

Information technology — Open Systems Interconnection — The Directory: Authentication framework —

(ITU-T Rec. X.509 (1993) |
ISO/IEC 9594-8:1995)

ICS 35.100.70

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

National foreword

This British Standard reproduces verbatim ISO/IEC 9594-8:1995 and implements it as the UK national standard. BS ISO/IEC 9594-8:1990 remains current because it applies to existing products that are still being manufactured and which are not covered in this standard. It is envisaged that BS ISO/IEC 9594-8:1990 will be withdrawn in due course.

Customer Services will respond to orders for BS ISO/IEC 9594-8 by supplying the latest edition. If copies of BS ISO/IEC 9594-8:1990 are required, orders should state clearly that BS ISO/IEC 9594-8:1990 is required.

The UK participation in its preparation was entrusted to Technical Committee IST/21, Open Systems Interconnection, Data Management and Open Distribution Processing, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee is available on request.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not puport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations

Summary of pages

This document comprised a front cover, an inside front cover, pages i and ii, the ISO/IEC title page, pages ii to iv, pages 1 to 30, an inside back cover and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Board and comes into effect on 15 February 1997

© BSI 11-1998

ISBN 0 580 26572 2

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
National foreword	Inside front cover
Foreword	iv
Text of ISO 9594-8	1

INTERNATIONAL
STANDARD

ISO/IEC
9594-8

Second edition
1995-09-15

**Information technology — Open Systems
Interconnection — The Directory:
Authentication framework**

*Technologies de l'information — Interconnexion de systèmes ouverts
(OSI) — L'Annuaire: Cadre général d'authentification*



Reference number
ISO/IEC 9594-8:1995(E)

Contents

	Page
Foreword	iv
Introduction	1
Section 1. General	1
1 Scope	2
2 Normative references	3
2.1 Identical Recommendations International Standards	3
2.2 Paired Recommendations International Standards equivalent in technical content	3
3 Definitions	4
3.1 OSI Reference Model security architecture definitions	4
3.2 Directory model definitions	4
3.3 Authentication framework definitions	4
4 Abbreviations	6
5 Conventions	6
Section 2. Simple authentication	7
6 Simple authentication procedure	7
6.1 Generation of protected identifying information	7
6.2 Procedure for protected simple authentication	8
6.3 User Password attribute type	9
Section 3. Strong authentication	10
7 Basis of strong authentication	10
8 Obtaining a user's public key	10
8.1 Optimization of the amount of information obtained from the Directory	12
8.2 Example	13
9 Digital signatures	14
10 Strong authentication procedures	16
10.1 Overview	16
10.2 One-way authentication	17
10.3 Two-way authentication	17
10.4 Three-way authentication	18
11 Management of keys and certificates	19
11.1 Generation of key pairs	19
11.2 Management of certificates	19
Annex A Authentication Framework in ASN.1	21
Annex B Security requirements	23
Annex C An introduction to public key cryptography	25
Annex D The RSA Public Key Cryptosystem	27
Annex E Hash functions	29
Annex F Threats protected against by the strong authentication method	29
Annex G Data confidentiality	29
Annex H Reference definition of algorithm object identifiers	30
Annex J Amendments and corrigenda	Inside back cover
Figure 1 — The unprotected simple authentication procedure	7
Figure 2 — Protected simple authentication	8
Figure 3 — The protected simple authentication procedure	8
Figure 4 — CA hierarchy — A hypothetical example	13
Figure 5 — Non-hierarchical certification path — An example	14

	Page
Figure 6 — Digital signatures	15
Figure 7 — One-way authentication	17
Figure 8 — Two-way authentication	18
Figure 9 — Three-way authentication	18
Figure C.1 — Use of a PKCS to exchange secret information	26
Table 1 — Notation	6
Table B.1 — Threats and protection	25

Descriptors: Data processing, information interchange, network interconnection, open systems interconnection, application layer, directories, authentication.

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 9594-8 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.509.

Implementors should note that a defect resolution process exists and that corrections may be applied to this part of ISO/IEC 9594 in the form of technical corrigenda. A list of approved technical corrigenda for this part of ISO/IEC 9594 can be obtained from the subcommittee secretariat. Published technical corrigenda are available from your national standards organization.

This second edition technically revises and enhances ISO/IEC 9594-8:1990. It also incorporates technical corrigendum 1:1991. Implementations may still claim conformance to the first edition of this part of ISO/IEC 9594. However, at some point, the first edition will no longer be supported (i.e. reported defects will no longer be resolved). It is recommended that implementations conform to this second edition as soon as possible.

