 security domain authority: A security authority that is responsible for the implementation of a security policy for a security domain.

3.3.22 security information: Information needed to implement security services.

3.3.23 security recovery: Actions that are taken and procedures that are carried out when a violation of security is either detected or suspected to have taken place.

3.3.24 secure interaction rules: Security policy rules that regulate interactions between security domains.

3.3.25 security policy rules: A representation of a security policy for a security domain within a real system.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.3.26 security token: A set of data protected by one or more security services, together with security information used in the provision of those security services, that is transferred between communicating entities.

3.3.27 symmetric cryptographic algorithm: An algorithm for performing encipherment or the corresponding algorithm for performing decipherment in which the same key is required for both encipherment and decipherment.

3.3.28 trust: Entity X is said to *trust* entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.

3.3.29 trusted entity: An entity that can violate a security policy, either by performing actions which it is not supposed to do, or by failing to perform actions which it is supposed to do.

3.3.30 trusted third party: A security authority or its agent that is trusted with respect to some security-relevant activities (in the context of a security policy).

3.3.31 unconditionally trusted entity: A trusted entity that can violate a security policy without being detected.

4 Abbreviations

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

ACI Access Control Information

OSI Open Systems Interconnection

ODP Open Distributed Processing

SI Security Information

TTP Trusted Third Party

5 Notation

The layer notation used is the same as that defined in ITU-T Rec. X.200 | ISO/IEC 7498-1.

The term *service*, where not otherwise qualified, is used to refer to a security service.

The term *certificate*, where not otherwise qualified, is used to refer to a security certificate.

6 Organization

The security frameworks are parts of a multi-part International Standard (ISO/IEC 10181) and a series of ITU Recommendations. The security frameworks are described below. Additional security frameworks may be identified in the future. The key management framework is not a part of ISO/IEC 10181, but it has a similar scope and its description is included for completeness.

6.1 Part 1 – Overview

See clause 1.

6.2 Part 2 – Authentication

This framework describes all aspects of authentication as these apply to Open Systems, the relationship of authentication with other security functions such as access control and the management requirements for authentication.

This framework:

a) defines the basic concepts of authentication;

b) identifies the possible classes of authentication mechanisms;

c) defines the services for these classes of authentication mechanism;

d) identifies functional requirements for protocols to support these classes of authentication mechanism; and

e) identifies general management requirements for authentication.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The Authentication Framework occupies a position at the top of a hierarchy of authentication standards that provide concepts, nomenclature and a classification for authentication methods. Directly below it, standards such as ISO/IEC 9798 (Entity Authentication Mechanisms) provide a particular set of these methods in more detail. Finally, at the bottom of the hierarchy, standards such as ITU-T Rec. X.509 | ISO/IEC 9594-8 (the Directory Authentication Framework) use these concepts and methods in the context of a specific application or requirement.

The Authentication Framework describes a model of authentication, a number of phases into which authentication activities can be categorized, the use of a trusted third party, the use of authentication certificates to exchange authentication information, a generic authentication service based on these phases, and at least five classes of authentication mechanism which provide the generic authentication service. These include mechanisms protecting against disclosure of authentication information, and disclosure and replay on the same (and/or different) verifiers.

6.3 Part 3 – Access control

This framework describes all aspects of access control (e.g. user-to-processes, user-to-data, process-to-process, process-to-data) in Open Systems, the relationship to other security functions, such as authentication and audit, and the management requirements for access control.

This framework:

a) defines the basic concepts for access control;

b) demonstrates the manner in which the basic concepts of access control can be specialized to support some commonly recognized access control services and mechanisms;

c) defines these services and the corresponding access control mechanisms;

d) identifies functional requirements for protocols to support these access control services and mechanisms;

e) identifies management requirements to support these access control services and mechanisms;

f) addresses the interaction of access control services and mechanisms with other security services and mechanisms.

This security framework describes a model of access control, a number of phases into which access control activities can be categorized, a generic access control service based on these phases, and at least three classes of access control mechanism which provide the generic access control service. These include access control lists, capabilities and labels.

6.4 Part 4 – Non-repudiation

This framework refines and extends the concepts of the non-repudiation services described in CCITT Rec. X.800 | ISO 7498-2, and provides a framework for the development and provision of these services.

This framework:

a) defines the basic concepts for non-repudiation;

b) defines general non-repudiation services;

c) identifies possible mechanisms to provide the non-repudiation services;

d) identifies general management requirements for non-repudiation services and mechanisms.

6.5 Part 5 – Confidentiality

The purpose of the confidentiality service is to protect information from unauthorized disclosure. This framework addresses the confidentiality of information in retrieval, transfer and management.

This framework:

a) defines the basic concepts of confidentiality;

b) identifies possible classes of confidentiality mechanism;

c) defines facilities of each class of confidentiality mechanism;

d) identifies management required to support the classes of confidentiality mechanisms; and

e) addresses the interaction of the confidentiality mechanism and the supporting services with other security services and mechanisms.

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.6 Part 6 – Integrity

The property that data has not been altered or destroyed in an unauthorized manner is called integrity. This framework addresses the integrity of data in information retrieval, transfer, and management.

