AS 4539.1.3—1999
(Incorporating Amendment No. 1)

Australian Standard™

Information technology—Public Key Authentication Framework (PKAF)

Part 1.3: General—X.509 supported algorithms profile

Standards Australia

This Australian Standard was prepared by Committee IT/12, Information Systems, Security and Identification Technology. It was approved on behalf of the Council of Standards Australia on 30 December 1998 and published on 5 May 1999.

The following interests are represented on Committee IT/12:

Attorney-General's Department

Australia Post

Australian Association of Permanent Building Societies

Australian Bankers Association

Australian Chamber of Commerce and Industry

Australian Customs Service (Commonwealth)

Australian Electrical and Electronic Manufacturers Association

Australian Information Industry Association

Consumers Federation of Australia

Department of Defence (Australia)

N.S.W. Police Service

Reserve Bank of Australia

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Australia web site at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Australian Standard*, has a full listing of revisions and amendments published each month.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.com.au, or write to the Chief Executive, Standards Australia International Ltd, PO Box 1055, Strathfield, NSW 2135.

This Standard was issued in draft form for comment as DR 98411.

Australian Standard™

Information technology—Public Key Authentication Framework (PKAF)

Part 1.3: General—X.509 supported algorithms profile

First published as AS 4539.1.3—1999.
Reissued incorporating Amendment No. 1 (June 2000).

Published by Standards Australia International Ltd
PO Box 1055, Strathfield, NSW 2135, Australia

ISBN 0 7337 2554 6

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT/12, Information Systems, Security and Identification Technology.

This Standard incorporates Amendment No. 1 (June 2000). The changes required by the Amendment is indicated in the text by a marginal bar and amendment number against the clause, note, table, figure, or part thereof affected.

The Standard is the result of a consensus among representatives on the Joint Committee that it be produced as an Australian Standard.

The objective of this Standard is to specify the Public Key Authentication Framework (PKAF) profile for X.509 supported algorithms. This Standard has been produced to facilitate interoperability between systems that create and use digital signatures, certificates and certificate revocation lists within the Australian PKAF.

This Standard is one of a series of PKAF Standards under development. Other Parts in the series will be as follows:

General — PKAF architecture

General — X.509 certificate and Certification Revocation Lists (CRL) profile

Accreditation — A framework for assurance of Certification Authorities

Registration — Identification and authentication

Registration — Selected identification items

CONTENTS

STANDARDS AUSTRALIA

Australian Standard

Information technology — Public Key Authentication Framework (PKAF)

Part 1.3: General — X.509 supported algorithms profile

1 SCOPE

This Standard specifies a profile of supported algorithms for use within X.509 certificates and certificate revocation lists (CRLs) to support generic applications requiring broad interoperability and limited special purposes requirements.

The Standard lists digital signature algorithms as well as formats for the keys used in X.509 certificates, as described in ISO/IEC 9594-8, ITU-T Rec.X.208 and ITU-T Rec.X.509. An object identifier is defined for each algorithm along with ASN.1 types for its parameters and output values.

The Standard stipulates which algorithms are required for PKAF-compliant implementations.

2 COMPLIANCE

Certification authorities (CAs) and applications shall use and support the algorithms as specified in Clause 6. Conforming CAs shall use the identified object identifiers (OIDs) when issuing certificates containing public keys for these algorithms. Conforming applications supporting any of these algorithms shall, at a minimum, recognize the OIDs identified in this Standard.

3 NORMATIVE REFERENCES

The following documents are referred to in this Standard:

ISO/IEC

9594 Information technology—Open Systems Interconnection—The Directory

9594-8 Part 8: Authentication framework

ITU-T

Rec. X.208 Specification of Abstract Syntax Notation One (ASN.1)

Rec. X.509 Information Technology—Open systems interconnection—The directory: Authentication framework

4 ABBREVIATIONS

For the purpose of this Standard, the abbreviations below apply.

ASN.1	Abstract Syntax Notation One
CA	Certification Authority (i.e. any implementation that can create certificates)
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FIPS	US Federal Information Processing Standard