

Australian Standard[®]

**Information technology—
Open Systems Interconnection—
The Directory**

Part 8: Authentication framework

This Australian Standard was prepared by Committee IT/1, Information Systems—Interconnection. It was approved on behalf of the Council of Standards Australia on 2 March 1992 and published on 16 April 1992.

The following interests are represented on Committee IT/1:

AUSSAT

Australian Association of Permanent Building Societies

Australian Bankers' Association

Australian Bureau of Statistics

Australian Committee of Directors and Principals

Australian Computer Society

Australian Computer Users Association

Australian Information Industry Association

Australian Telecommunications Users Group

Australian Vice Chancellors Committee

Confederation of Australian Industry

CSIRO—Institute of Information and Communication Technologies

Department of Defence

Department of Industry, Technology and Commerce

Information Exchange Steering Committee

Life Insurance Federation of Australia

OTC

Standards Association of New Zealand

Telecom Australia

Review of Australian Standards. *To keep abreast of progress in industry, Australian Standards are subject to periodic review and are kept up to date by the issue of amendments or new editions as necessary. It is important therefore that Standards users ensure that they are in possession of the latest edition, and any amendments thereto.*

Full details of all Australian Standards and related publications will be found in the Standards Australia Catalogue of Publications; this information is supplemented each month by the magazine 'The Australian Standard', which subscribing members receive, and which gives details of new publications, new editions and amendments, and of withdrawn Standards.

Suggestions for improvements to Australian Standards, addressed to the head office of Standards Australia, are welcomed. Notification of any inaccuracy or ambiguity found in an Australian Standard should be made without delay in order that the matter may be investigated and appropriate action taken.

Australian Standard[®]

**Information technology—
Open Systems Interconnection—
The Directory**

Part 8: Authentication framework

First published as AS 4019.8—1992.

PUBLISHED BY STANDARDS AUSTRALIA
(STANDARDS ASSOCIATION OF AUSTRALIA)
1 THE CRESCENT, HOMEBUSH, NSW 2140

ISBN 0 7262 7434 8

AVA **Documents**
Document Sharing Hub

PREFACE

This Standard was prepared by the Standards Australia Committee on Information Systems—Interconnection. It is identical with and has been reproduced from ISO/IEC 9594-8:1990, *Information technology—Open Systems Interconnection—The Directory—Part 8: Authentication framework*.

Technical Corrigendum 1 is found at the end of this Standard. Text affected by this Corrigendum is marked by a marginal bar.

The Standard is one of a series of Open Systems Interconnection (OSI) Standards which are currently under development. Since OSI Standards are developmental, there may be some minor difficulties encountered in their implementation. For this reason, Standards Australia will be providing, through the OSI Help Desk, a service to coordinate and disseminate information concerning difficulties which are identified in using this Standard.

Under arrangements made between Standards Australia and the international Standards bodies, ISO and IEC, as well as certain other Standards organizations, users of this Australian Standard are advised of the following:

- (a) Copyright is vested in Standards Australia.
- (b) The number of this Standard is not reproduced on each page; its identity is shown only on the cover and title pages.

For the purpose of this Australian Standard, the ISO/IEC text should be modified as follows:

- (i) *Terminology* The words ‘Australian Standard’ should replace the words ‘International Standard’ wherever they appear.
- (ii) *References* The references to International Standards should be replaced by references to Australian Standards as follows:

<i>Reference to International Standard or other publication</i>		<i>Australian Standard</i>	
ISO/IEC		AS	
7498	Information Processing Systems—Open Systems Interconnection—Basic Reference Model	2777	Information processing systems—Open Systems Interconnection—Basic reference model
7498-2	Part 2: Security Architecture	2777.2	Part 2: Security architecture
ISO			
8824	Information Technology—Open Systems Interconnection—Specifications of Abstract Syntax Notation One (ASN.1)	3625	Information technology—Open Systems Interconnection—Specification of Abstract Syntax Notation One (ASN.1)
8825	Information Technology—Open Systems Interconnection—Specification of Basic Encoding rules for Abstract Syntax Notation One (ASN.1)	3626	Information technology—Open Systems Interconnection—Specification of basic encoding for Abstract Syntax Notation One (ASN.1)
10021	Information Technology—Text Communication—Message Oriented Interchange System (MOTIS)	—	Information technology—Text communication—Message oriented text interchange systems
10021-3	Part 3: Abstract Service Definition Conventions	—	Part 3: Abstract service definition conventions

© Copyright — STANDARDS AUSTRALIA

Users of Standards are reminded that copyright subsists in all Standards Australia publications and software. Except where the Copyright Act allows and except where provided for below no publications or software produced by Standards Australia may be reproduced, stored in a retrieval system in any form or transmitted by any means without prior permission in writing from Standards Australia. Permission may be conditional on an appropriate royalty payment. Requests for permission and information on commercial software royalties should be directed to the head office of Standards Australia.

Standards Australia will permit up to 10 percent of the technical content pages of a Standard to be copied for use exclusively in-house by purchasers of the Standard without payment of a royalty or advice to Standards Australia.

Standards Australia will also permit the inclusion of its copyright material in computer software programs for no royalty payment provided such programs are used exclusively in-house by the creators of the programs.

Care should be taken to ensure that material used is from the current edition of the Standard and that it is updated whenever the Standard is amended or revised. The number and date of the Standard should therefore be clearly identified.

The use of material in print form or in computer software programs to be used commercially, with or without payment, or in commercial contracts is subject to the payment of a royalty. This policy may be varied by Standards Australia at any time.

CONTENTS

	<i>Page</i>
SECTION 1: GENERAL	4
1 Scope	4
2 Normative references	4
3 Definitions	5
4 Notation and Abbreviations	6
SECTION 2: SIMPLE AUTHENTICATION	6
5 Simple Authentication Procedure	6
SECTION 3: STRONG AUTHENTICATION	8
6 Basis of Strong Authentication	8
7 Obtaining a User's Public Key	9
8 Digital Signatures	11
9 Strong Authentication Procedures	13
10 Management of Keys and Certificates	14
Annex A — Security Requirements	17
Annex B — An Introduction to Public Key Cryptography	20
Annex C — The RSA Public Key Cryptosystem	21
Annex D — Hash Functions	23
Annex E — Threats Protected Against by the Strong Authentication Method	24
Annex F — Data Confidentiality	25
Annex G — Authentication Framework in ASN.1	26
Annex H — Reference Definition of Algorithm Object Identifiers	29

Information technology—Open Systems Interconnection—The Directory

Part 8: Authentication framework

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 offline 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 3.3f) (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.

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.

Note — In the table, the symbols X, X₁, X₂ etc. occur in place of the names of users, while the symbol I occurs in place of arbitrary information.

4 Notation and Abbreviations

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

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(...n times...(X)))
X ₁ «X ₂ »	the certificate of user X ₂ issued by certification authority X ₁ .
X ₁ «X ₂ »X ₂ «X ₃ »	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 «X _{n+1} ». For example, possession of A«B»B«C» provides the same capability as A«C», namely the ability to find out C _p given A _p .
X _{1p} • X ₁ «X ₂ »	the operation of unwrapping a certificate (or certificate chain) to extract a public key. It is an infix operator, whose left operand is the public key of a certification authority, and whose right operand is a certificate issued by that certification authority. The outcome is the public key of the user whose certificate is the right operand. For example: A _p • A«B» B«C» denotes the operation of using the public key of A to obtain B's public key, B _p , from its certificate, followed by using B _p to unwrap C's certificate. The outcome of the operation is the public key of C, C _p .
A → B	a certification path from A to B, formed of a chain of certificates, starting with CA(A)«CA ² (A)» and ending with CA(B)«B».

SECTION 2: SIMPLE AUTHENTICATION

5 Simple Authentication Procedure

5.1 Simple authentication is intended to provide local authorization based upon a Distinguished Name of a user, a bilaterally agreed (optional) password, and a bilateral understanding of the means of using and handling this password within a single domain. Utilization of simple authentication is primarily intended for local use only, i.e. for peer entity authentication between one DUA and one DSA or between one DSA and one DSA. Simple authentication may be achieved by several means:

- the transfer of the user's distinguished name and (optional) password in the clear (non-protected) to the recipient for evaluation;
- the transfer of the user's distinguished name, password, and a random number and/or a timestamp, all of which are protected by applying a one-way function;
- the transfer of the protected information described in b) together with a random number and/or a timestamp, all of which is protected by applying a one-way function.

Notes

1. There is no requirement that the one-way functions applied be different.
2. The signalling of procedures for protecting passwords may be a matter for extension to the document.

5.2 Where passwords are not protected, a minimal degree of security is provided for preventing unauthorized access. It should not be considered a basis for secure services. Protecting the user's distinguished name and password provides greater degrees of security. The algorithms to be used for the protection mechanism are typically non-enciphering one-way functions that are very simple to implement.

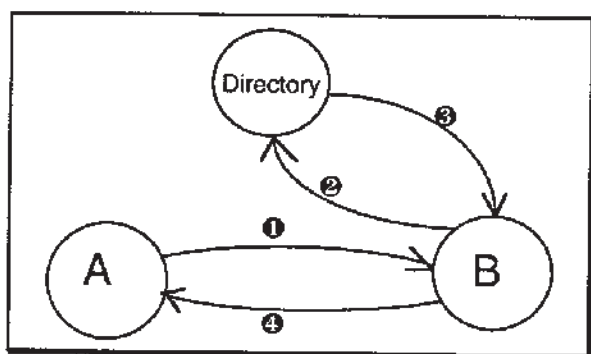


Figure 1 — The Unprotected Simple Authentication Procedure

5.3 The general procedure for achieving simple authentication is shown in figure 1.

5.3.1 The following steps are involved:

- 1 an originating user A sends its distinguished name and password to a recipient user B;
- 2 B sends the purported distinguished name and password of A to the Directory, where the password is checked against that held as the **UserPassword** attribute within the directory entry for A (using the Compare operation of the Directory);
- 3 the Directory confirms (or denies) to B that the credentials are valid;
- 4 the success (or failure) of authentication may be conveyed to A.

5.3.2 The most basic form of simple authentication involves only step 1 and after B has checked the distinguished name and password, may include step 4

5.4 Figure 2 illustrates two approaches by which protected identifying information may be generated. $f1$ and $f2$ are one-way functions (either identical or different) and the timestamps and random numbers are optional and subject to bilateral agreements.

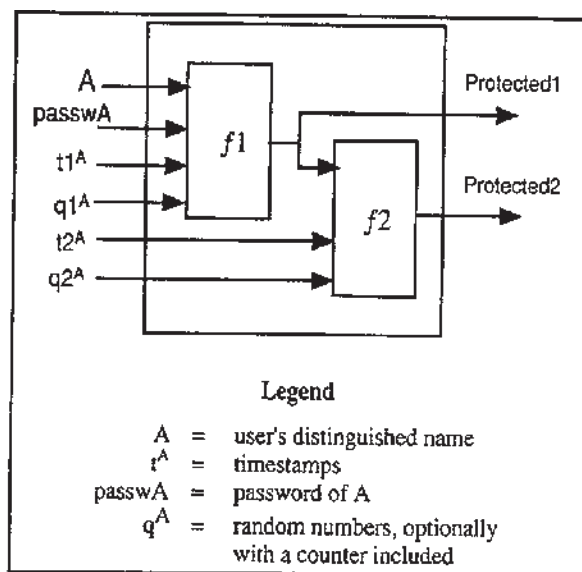


Figure 2—Protected Simple Authentication

5.4.1 Figure 3 illustrates the procedure for protected simple authentication.

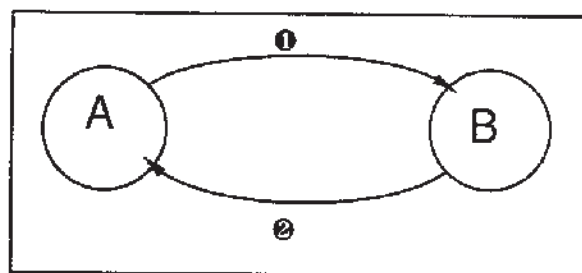


Figure 3 — The Protected Simple Authentication Procedure

The following steps are involved (initially using $f1$ only):

- 1 an originating user, user A, sends its protected identifying information (Authenticator 1) to user B. Protection is achieved by applying the one-way function ($f1$) of figure 2, where the timestamp and/or random number (when used) is used to minimize replay and to conceal the password.