This framework:

a) defines the basic concept of integrity;

b) identifies possible classes of integrity mechanisms;

c) defines facilities for each class of integrity mechanisms;

d) identifies management required to support the classes of integrity mechanism;

e) addresses the interaction of the integrity mechanism and the supporting services with other security services and mechanisms.

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

The integrity addressed by this framework is that defined by the constancy of a data value, not that of the constancy of the information that the data is deemed to represent. Other forms of invariance are excluded.

6.7 Part 7 – Security audit and alarms

This framework:

a) defines the basic concepts of security audit and alarms;

b) provides a general model for security audit and alarms;

c) identifies the relationship of the security audit and alarms service with the other security services.

As with other security services, a security audit can only be provided within the context of a defined security policy. The security policy will be defined by security authorities within their security domain. Any standard(s) specifying mechanisms based upon this framework should be able to support various security policies.

6.8 Key management

The key management framework, part 1 of ISO/IEC 11770, has a special relationship to the other security frameworks in that it is concerned with functions that are not directly related to the security services identified in CCITT Rec. X.800 | ISO 7498-2. Those functions are applicable in any information technology environment where encipherment or digital signature is appropriate.

This framework:

a) identifies objectives of key management;

b) describes general models on which key management mechanisms are based;

c) defines the basic concepts of key management common to all the parts of this multi-part standard;

d) defines key management services;

e) identifies the characteristics of key management mechanisms;

f) specifies requirements for the management of keying material during its life cycle;

g) describes a framework for the management of keying material during its life cycle.

7 Common concepts

Many concepts are required in more than one part of the security frameworks. This standard defines these concepts for use within the remaining parts of this Recommendation | International Standard.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.1 Security information

Security Information (SI) is information needed to implement security services. Examples of security information include:

- security policy rules;
- information to realize specific security services, such as Authentication Information (AI) and Access Control Information (ACI); and
- information relevant to security mechanisms, such as security labels, cryptographic checkvalues, security certificates and security tokens.

The types of SI common to more than one of the security frameworks are discussed in clause 8.

7.2 Security domain

A security domain is a set of elements under a given security policy administered by a single security authority for some specific security-relevant activities. The activities of a security domain involve one or more elements from that security domain and, possibly, elements of other security domains.

Examples of activities are:

- accesses to elements;
- establishment or use of OSI (N)-layer connections;
- operations relating to a specific management function;
- non-repudiation operations involving a notary.

An activity may be security-relevant even if it is currently not the subject of mechanisms that could enforce an arbitrary policy regarding its use. In particular, activities that cannot be prevented from taking place among any group of elements can be security-relevant and may become the subject of controlling mechanisms in the future.

Examples of the elements of a security domain in an Open Systems environment include logical or physical elements such as real open systems, application processes, (N)-entities, (N)-protocol data units, relays, and human users of real open systems. There are occasions when the human users must be distinguished from the other elements in a security domain. In such cases, to distinguish the non-human elements, the term *data objects* will be used.

7.2.1 Security policy and security policy rules

A security policy expresses security requirements for a security domain in general terms. For example, a security policy may identify requirements that apply to all members of a security domain when operating under specific conditions, or that apply to all information in a security domain. The implementation of a security policy will result in security services being identified that will satisfy the security policy, and security mechanisms will be chosen to implement the security services. The decision as to which security mechanisms are chosen is influenced by the threats that are anticipated and by the value of the resources to be protected.

Security policies are commonly stated as broad principles in a natural language. These principles reflect the security requirements of a particular organization or the members of a security domain. Before these requirements can be reflected in real open systems, the security policy must be refined so that a set of security policy rules can be derived from them. The interpretation of these requirements as security policy rules is an engineering activity. A security policy constrains the activities of elements subject to that security policy, either by requiring certain actions or by prohibiting certain activities. A security policy may also give elements permission to take part in certain activities. This is a broader interpretation of security policy than that contained in CCITT Rec. X.800 | ISO 7498-2, which is concerned only with OSI. Aspects of security policy which are specific to a particular security service are discussed in the security framework for that service.

Security policy rules for a security domain are of two types, those for activities within a security domain and those for activities between security domains. Security policy rules of the latter type are referred to as secure interaction rules. A security policy may also define which rules apply to relations with all security domains, and which rules apply to relations with particular security domains.

The security policy rules for a security domain must be kept valid as the system changes or the activities and security policy of the security domain are modified.

NOTE – This framework is not concerned with the following aspects of security policy:

- the party who establishes or maintains a security policy itself;
- procedures for establishing or maintaining a security policy;

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

- the contents of a security policy;
- procedures for binding a security policy to a security domain.

7.2.2 Security domain authority

A security domain authority is a security authority that is responsible for the implementation of a security policy for a security domain.

A security domain authority:

- may be a composite entity; such an entity must be identifiable;
- may, depending on any security policy that the security domain authority may be subject to, delegate the responsibility for implementing the security policy to one or more entities;
- has authority over the elements in the security domain.