ISO/IEC 9594 consists of the following parts, under the general title *Information technology — Open Systems Interconnection — The Directory*:

- *Part 1: Overview of concepts, models and services;*
- *Part 2: Models;*
- *Part 3: Abstract service definition;*
- *Part 4: Procedures for distributed operation;*
- *Part 5: Protocol specifications;*
- *Part 6: Selected attribute types;*
- *Part 7: Selected object classes;*
- *Part 8: Authentication framework;*
- *Part 9: Replication.*

Annex A forms an integral part of this part of ISO/IEC 9594. Annexes B to J are for information only.

Section 1. General

Introduction

This Recommendation | International Standard, together with other Recommendations | International Standards, has been produced to facilitate the interconnection of information processing systems to provide directory services. A set of such systems, together with the directory information which they hold, can be viewed as an integrated whole, called the *Directory*. The information held by the Directory, collectively known as the Directory Information Base (DIB), is typically used to facilitate communication between, with or about objects such as application-entities, people, terminals and distribution lists.

The Directory plays a significant role in Open Systems Interconnection, whose aim is to allow, with a minimum of technical agreement outside of the interconnection standards themselves, the interconnection of information processing systems:

- from different manufacturers;
- under different managements;
- of different levels of complexity; and
- of different ages.

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 briefly described in Annex B. Virtually all security services are dependent upon the identities of the communicating parties being reliably known, i.e. authentication.

This Recommendation | International Standard defines a framework for the provision of authentication services by the Directory to its users. These users include the Directory itself, as well as other applications and services. The Directory can usefully be involved in meeting their needs for authentication and other security services because it is a natural place from which communicating parties can obtain authentication information of each other — knowledge which is the basis of authentication. The Directory is a natural place because it holds other information which is required for communication and obtained prior to communication taking place. Obtaining the authentication information of a potential communication partner from the Directory is, with this approach, similar to obtaining an address. Owing to the wide reach of the Directory for communications purposes, it is expected that this authentication framework will be widely used by a range of applications.

This second edition technically revises and enhances, but does not replace, the first edition of this Recommendation | International Standard. Implementations may still claim conformance to the first edition.

This second edition specifies version 1 of the Directory service and protocols. The first edition also specifies version 1. Differences between the services and between the protocols defined in the two editions are accommodated using the rules of extensibility defined in this edition of X.519 | ISO/IEC 9594-5.

Annex A, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module which contains all of the definitions associated with the authentication framework.

Annex B, which is not an integral part of this Recommendation | International Standard, describes security requirements.

Annex C, which is not an integral part of this Recommendation | International Standard, is an introduction to public key cryptography.

Annex D, which is not an integral part of this Recommendation | International Standard, describes the RSA Public Key Cryptosystem.

Annex E, which is not an integral part of this Recommendation | International Standard, describes hash functions.

Annex F, which is not an integral part of this Recommendation | International Standard, describes threats protected against by the strong authentication method.

Annex G, which is not an integral part of this Recommendation | International Standard, describes data confidentiality.

Annex H, which is an integral part of this Recommendation | International Standard, defines object identifiers assigned to authentication and encryption algorithms, in the absence of a formal register.

Annex J, which is not an integral part of this Recommendation | International Standard, lists the amendments and defect reports that have been incorporated to form this edition of this Recommendation | International Standard.

1 Scope

This Recommendation | International Standard:

- specifies the form of authentication information held by the Directory;
- describes how authentication information may be obtained from the Directory;
- states the assumptions made about how authentication information is formed and placed in the Directory;
- defines three ways in which applications may use this authentication information to perform authentication and describes how other security services may be supported by authentication.

This Recommendation | International Standard describes two levels of authentication: simple authentication, using a password as a verification of claimed identity; and strong authentication, involving credentials formed using cryptographic techniques. While simple authentication offers some limited protection against unauthorized access, only strong authentication should be used as the basis for providing secure services. It is not intended to establish this as a general framework for authentication, but it can be of general use for applications which consider these techniques adequate.

Authentication (and other security services) can only be provided within the context of a defined security policy. It is a matter for users of an application to define their own security policy which may be constrained by the services provided by a standard.

It is a matter for standards defining applications which *use* the authentication framework to specify the protocol exchanges which need to be performed in order to achieve authentication based upon the authentication information obtained from the Directory. The protocol used by applications to obtain credentials from the Directory is the Directory Access Protocol (DAP), specified in ITU-T Recommendation X.519 | ISO/IEC 9594-5.

The strong authentication method specified in this Recommendation | International Standard is based upon public-key cryptosystems. It is a major advantage of such systems that user certificates may be held within the Directory as attributes, and may be freely communicated within the Directory System and obtained by users of the Directory in the same manner as other Directory information. The user certificates are assumed to be formed by “off-line” means, and placed in the Directory by their creator. The generation of user certificates is performed by some off-line Certification Authority which is completely separate from the DSAs in the Directory. In particular, no special requirements are placed upon Directory providers to store or communicate user certificates in a secure manner.