The protection of A's password is of the form:

$$\text{Protected1} = f1(t1^A, q1^A, A, \text{passwdA})$$

The information conveyed to B is of the form:

$$\text{Authenticator1} = t1^A, q1^A, A, \text{Protected1}$$

B verifies the protected identifying information offered by A by generating (using the distinguished name and optional timestamp and/or random number provided by A, together with a local copy of A's password) a local protected copy of A's password (of the form Protected1). B compares for equality the purported identifying information (Protected1) with the locally generated value.

- ② B confirms or denies to A the verification of the protected identifying information.

5.4.2 The procedure of 5.4.1 can be modified to afford greater protection using f_1 and f_2 . The main differences are as follows:

- ① A sends its additionally protected identifying information (Authenticator2) to B. Additional protection is achieved by applying a further oneway function, f_2 , as illustrated in figure 2. The further protection is of the form:

$$\text{Protected2} = f_2(t_2^A, q_2^A, \text{Protected1})$$

The information conveyed to B is of the form:

$$\text{Authenticator2} = t_1^A, t_2^A, q_1^A, q_2^A, A, \text{Protected2}$$

For comparison, B generates a local value of A's additionally protected password and compares it for equality with that of Protected2 (this is similar in principle to step ① of 5.4.1).

- ② B confirms or denies to A the verification of the protected identifying information.

Note — The procedures defined in these clauses are specified in terms of A and B. As applied to the Directory (specified in ISO/IEC 9594-3 and ISO/IEC 9594-4), A could be a DUA binding to a DSA, B; alternatively, A could be a DSA binding to another DSA, B.

5.5 A User Password attribute type contains the password of an object. An attribute value for the user password is a string specified by the object.

**UserPassword ::= ATTRIBUTE
WITH ATTRIBUTE-SYNTAX
OCTET STRING (SIZE (0..ub-user-password))
MATCHES FOR EQUALITY**

5.6 The following ASN.1 macro may be used to define the data type arising from applying a one-way function to a given other data type:

PROTECTED MACRO ::= SIGNATURE

SECTION 3: STRONG AUTHENTICATION

6 Basis of Strong Authentication

6.1 The approach to strong authentication taken in this part of ISO/IEC 9594 makes use of the properties of a family of cryptographic systems, known as public-key cryptosystems (PKCS). These cryptosystems, also described as asymmetric, involve a pair of keys, one secret and one public, rather than a single key as in conventional cryptographic systems. Annex B gives a brief introduction to these cryptosystems and the properties which make them useful in authentication. For a PKCS to be usable in this authentication framework at this present time, it shall have the property that both keys in the key pair can be used for encipherment, with the secret key being used to decipher if the public key was used, and the public key being used to decipher if the secret key was used. In other

words, $X_p \cdot X_s = X_s \cdot X_p$ where X_p/X_s are encipherment/decipherment functions using the public/private keys of user X.

Note — Alternative types of PKCS, i.e., ones which do not require the property of permutability and that can be supported without great modification to this part of ISO/IEC 9594, are a possible future extension.

6.2 This authentication framework does not mandate a particular cryptosystem for use. It is intended that the framework shall be applicable to any suitable public key cryptosystem, and shall thus support changes to the methods used as a result of future advances in cryptography, mathematical techniques or computational

capabilities. 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 shall serve to maximize the community of users able to authenticate and communicate securely. One example of a cryptographic algorithm can be found in annex C.

6.3 Authentication relies on each user possessing a unique distinguished name. The allocation of distinguished names is the responsibility of the Naming Authorities. Each user shall therefore trust the Naming Authorities not to issue duplicate distinguished names.

6.4 Each user is identified by its possession of its secret key. A second user is able to determine if a communication partner is in possession of the secret key, and can use this to corroborate that the communication partner is in fact the user. The validity of this corroboration depends on the secret key remaining confidential to the user.

6.5 For a user to determine that a communication partner is in possession of another user's secret key, it shall itself be in possession of that user's public key. Whilst obtaining the value of this public key from the user's entry in the Directory is straightforward, verifying its correctness is more problematic. there are many possible ways for doing this: clause 7 describes a process whereby a user's public key can be checked by reference to the Directory. This process can only operate if there is an unbroken chain of trusted points in the Directory between the users requiring