NOTE – A security policy may be null if the security domain authority has decided not to impose any constraints.

Two security domain authorities are said to be linked if they are constrained to coordinate their security policies.

7.2.3 Inter-relationships among security domains

The notion of a security domain is deemed to be important for two reasons. Namely:

- it can be used to describe how security is managed and administered; and
- it can be used as a building block in modeling security-relevant activities that involve elements under distinct security authorities.

Security domains may be related in one or more ways. Some possible security domain relationships are discussed here. Relationships among security domains must be reflected in the security policies of the security domains as agreed by their security authorities. These relationships are stated in terms of elements and activities of the security domains and are reflected in the secure interaction rules for each of the related security domains. Some particular security domain relationships are described in the remainder of this subclause. Many other security domain relationships are possible.

a) Two security domains are said to be *isolated* from each other if they have no data objects in common and no activities in common and, therefore, cannot interact.

b) Two security domains are said to be *independent* of each other if:

- they have no data objects in common; and
- the activities within each security domain are constrained only by their own security policies (and corresponding sets of security policy rules); and
- the security authorities of the security domains are not constrained to coordinate their security policies.

Two or more independent security domains may choose to enter into an agreement to coordinate sharing of information among them (see 7.2.4).

c) Security domain A is said to be a *security subdomain* of another security domain B if, and only if:

- the set of elements of A is a subset of, or is the same as, the set of elements of B;
- the set of activities in A is a subset of, or is the same as, the set of activities in B;
- jurisdiction for A is delegated from the security authority of B to the security authority of A; and
- the security policy of A does not conflict with the security policy of B. A may introduce additional security policy if required, and if permitted by the security policy of B.

NOTE 1 – A subset may be equal to the full set. A security subdomain may be formed on one extreme of the full set of elements of the security superdomain for some classes of activity or on another extreme of all the classes of activity for some subset from the set of elements of the security superdomain. Between these two extremes many variations may exist.

d) security domain A is said to be a *security superdomain* of another security domain B if and only if B is a security subdomain of A.

NOTE 2 – The Security Frameworks do not require the isolated, independent, subdomain or superdomain concepts to be supported by any particular protocol, specification or implementation.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.2.4 Establishment of secure interaction rules

To be able to exchange information among security domains, there must be an agreed set of security policy rules for this exchange. These security policy rules are called secure interaction rules. They are part of each security domain's security policy rules. Secure interaction rules enable common security services and mechanisms to be selected, possibly through negotiation, and security information items in each security domain to be related to one another, possibly through mapping. Security management information needed to support secure interaction rules may be exchanged among security domains. Depending on the relationships among security domains, the secure interaction rules may be determined in different ways.

For secure interactions among independent security domains, the secure interaction rules must be agreed by the security authorities for the security domains involved.

For secure interactions among security subdomains, the secure interaction rules can be established by the security authority for the security superdomain. If allowed by the security superdomain's security policy, the security subdomains may establish their own secure interaction rules.

7.2.5 Inter-domain security information transfer

Secure interaction rules may themselves constitute security information, and this security information may need to be transferred between security domains. The following cases are considered:

- The semantics and the representation of the security information in each of the security domains is identical. This means that translation is unnecessary.
- The semantics of the security information in each of the security domains is identical, but the representations differ. This means that the method by which the security information is described is different, and thus that syntax translation is necessary.
- Both the semantics and the representation of the security information are different in each of the security domains. This means that the secure interaction rules must specify how security information of one domain is to be translated into security information of the other domain. Syntax translation may also be necessary.

7.3 Security policy considerations for specific security services

Access control mechanisms may be used in some implementations of an integrity service or a confidentiality service. In such cases, the security policy rules concerned with the implementation of an integrity service or a confidentiality service must describe how the access control mechanisms will be used. Access control mechanisms are described in terms of initiators and targets (in ITU-T Rec. X.812 | ISO/IEC 10181-3). The security policy rules define how the entities, information and data items in the integrity and confidentiality policies are related to initiators and targets in the access control mechanisms.

Confidentiality policies are stated in terms of which entities may examine information items. There are two ways in which an action performed by an initiator on a target can reveal information to an entity. Firstly, the result of the action may provide the initiator with some information about the target. Secondly, the action request may provide the target with some information about the initiator. When access control mechanisms are used to provide a confidentiality service, entities which attempt to obtain information are considered to be initiators, and information items are considered to be targets.

Integrity policies are stated in terms of which entities may modify data items. There are two ways in which an action performed by an initiator on a target may cause the modification of data. Firstly, the action may directly cause data contained within the target to be modified. Secondly, the result of the action may cause the modification of data contained within the initiator. When access control mechanisms are used to provide an integrity service, entities which attempt to modify data are considered to be initiators, and data items are considered to be targets.

7.4 Trusted entities

An entity is said to be a *trusted entity* for some classes of activity, in the context of a security policy, if the entity can violate the security policy, either by performing actions which it is not supposed to do, or by failing to perform actions which it is supposed to do. The security policy defines which entities are trusted, and for each trusted entity defines the set of activities for which the entity is trusted. An entity which is trusted for a particular set of activities is not necessarily trusted for all activities within a security domain.

A declaration in a security policy that an entity should behave in a particular way does not necessarily guarantee that the entity will behave in that way. Accordingly, a security policy may require that there be a means to detect violations of

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

the security policy caused by the misbehaviour of a trusted entity. A trusted entity that can misbehave without detection is known as an *unconditionally trusted entity*. A trusted entity that can violate the security policy, but cannot do so without being detected, is known as a *conditionally trusted entity*.

A trusted entity may be unconditionally trusted for a subset of its activities while also being conditionally trusted for a different subset of its activities. Such an entity can undetectably violate the security policy in some respects, but cannot undetectably violate the security policy in other respects.

A security domain's security policy may declare that an element which is not in the security domain is trusted for some set of activities within the security domain. Secure interaction rules (as discussed in 7.2.4) may define how entities within the security domain should interact with a trusted entity outside the security domain.

7.5 Trust

An entity X is said to *trust* an entity Y (for a set of activities) if and only if X relies upon Y behaving in a particular way with respect to the activities.

Trust is not necessarily mutual. An entity which is not a trusted entity may make use of services provided by a trusted entity. An example of a situation in which trust is mutual is when two trusted entities cooperate in performing an activity, and each of the two entities relies upon the other to assist it in enforcing the security policy.

Trust is not necessarily transitive. A security policy may define the transitivity of the trust relationship in specific instances. If entity A relies upon services provided by trusted entity B, and trusted entity B relies upon services provided by trusted entity C, then A may be indirectly relying upon C behaving in a particular way. In instances where this is the case, trust is transitive. However, in other circumstances B might take steps to ensure that misbehaviour by C cannot affect A's activities. In this case, trust is not transitive.

7.6 Trusted third parties

A trusted third party is a security authority or its agent that is trusted (in the context of a security policy) with respect to some security-relevant activities.

Examples of trusted third parties include:

- a trusted third party in authentication;
- a notary or a time stamping service in non-repudiation;
- a key distribution centre in key management.

8 Generic security information

Some types of security information are required in more than one of the security frameworks. This clause describes these types of security information.

The security mechanisms described in the security frameworks normally involve the exchange of security information either between entities which require security services for an interaction or between a security authority and the interacting entities. Four common forms of security information are used by the mechanisms described in these frameworks:

- security labels used to indicate the security policy applicable to an element, a communication channel or a data item;
- cryptographic checkvalues used to detect modifications of a data item;
- security certificates used to protect security information obtained from a security authority or TTP for use by one or more interacting parties;
- security tokens used to protect security information that is passed between interacting parties.

NOTE – Security information can be protected by several different security mechanisms. Some security mechanisms are based on the use of cryptography, while others use physical means.

8.1 Security labels

A security label is a set of security attributes that is bound to an element, communication channel or data item. A security label also indicates, either explicitly or implicitly, the security authority responsible for creating the binding and the security policy applicable to the use of the label. A security label can be used to support a combination of security services.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Examples of uses of security labels include:

- to support a security label-based access control scheme including the application of access control to provide integrity and/or confidentiality;
- to indicate the degree of confidence that can be placed in the data, and its handling requirements;
- to indicate the sensitivity of the data and its handling requirements;
- to indicate protection, disposal and other handling requirements.

8.2 Cryptographic checkvalues

A cryptographic checkvalue is information that is derived by performing a cryptographic transformation on a data unit. Seals, digital signatures and digital fingerprints are three examples of cryptographic checkvalues.

A seal is a form of cryptographic checkvalue computed using a symmetric cryptographic algorithm and a secret key shared by the communicating entities. Seals are used to detect modification of data during transfer.

A digital signature is a cryptographic checkvalue that protects against forgery by the recipient, and is computed using a private key and an asymmetric cryptographic algorithm. Validation of the digital signature requires the same cryptographic algorithm and the corresponding public key.

NOTE 1 – Although there are other means of preventing the recipient from forging a cryptographic checkvalue (e.g. using tamper resistant cryptographic modules), the Security Frameworks use the term digital signature to mean a cryptographic checkvalue produced using an asymmetric cryptographic algorithm.

NOTE 2 – With some asymmetric cryptographic algorithms, the computation of a digital signature requires the use of more than one private key. When such algorithms are used, possession of each of the private keys may be restricted to different entities. This ensures that the entities must cooperate to generate a digital signature.

A digital fingerprint is a characteristic of a data item that is sufficiently peculiar to the data item that it is computationally infeasible to find another data item with the same digital fingerprint. Some forms of cryptographic checkvalue (e.g. the result of applying a one-way function to the data) can be used to provide a digital fingerprint. Digital fingerprints can be provided by means other than cryptographic algorithms. For example, a copy of a data item is a digital fingerprint.

NOTE 3 – One-way functions are not equivalent to digital fingerprints. Some one-way functions are not suitable for creating digital fingerprints, and some digital fingerprints are not created using one-way functions.