A brief introduction to public-key cryptography can be found in Annex C.

In general, the authentication framework is not dependent on the use of a particular cryptographic algorithm, provided it has the properties described in 7.1. Potentially a number of different algorithms may be used. However, two users wishing to authenticate shall support the same cryptographic algorithm for authentication to be performed correctly. Thus, within the context of a set of related applications, the choice of a single algorithm will serve to maximize the community of users able to authenticate and communicate securely. One example of a public key cryptographic algorithm can be found in Annex D.

Similarly, two users wishing to authenticate shall support the same hash function [see 3.3 f)] (used in forming credentials and authentication tokens). Again, in principle, a number of alternative hash functions could be used, at the cost of narrowing the communities of users able to authenticate. A brief introduction to hash functions can be found in Annex E.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard part. 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 editions 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.500 (1993) | ISO/IEC 9594-1:1995, *Information Technology — Open Systems Interconnection — The Directory: Overview of concepts, models and services*.
- ITU-T Recommendation X.501 (1993) | ISO/IEC 9594-2:1995, *Information Technology — Open Systems Interconnection — The Directory: Models*.
- ITU-T Recommendation X.511 (1993) | ISO/IEC 9594-3:1995, *Information Technology — Open Systems Interconnection — The Directory: Abstract service definition*.
- ITU-T Recommendation X.518 (1993) | ISO/IEC 9594-4:1995, *Information Technology — Open Systems Interconnection — The Directory: Procedures for distributed operation*.
- ITU-T Recommendation X.519 (1993) | ISO/IEC 9594-5:1995, *Information Technology — Open Systems Interconnection — The Directory: Protocol specifications*.
- ITU-T Recommendation X.520 (1993) | ISO/IEC 9594-6:1995, *Information Technology — Open Systems Interconnection — The Directory: Selected attribute types*.
- ITU-T Recommendation X.521 (1993) | ISO/IEC 9594-7:1995, *Information Technology — Open Systems Interconnection — The Directory: Selected object classes*.
- ITU-T Recommendation X.525 (1993) | ISO/IEC 9594-9:1995, *Information Technology — Open Systems Interconnection — The Directory: Replication*.
- ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1:1995, *Information Technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- ITU-T Recommendation X.681 (1994) | ISO/IEC 8824-2:1995, *Information Technology — Abstract Syntax Notation One (ASN.1): Information object specification*.
- ITU-T Recommendation X.682 (1994) | ISO/IEC 8824-3:1995, *Information Technology — Abstract Syntax Notation One (ASN.1): Constraint specification*.
- ITU-T Recommendation X.683 (1994) | ISO/IEC 8824-4:1995, *Information Technology — Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.
- ITU-T Recommendation X.690 (1994) | ISO/IEC 8825-1:1995, *Information Technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.
- ITU-T Recommendation X.880 (1994) | ISO/IEC 13712-1:1995, *Information technology — Remote Operations: Concepts, model and notation*.
- ITU-T Recommendation X.881 (1994) | ISO/IEC 13712-2:1995, *Information technology — Remote Operations: OSI realizations — Remote Operations Service Element (ROSE) service definition*.

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.800 (1991), *Security Architecture for Open Systems Interconnection for CCITT Applications*.
- ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*.

3 Definitions

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

3.1

OSI Reference Model security architecture definitions

the following terms are defined in CCITT Rec. X.800 | ISO 7498-2:

- a) *asymmetric (encipherment)*;
- b) *authentication exchange*;
- c) *authentication information*;
- d) *confidentiality*;
- e) *credentials*;
- f) *cryptography*;
- g) *data origin authentication*;
- h) *decipherment*;
- i) *encipherment*;
- j) *key*;
- k) *password*;
- l) *peer-entity authentication*;
- m) *symmetric (encipherment)*.

3.2

directory model definitions

the following terms are defined in ITU-T Rec. X.501 | ISO/IEC 9594-2:

- a) *attribute*;
- b) *Directory Information Base*;
- c) *Directory Information Tree*;
- d) *Directory System Agent*;
- e) *Directory User Agent*;
- f) *distinguished name*;
- g) *entry*;
- h) *object*;
- i) *root*.

3.3 Authentication framework definitions

The following terms are defined in this Recommendation | International Standard:

3.3.1

authentication token (token)

information conveyed during a strong authentication exchange, which can be used to authenticate its sender

3.3.2

user certificate; certificate

the public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it

3.3.3

certification authority

an authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys