

**Implementation of
ISO/IEC 9594-8:1990**

Information Technology — Open Systems Interconnection — The Directory —

Part 8: Authentication framework

UDC 681.3:621.39

Committees responsible for this British Standard

The preparation of this British Standard was entrusted by the Information Systems Technology Standards Policy Committee (IST/-) to Technical Committee IST/21, upon which the following bodies were represented:

- Association for Payment Clearing Services
- British Computer Society
- British Gas plc
- British Railways Board
- British Telecommunications plc
- Computing Services Association
- Department of Trade and Industry (Alvey — Advanced Network Systems Architecture)
- Department of Trade and Industry (Information Technology Division)
- Department of Trade and Industry (National Physical Laboratory)
- EEA (the Association of Electronics, Telecommunications and Business Equipment Industries)
- HM Treasury (Central Computer and Telecommunications Agency)
- Institute of Chartered Secretaries and Administrators
- Institution of Electrical Engineers
- Inter-universities Computing Committee
- Joint Network Team
- Ministry of Defence
- National Health Services
- United Kingdom Atomic Energy Authority
- University of London Computer Centre

This British Standard, having been prepared under the direction of the Information Systems Technology Standards Policy Committee, was published under the authority of the Standards Board and comes into effect on 29 March 1991

© BSI 04-2000

The following BSI references relate to the work on this standard:
Committee reference IST/21
Draft for comment 88/62308 DC

ISBN 0 580 19550 3

Amendments issued since publication

Amd. No.	Date	Comments
7151	July 1992	Indicated by a sideline in the margin

Contents

	Page
Committees responsible	Inside front cover
National foreword	ii
Foreword	iii
Text of ISO/IEC 9594-8	1

National foreword

This British Standard reproduces verbatim ISO/IEC 9594-8:1990, including Technical Corrigendum 1 and implements it as the UK national standard.

This British Standard is published under the direction of the Information Systems Technology Standards Policy Committee whose Technical Committee IST/21 has the responsibility to:

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

NOTE International and European Standards, as well as overseas standards, are available from BSI Sales Department, BSI, Linford Wood, Milton Keynes, MK14 6LE.

A British Standard does not purport 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 comprises a front cover, an inside front cover, pages i and ii, the ISO/IEC title page, pages ii to iv, pages 1 to 28 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.

INTERNATIONAL STANDARD

ISO/IEC 9594-8

First edition
1990-12-15

Information technology — Open Systems Interconnection — The Directory —

Part 8: Authentication framework

Technologies de l'information — Interconnexion de systèmes ouverts — L'annuaire —

Partie 8: Cadre général d'authentification



Reference number
ISO/IEC 9594-8 : 1990 (E)

Contents

	Page
Foreword	iii
Introduction	1
Section 1. General	
1 Scope	1
2 Normative references	2
3 Definitions	2
4 Notation and Abbreviations	4
Section 2. Simple authentication	
5 Simple Authentication Procedure	5
Section 3. Strong authentication	
6 Basis of Strong Authentication	7
7 Obtaining a User's Public Key	8
8 Digital Signatures	12
9 Strong Authentication Procedures	14
10 Management of Keys and Certificates	17
Annex A (informative) Security Requirements	20
Annex B (informative) An Introduction to Public Key Cryptography	22
Annex C (informative) The RSA Public Key Cryptosystem	23
Annex D (informative) Hash Functions	25
Annex E (informative) Threats Protected Against by the Strong Authentication Method	25
Annex F (informative) Data Confidentiality	26
Annex G (normative) Authentication Framework in ASN.1	26
Annex H (informative) Reference Definition of Algorithm Object Identifiers	28
Figure 1 — The Unprotected Simple Authentication Procedure	5
Figure 2 — Protected Simple Authentication	6
Figure 3 — The Protected Simple Authentication Procedure	6
Figure 4 — CA Hierarchy — A Hypothetical Example	10
Figure 5 — Non-hierarchical Certification Path — An Example	12
Figure 6 — Digital Signatures	12
Figure 7 — One-way Authentication	15
Figure 8 — Two-way Authentication	16
Figure 9 — Three-way Authentication	17
Figure B.1 — Use of a PKCS to Exchange Secret Information	22
Table 1 — Notation	4
Table A.1	22

Descriptors: Data processing, information interchange, network interconnection, open systems interconnection, 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*.

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.*

Annex G forms an integral part of this part of ISO/IEC 9594. Annex A, Annex B, Annex C, Annex D, Annex E, Annex F and Annex H are for information only.