NOTE 4 – The calculation of a digital signature using an asymmetric algorithm can take a long time because asymmetric algorithms are, in general, computationally intensive. A digital signature may be computed from a digital fingerprint of the data rather than from the data itself. This can result in improved performance, as it can be faster to compute a digital signature of a short digital fingerprint than it is to compute a digital signature of a long message.

A cryptographic checkvalue does not necessarily protect against the replay of a single data unit. Replay protection can be achieved by including in the data some information which can be used to detect replays, such as a sequence number or time stamp, or by using cryptographic chaining. To provide protection against replay, this information must be checked by the recipient of the protected data unit.

8.3 Security certificates

8.3.1 Introduction to security certificates

A security certificate is a set of security-relevant data issued by a security authority or a trusted third party, together with security information which is used to provide the integrity and data origin authentication services for the data. A security certificate contains an indication of the time-periods in which the data is valid.

Security certificates are used to convey security information from a security authority (or a trusted third party) to entities which require this information to perform security functions. A security certificate may contain security information for more than one security service.

As described in the other security frameworks, a security certificate may contain SI used for:

- access control purposes;
- authentication purposes;
- integrity purposes;
- confidentiality purposes;
- non-repudiation purposes;
- audit purposes;
- key management purposes.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.3.2 Verification and chaining of security certificates

The verification of a security certificate consists of validating its integrity, verifying the claimed identity of the security certificate issuer, and checking that the issuer is authorized to create the security certificate. These operations may require further SI to be present.

If the verifier of a security certificate does not have the SI needed to verify a security certificate, a security certificate from another security authority may be used to provide the necessary SI. This process can be repeated to provide a chain of security certificates. These carry SI which provides a secure path from a known security authority (i.e. one for which SI has already been established) to the entity requiring certified SI.

A chain of security certificates should only be used when it complies with the restrictions imposed by all relevant security policies. The existence of a chain is not sufficient. A chain should be used only if such use is permitted by the trust relationships between the verifier of the chain and the security authorities which created the certificates in the chain, and is also permitted by the trust relationships amongst those security authorities. These relationships are defined by the security policy of the verifier of the certificate chain and the security policies of the security authorities. In particular, some security authorities are trusted to issue security certificates for some other security authorities, while some others are trusted only to issue security certificates for the entities they administer.

8.3.3 Revocation of security certificates

The SI contained within a security certificate may cease to be valid. For example, if a private key is compromised, then the corresponding public key should no longer be used, and hence security certificates which contain this public key should be revoked.

The mechanisms which can be used to revoke security certificates include revocation certificates and revocation list certificates. A *revocation certificate* is a security certificate that indicates that a particular certificate has been revoked. A *revocation list certificate* is a security certificate that identifies a list of security certificates which have been revoked.

8.3.4 Re-use of security certificates

Some security certificates are intended to be used in support of more than one instance of communication, while others are intended to be used only once. An example of a security certificate which is intended to be used more that once is the authentication certificate defined in ITU-T X.509 | ISO/IEC 9594-8. An example of a security certificate which is intended to be used once only is an access control certificate which authorizes a single access. Security certificates which are intended to be used only once may contain information to prevent their re-use (e.g. a unique number).

8.3.5 Security certificate structure

The general form of a security certificate has three components:

- information required in all security certificates;
- security information specific to one or more security services;
- information to control or limit the use of the security information.

The information required in all security certificates falls into two categories:

a) Information which provides both integrity and data origin authentication (e.g. a cryptographic checkvalue and indications of the information to be used to verify it). Since the data origin authentication service is provided, an indication of the identity of the claimed source of the security certificate (i.e. the issuing authority) must also be provided.

b) Information from which a period of validity can be identified (e.g. an explicit validity period), or derived (e.g. a creation time and an implicit validity period). This prevents the indefinite re-use of the security certificate, although the security certificate may be re-used many times within the validity period.

The information used to control or limit the use of the security information falls into three categories:

a) *Information used to protect the security certificate from unauthorized use*

Examples are:

- information (e.g. a distinguishing identifier) that identifies the entity or entities whose SI is included in the security certificate;
- information that identifies the entities that are permitted to make use of the SI contained within the security certificate;
- information that controls the number of times that the certificate may be used;

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

- information that identifies the security policy under which the security certificate must be used;
- protection methods and associated parameters to protect the security certificate from theft (see Annex A for examples);
- information used for replay protection (e.g. a unique number or a challenge).

b) *Information that can be used to aid a security audit*

Examples include:

- a security certificate reference identifier (e.g. a serial number) which is unique to the security certificate with respect to all security certificates issued by the same security authority or agent;
- the identity (for audit purposes) of the entity for which the security certificate was originally issued.

c) *Information that can be used to aid security recovery*

Examples include:

- a security certificate reference identifier which can be used to revoke a specific security certificate;
- a security certificate group identifier which can be used to revoke a group of security certificates.

8.4 Security tokens

A security token is a set of data protected by one or more security services, together with security information that is used in the provision of those security services, that is transferred between communicating entities. Security tokens may be classified according to who creates them and which security services are used to protect their contents.

A security token which is issued by a security authority and protected by the integrity and data origin authentication services is known as a security certificate (see 8.3).

Many security mechanisms require an integrity-protected exchange of security information between two communicating entities, neither of which is a security authority. The security tokens used to achieve these integrity-protected exchanges are not security certificates, because the entities which generate them are not security authorities. Such security tokens are known as *integrity-protected security tokens.*

All integrity-protected security tokens contain the following information:

- information which provides both integrity and data origin authentication (e.g. a cryptographic checkvalue and an indication of the information to be used to verify it).

An integrity-protected security token may contain one or more of the following additional items of information:

- information from which a period of validity can be identified;
- information used for replay protection (e.g. a unique number).

9 Generic security facilities

Many facilities are required in more than one of the security frameworks. This clause defines these facilities for use within the other security frameworks.

9.1 Management related facilities

This subclause identifies generic types of management facility. Sub-classes of these management facilities may exist, which may be specific to a particular security mechanism.

9.1.1 Install SI

This facility establishes an initial set of SI bound to an element.

9.1.2 Deinstall SI

This facility causes an entity to be removed from a security domain, by revoking the SI which declares the entity to be a member of the security domain.

9.1.3 Change SI

This facility is invoked to modify the SI associated with an element.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.1.4 Validate SI

This facility binds a set of SI to an element. The *validate SI* facility is invoked by a security authority or its agent.

9.1.5 Invalidate SI

This facility disables any use of SI associated with an element. The *invalidate SI* facility is invoked by a security authority or its agent. SI which has been disabled with the *invalidate SI* facility may remain stored within the system for the purposes of audit and to ensure that the SI remains disabled.

9.1.6 Disable/Re-enable security service

These facilities disable and re-enable identified aspects of a security service.

9.1.7 Enrol

This facility causes a security authority to record some security information associated with an entity. The enrol facility may be invoked by an entity other than a security authority. For example, an entity wishing to join a security domain can use the enrol facility to notify a security authority that it wishes to join the security domain.

9.1.8 Un-enrol

This facility causes an element to be removed from a security domain and its associated SI to be revoked. This facility is invoked by a security authority or its agent. A security policy may require that some types of SI are never destroyed.

9.1.9 Distribute SI

This facility is used by a security authority or its agent to make items of SI available to other entities.

9.1.10 List SI

This facility lists the SI that is bound to a given element.

9.2 Operational related facilities

9.2.1 Identify trusted security authorities

This facility identifies those security authorities that are trusted in the context of a security policy for specific elements and for given security activities (e.g. to provide encipherment keys, to provide access control security certificates, or to provide authentication security certificates).

9.2.2 Identify secure interaction rules

This facility identifies secure interaction rules to be used. This may be accomplished through pre-established information or through negotiation between elements of domains related to each other as described in 7.2.4.

NOTE – Secure interactions rules are established by agreement between security domains, not by the use of this facility. This facility identifies which of the already established secure interaction rules are applicable to a particular activity.

9.2.3 Acquire SI

This facility acquires SI prior to an activity.

Examples of sub-classes of this facility are:

- Access control: Get initiator ACI, Get target ACI;
- Authentication: Acquire.

9.2.4 Generate SI

This facility generates SI for a specific security related activity. The SI may be bound to data.

Examples of sub-classes of this facility are:

- Access control: Bind action ACI;
- Authentication: Generate;
- Non-repudiation: Generate Evidence.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

9.2.5 Verify SI

This facility verifies the validity of SI produced by an invocation of the *generate SI* facility. The *verify SI* facility may itself produce SI to be passed back to another invocation of the *verify SI* facility.

Examples of sub-classes of this facility are:

- Access control: Verify action ACI;
- Authentication : Verify;
- Non-repudiation: Validate Evidence.

An example of a situation in which the output of the *verify SI* facility is passed back for further verification is a two-way protocol for mutual authentication. Suppose entities A and B wish to authenticate each other, and A initiates the protocol exchange. A invokes the *generate* facility to create authentication information which contains both a proof of A's identity and a challenge to which B is expected to respond. B invokes the *verify* facility to check that the challenge came from A, and also creates a new item of authentication information containing a proof of B's identity and a reply to A's challenge. A then invokes the *verify* facility to process B's response. The *verify* facility checks that the response came from B and that it matches the original challenge.

10 Interactions between security mechanisms

It is often the case that several different security services are required for a single instance of communication. This requirement may be satisfied either by using a single security mechanism which provides multiple security services, or by using several different security mechanisms simultaneously.

When different security mechanisms are used simultaneously, it is sometimes the case that the mechanisms interact in adverse manner which can be exploited by an attacker. That is, mechanisms which provide an acceptable level of security, when used in isolation may become more vulnerable when they are used in combination with other mechanisms. It is often the case that two security mechanisms can be combined in several different ways; the vulnerabilities of the combined mechanisms may differ according to the manner in which they were combined.

A particularly important case of an interaction between mechanisms occurs when two cryptographic mechanisms are combined (e.g. an integrity mechanism with a confidentiality mechanism; or a non-repudiation mechanism with a confidentiality mechanism). The security properties of the combined mechanisms depend on the order in which the two cryptographic transformations are applied.