Introduction

0.1 This part of ISO/IEC 9594, together with the other parts, has been produced to facilitate the interconnection of information processing systems to provide directory services. The set of all 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 OSI application-entities, people, terminals and distribution lists.

0.2 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.

0.3 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 A. Virtually all security services are dependent upon the identities of the communicating parties being reliably known, i.e. authentication.

0.4 This part of ISO/IEC 9594 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.

Section 1. General

1 Scope

1.1 This part of ISO/IEC 9594:

- 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.

1.2 This part of ISO/IEC 9594 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.

1.3 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.

1.4 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 ISO/IEC 9594-5.

1.5 The strong authentication method specified in this part of ISO/IEC 9594 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 B.

1.6 In general, the authentication framework is not dependent on the use of a particular cryptographic algorithm, provided it has the properties described in 6.1. 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 C.

1.7 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 together with one example hash function can be found in Annex D.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9594. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 9594 are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7498-2:1987, *Information Processing Systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*.

ISO/IEC 8824:1990, *Information Technology — Open Systems Interconnection — Specification of Abstract Syntax Notation One (ASN.1)*.

ISO/IEC 8825:1990, *Information Technology — Open Systems Interconnection — Specification of Basic Encoding rules for Abstract Syntax Notation One (ASN.1)*.

ISO/IEC 10021-3:1990, *Information Technology — Text Communication — Message Oriented Interchange System (MOTIS) — Part 3: Abstract Service Definition Conventions*.

3 Definitions

3.1 This part of ISO/IEC 9594 makes use of the following general security-related terms defined in 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 The following terms used in this part of ISO/IEC 9594 are defined in ISO/IEC 9594-2:

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

3.3 For the purpose of this part of ISO/IEC 9594 the following definitions apply:

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 secret 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

3.3.4

certification path

an ordered sequence of certificates of objects in the DIT which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path

3.3.5

cryptographic system, cryptosystem

a collection of transformations from plain text into ciphertext and vice versa, the particular transformation(s) to be used being selected by keys. The transformations are normally defined by a mathematical algorithm

3.3.6

hash function

a (mathematical) function which maps values from a large (possibly very large) domain into a smaller range. A "good" hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range

3.3.7

one-way function

a (mathematical) function f which is easy to compute, but which for a general value y in the range, it is computationally difficult to find a value x in the domain such that $f(x) = y$. There may be a few values y for which finding x is not computationally difficult

3.3.8

public key

(in a public key cryptosystem) that key of a user's key pair which is publicly known

3.3.9

private key (secret key — deprecated)

(in a public key cryptosystem) that key of a user's key pair which is known only by that user

3.3.10

simple authentication

authentication by means of simple password arrangements

3.3.11**security policy**

the set of rules laid down by the security authority governing the use and provision of security services and facilities

3.3.12**strong authentication**

authentication by means of cryptographically derived credentials

3.3.13**trust**

generally, an entity can be said to “trust” a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects. This trust may apply only for some specific function. The key role of trust in the authentication framework is to describe the relationship between an authenticating entity and a certification authority; an authenticating entity shall be certain that it can trust the certification authority to create only valid and reliable certificates

3.3.14**certificate serial number**

an integer value, unique within the issuing CA, which is unambiguously associated with a certificate issued by that CA

4 Notation and Abbreviations

4.1 The notation used in this part of ISO/IEC 9594 is defined in Table 1 below.

NOTE in the table, the symbols X , X_1 , X_2 etc. occur in place of the names of users, while the symbol I occurs in place of arbitrary information

4.2 The following abbreviations are used in this part of ISO/IEC 9594:

CA	Certification Authority
DIB	Directory Information Base
DIT	Directory Information Tree
PKCS	Public key cryptosystem

Table 1 — Notation

NOTATION	MEANING
X_p	public key of a user X .
X_s	secret key of X .
$X_p[I]$	encipherment of some information, I , using the public key of X .
$X_s[I]$	encipherment of I using the secret key of X .
$X\{I\}$	the signing of I by user X . It consists of I with an enciphered summary appended.
$CA(X)$	a certification authority of user X .
$CA^n(X)$	(where $n > 1$): $CA(CA(\dots n \text{ times} \dots (X)))$
$X_1 \ll X_2 \gg$	the certificate of user X_2 issued by certification authority X_1 .
$X_1 \ll X_2 \gg X_2 \ll X_3 \gg$	a chain of certificates (can be of arbitrary length), where each item is the certificate for the certification authority which produced the next. It is functionally equivalent to the following certificate $X_1 \ll X_{n+1} \gg$. For example, possession of $A \ll B \gg B \ll C \gg$ provides the same capability as $A \ll C \gg$, namely the ability to find out C_p given A_p .