In general, when asymmetric cryptographic algorithms are used, an integrity or non-repudiation transformation should be applied to plaintext, and the resulting signed or sealed data should then be enciphered.

An example of a case where it is necessary to apply the two services in the reverse order (i.e. confidentiality first), is when the services apply between different entities, and an entity needs to be able to verify the integrity of the ciphertext without being permitted to know the plaintext. This situation can occur in message handling systems, where a message transfer agent may need to verify the integrity and origin of the message without being permitted to know what the plaintext of the message is.

Use of confidentiality and integrity services in this reverse order carries a risk that the integrity service will not be able to support non-repudiation. If all three services are desired, and the reverse order of integrity and confidentiality is necessary, then it is possible to apply two integrity mechanisms, one before the confidentiality mechanism and one after. An example of this situation occurs in message handling systems; if confidentiality is provided, then two different digital signatures can be placed on the message (one computed on the ciphertext for the consumption of the message transfer agent, and one computed on the plaintext to provide the recipient with non-repudiation of origin).

11 Denial of service and availability

Denial of service occurs whenever a service falls below the level required, including when the service becomes unavailable. Such a denial of service may be caused by an intentional attack or by accidental conditions such as a storm or earthquake. Availability is a condition in which there is no denial of service or degraded communications quality.

It is not always possible to prevent a denial of service condition. Security services can be used to detect the denial of a service so that corrective measures may be taken. Such detection may not be able to determine whether the condition was the result of an attack or an accidental condition. A particular security policy may require that when a denial of service condition is identified, it should be logged (for audit purposes) and an alarm sent to the alarm processor.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Once a denial of service condition has been identified, security services may also be used to correct it and return to an acceptable level of service. This identification and these corrective actions may involve the use of security services and non-security services (e.g. rerouting traffic over other links, switching to backup storage facilities, or bringing backup processors on line).

Many different types of service are subject to denial of service attacks, and the mechanisms used to prevent them may vary with each type of application being protected. This means that it is not possible to classify mechanisms protecting against denial of service in a general way and the individual security frameworks do not, therefore, address them further.

12 Other requirements

Security measures beyond those described in these frameworks may be needed (e.g. physical and personnel security measures). The definition of security services to support such measures is outside the scope of this Recommendation | International Standard. The use of such additional security measures may even obviate the need for some of the security services described in these frameworks.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A

Some examples of protection mechanisms for security certificates

(This annex does not form an integral part of this Recommendation | International Standard)

A potential threat involving security certificates is the threat that an attacker will falsely claim to be the entity to which the security certificate refers. Such an unauthorized use of a security certificate is referred to as theft of the security certificate.

This threat can be both an outsider and an insider threat. The outsider threat is that an attacker might obtain a security certificate by eavesdropping upon communications in which it is not otherwise involved. The insider threat is that an entity which has a legitimate need to obtain a certificate (e.g. in order to establish the SI of an entity with which it is communicating) might falsely claim to be the entity referred to in the certificate.

A security certificate may be protected against theft by using OSI communications security services directly or by using an alternative protection method requiring additional parameters, internal and external to the security certificate.

A protection mechanism for security certificates is said to support delegation if an entity which has the right to use the security certificate may transfer this right to another entity. Some of the mechanisms described in this annex support delegation.

A.1 Protection using an OSI communications security service

The threat of theft by an outsider may be countered by using a confidentiality service when the security certificate is transferred between communicating entities.

A.2 Protection using a parameter within the security certificate

There are a number of alternative methods to protect security certificates from theft. Each of these methods relies upon internal parameters within the certificate and associated external parameters. The particular methods used may be indicated within the security certificate.

These methods include:

- the authentication method;
- the secret key method;
- the public key method;
- the one-way function method.

A security certificate may use a combination of several of these methods.

A.2.1 The authentication method

In this method, the internal parameter is the distinguishing identifiers of the entities which are permitted to use the certificate. The external parameter is the distinguishing identifier of the entity which is attempting to use the certificate. This external parameter is provided by an authentication service. Optionally, the certificate may include additional internal parameters such as the serial number of the authentication certificate which is to be used in the authentication process.

The authentication method provides the following protection for the security certificate:

- It restricts the use of the security certificate to the entities whose identifiers are included in the security certificate.

This method does not permit an authorized user of the certificate to pass on this right to another entity, as the entities that may use the certificate are fixed at the time that the certificate is created. That is, this method does not support delegation.

A.2.2 The secret key method

In this method, the entire certificate is enciphered using a symmetric cryptographic algorithm. The external parameter in this method is the secret key that was used to encipher the certificate.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The secret key method provides the following protection for the security certificate:

- It restricts the use of the security certificate to the entities who know the value of the secret key (and hence are able to decipher the enciphered certificate).

This method supports delegation, as an authorized user of the certificate may pass on this right to another entity by giving it either the secret key or the deciphered certificate.

A.2.3 The public key method

In this method, the internal parameter is a public key. The external parameter is the corresponding private key.

The public key method provides the following protection for the security certificate:

- It restricts the use of the security certificate to the entities who know the value of the private key (and hence are able to compute digital signatures using the private key).

This method supports delegation, as an authorized user of the certificate may pass on this right to another entity by giving it the private key.

A.2.4 The one-way function method

In this method, the internal parameter is the result of applying a one-way function to the external parameter. The internal parameter is known as a *protection key*, while the external parameter is known as a *control key*.

The one-way function method provides the following protection for the security certificate:

- It restricts the use of the security certificate to the entities who know the value of the control key (and hence are able to prove that they know the control key by revealing its value).

This method supports delegation, as an authorized user of the certificate may pass on this right to another entity by giving it the control key.

A.3 Protection of the internal and external parameters while in transit

There are four cases to be considered:

- Transfer of the internal parameter to the issuing authority before the certificate is created. This case is only required if the internal and external parameters are not generated by the issuing authority.
- Transfer of the external parameter from the issuing authority after the certificate is created. This case is only required if the internal and external parameters are generated by the issuing authority.
- Transfer of the external parameter between entities when the right to use the certificate is asserted.
- Transfer of the external parameter between entities when the right to use the certificate is delegated.

A.3.1 Transfer of internal parameters to the issuing security authority

In the authentication method, the public key method and the one-way function method, the internal parameter may be communicated to the security authority before being placed in the security certificate. The internal parameter must be integrity protected while it is being transferred to the security authority.

In the secret key method, the external parameter (i.e. the secret key) may be communicated to the security authority before the certificate is created. This transfer requires both integrity and confidentiality protection.

A.3.2 Transfer of external parameters among entities

In the authentication method, the external parameter (the certificate user's identity) is provided by an authentication mechanism.

In the secret key method and the one-way function method, the external parameter must be transferred between entities when the certificate is used. This limits the use of the security certificate to those who know the correct value of the secret key or the control key. The external parameter must be confidentiality protected when communicated between entities.

A difference between these two methods is that when using the secret key method, it is necessary to reveal the value of the external parameter before the cryptographic checkvalue of the security certificate can be verified, whereas in the one-way function method, the checkvalue of the security certificate may be verified before the external parameter is revealed.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

In the private key method, the external parameter does not need to be transferred between entities when the certificate is used, as an entity can prove that it knows the private key without revealing it (by creating a digital signature). With this method, the external parameter (the private key) only needs to be transferred when the right to use the certificate is delegated. The private key must be confidentiality protected when it is communicated between entities.

A.4 Use of security certificates by single entities or by groups of entities

The protection methods described above may be used to restrict the use of a security certificate either to a single named entity or to a named group of entities:

- A security certificate may be bound to a specific entity; the secret key, private key or control key is communicated to the single entity in an enciphered form, and the distinguishing identifier or security attributes of the entity appear in the security certificate.
- A security certificate may be bound to a named group of entities; the secret key, private key or control key is communicated to the members of the group in enciphered form, and the distinguishing identifier or security attributes of the group appear in the security certificate. In this way, any member of the group may use the security certificate.

A.5 Linking a security certificate with accesses

Security certificates can be used for access control. In this case, it is important to establish a secure link between a security certificate and the access requests which it supports. If there is no such secure link, then the security certificate is vulnerable to a replay attack in which an attacker transmits a copy of a genuine security certificate followed by a forged access request.

This attack can be prevented by using an integrity service to bind together the security certificate, the external parameter, and the access request.

When the authentication method is used, this binding can be achieved by linking the authentication exchange with an integrity mechanism. This is described in the Authentication Framework (see ITU-T Rec. X.811 | ISO/IEC 10181-2).

When the secret key method is used, this binding can be achieved by including a key for an integrity mechanism within the body of the security certificate, and using this key to seal the access request. Alternatively, the secret key (or a variant of it) may be used as the key for an integrity mechanism.

NOTE – The use of the same cryptographic key with both an integrity mechanism and a confidentiality mechanism may make some attacks possible. To protect against this threat, *key variants* may be used. A variant of a cryptographic key is another cryptographic key which is derived from, but not the same as, the original key.

When the one-way function method is used, this binding can be achieved by using the control key as the key in an integrity mechanism based on one-way functions.

When the public key method is used, this binding can be achieved by using the private key to sign access requests.

With all of these methods, the binding between the security certificate, the external parameter and the access request may also be achieved by using an integrity service which is provided as part of an OSI communications service.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B

Bibliography

(This annex does not form an integral part of this Recommendation | International Standard)

- 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.*
- ITU-T Recommendation X.509 (1993) | ISO/IEC 9594-8:1995, *Information technology – Open Systems Interconnection – The Directory: Authentication framework.*
- ISO/IEC 11770-1[1)], *Information technology – Security techniques – Key management – Part 1: Key management framework.*
- ISO/IEC 9798-1:1991, *Information technology – Security techniques – Entity authentication mechanisms – Part 1: General model.*

1) To be published.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

This page intentionally left blank

--`,,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

© ISO/IEC

ICS 35.100

Descriptors: data processing, information interchange, network interconnection, open systems interconnection, communication procedure, protection of information, security techniques, overviews.

Price based on 20 pages

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale