

Australian Standard™

**Information technology—Public Key
Authentication Framework (PKAF)**

**Part 1.2.2: General—PICS Proforma for
digital signature certificates**



This Australian Standard was prepared by Committee IT-012, Information Systems, Security and Identification Technology. It was approved on behalf of the Council of Standards Australia on 21 November 2000 and published on 23 January 2001.

The following interests are represented on Committee IT-012:

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)
Department of Social Welfare, New Zealand
Government Communications Security Bureau, New Zealand
New Zealand Defence Force
NSW 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 Standards may also be withdrawn.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, GPO Box 5420, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 00103.

Australian Standard™

Information technology—Public Key Authentication Framework (PKAF)

Part 1.2.2: General—PICS Proforma for digital signature certificates

First published as AS 4539.1.2.2—2001.

COPYRIGHT

© Standards Australia International

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 3731 5

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification Technology.

There was 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 profile for the signature certificates (PAA, PCA, CA, external domain certificates and end use entities) for use in the Public Key Authentication Framework (PKAF)

This Standard is Part 1.2.2 of a series which, when complete, will consist of the following:

AS

4539 Information technology—Public Key Authentication Framework (PKAF)

4539.1.2.1 Part 1.2.1: General—X.509 Certificate and Certificate Revocation Lists (CRL) profile

4539.1.2.2 Part 1.2.2: General—PICS Proforma for digital signature certificates (this Standard)

4539.1.2.3 Part 1.2.3: General—PICS Proforma for Certificate Revocation Lists (CRL)

4539.1.3 Part 1.3: General—X.509 supported algorithms profile

4539.2.1 Part 2.1: Assurance framework—Certification Authorities

Statements expressed in mandatory terms in notes to tables are deemed to be requirements of this Standard.

The IT-012 Committee acknowledges the work of Subcommittee IT-012-04-01 in the production of this document. In particular the following organizations had significant input:

Adacel Technologies Ltd

Australian Stock Exchange

Authentic8 Pty Ltd

Baltimore

Centrelink

Defence Signal Directorate

Department of Communications, Information Technology & the Arts

DSTC Pty Ltd

Eracom Pty Ltd

Ernst & Young

Gadens Lawyers

Health Insurance Commission

Office for Government Online

Office of Information Technology NSW

Pacific Research Pty Limited

Price Waterhouse

QANTAS Airways Ltd

Quadriga Consulting Group

Rotek

Security Consulting Services

Spyrus Consulting Services

Telstra Corporation Limited

WESTPAC Banking Corporation

CONTENTS

	<i>Page</i>
1 SCOPE.....	4
2 APPLICATION	4
3 REFERENCED DOCUMENTS.....	4
4 DEFINITIONS	4
5 ABBREVIATIONS	5
6 DESCRIPTION OF TABLES.....	6
7 SUPPORT CLASSIFICATIONS	6
8 IDENTIFICATION OF THE IMPLEMENTATION.....	8
9 PAA SIGNATURE CERTIFICATE	9
10 PCA SIGNATURE CERTIFICATE	13
11 CA SIGNATURE CERTIFICATE.....	17
12 EXTERNAL DOMAIN CERTIFICATES	21
13 EE SIGNATURE CERTIFICATE	25
14 COMMON FIELDS.....	29

STANDARDS AUSTRALIA

Australian Standard

Information technology—Public Key Authentication Framework (PKAF)

Part 1.2.2: General—PICS Proforma for digital signature certificates

1 SCOPE

This Standard provides the Profile for the Signature Certificates (PAA, PCA, CA, external domain certificates, and end entities) for use in the Public Key Authentication Framework (PKAF).

NOTE: The structure for the Certificate is defined in the 1997 version of ITU-T X.509 / ISO/IEC 9594-8.

2 APPLICATION

The supplier of an implementation that claims to conform to ITU-T Rec. X.509 / ISO/IEC IS 9594-8 is required to complete a copy of the PICS Proforma provided in Sections 8 through 14 of this Standard and is required to provide information necessary to identify both the supplier and the implementation.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS

- | | |
|------------|--|
| 4539 | Information technology—Public Key Authentication Framework (PKAF) |
| 4539.1.2.3 | Part 1.2.3: General PICS Proforma for Certificate Revocation Lists (CRL) |
| 4539.1.3 | Part 1.3: General—X.509 supported algorithms profile |

ISO/IEC

- | | |
|--------|---|
| 9594 | Information technology—Open Systems Interconnection—The directory |
| 9594-8 | Part 8: Authentication framework |
| 9646 | Information technology—Open Systems Interconnection—Conformance testing methodology and framework |

ITU-T

- | | |
|------------|---|
| Rec. X.509 | Information Technology—Open Systems Interconnection—The Directory: Authentication Framework |
|------------|---|

IETF

- | | |
|---------|--|
| RFC2459 | Internet X.509 Public Key Infrastructure Certificate and CRL Profile |
|---------|--|

4 DEFINITIONS**4.1 Certificate definitions**

Certificate definitions given in ISO/IEC 9594-8 apply.

4.2 Conformance definitions

Conformance definitions given in ISO/IEC 9646-8 apply, i.e. those for conformance, mandatory requirement, optional requirement, and conditional requirement.

4.3 PAA certificate

A self-signed certificate issued by the Policy Approval Authority (PAA).

4.4 PCA certificate

A certificate issued to a Policy Certification Authority (PCA).

4.5 CA certificate

A certificate issued to a Certification Authority that is part of the PKAF, but which is neither a PAA, nor a PCA.

4.6 EE Certificate

A certificate issued to an End Entity (EE).

4.7 External Domain certificate

A certificate issued to a CA outside of the PKAF, but which is considered useable by applications within the PKAF.

4.8 Conforming certificate

A certificate that conforms to this profile

4.9 Conforming CA certificate

A PAA, PCA, CA or External Domain Certificate that conforms to this profile.

4.10 Conforming CA

A CA that issues conforming certificates and CRLs.

4.11 Conforming CRL

A Certification Revocation List that conforms to this profile.

4.12 Conforming Application

An application that can process conforming certificates and CRLs, and may process other certificates or CRLs.

5 ABBREVIATIONS

For the purposes of this Standard, the following abbreviations below apply.

ASN.1	Abstract Syntax Notation One
CA	Certification Authority
CRL	Certificate Revocation List
DN	Distinguished Name
EE	End Entity
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
OID	Object Identifier
PAA	Policy Approval Authority
PCA	Policy Creation Authority
PKAF	Public Key Authentication Framework
RFC	Request For Comment
SHA-1	Secure Hash Algorithm

6 DESCRIPTION OF TABLES

The following items give a guide to interpreting the tables:

- (a) The 'Item' and 'Notes' columns are provided for cross-referencing. The numbers in the 'Item' column are the row numbers. The numbers in the 'Notes' column indicate the table numbers followed by the 'item' number enclosed in parentheses. These two columns are used together to point to sub-elements. The 'Notes' column also refers to additional information supplied in the last row of the table.
- (b) The 'Protocol elements' column refers to the name of ASN.1 fields taken from the X.500 recommendations.
- (c) In each table, the 'Base' column reflects the level of support required for conformance to the base Standard*. The level of support refers to the support classification for the 'Base' column. The 'Base' column is broken into 'Proc.' (i.e. processing) and generation (i.e. Gen) columns. The 'Proc.' column reflects the level of support required by compliant certificate processing and using entities who process certificates. The 'Gen.' column reflects the level of support required in compliant signature certificates (i.e. the information that is included in the certificate). The types of signature certificates include: PAA (see Clause 9), PCA (see Clause 10), CA (see Clause 11), External Domain certificates (see Clause 12), and End Entities (see Clause 13). When the CA acts as an End Entity (e.g. when a CA verifies the signature on a message), then the 'Proc.' column applies.†
- (d) The 'Support' column is provided for completion by the supplier of the implementation as follows:

Y	The protocol element is fully supported (i.e., supporting the requirements of the m support classification).
N	The protocol element is not fully supported, further qualified to indicate the action taken on receipt of such an element as follows: ND - the element is discarded/ignored. NR - the PDU is rejected.
– or blank	The protocol element is not applicable.

7 SUPPORT CLASSIFICATIONS

Each of the protocol elements listed in Clauses 9‡, 10, 11, 12, and 13, and 14 are designated as having a support requirement of mandatory or optional. Where protocol elements are nested (i.e., the elements contain sub-elements), the requirement to support the nested element is relevant only when the immediately containing (parent) element is supported.

To specify the support level of the protocol elements, the following terminology is defined.

* If the PKAF defined a certificate extension, field, or attribute not in the base Standard (i.e., X.509), the classification for the 'Base' column is '—'

† 'Proc.' columns in the PAA, PCA, CA, External Domain, and EE certificate tables are identical.

‡ Implementation of Clause 9 is dependent on national policy. Formatting the trusted public key as a self-signed certificate is dependent on national policy (see CMI Authentication Framework).

7.1 Static capability

The following classifications are used to specify static conformance (i.e. capability):

- (a) *Mandatory support (m)* Implementations claiming to create certificates shall be able to generate the protocol element. Implementations claiming to process certificates shall be able to receive the protocol elements and perform all associated procedures (i.e., implying the ability to handle both the syntax and the semantics of the element) as relevant.
- (b) *Optional (o)* Implementations claiming to create certificates are not required to support generation of the protocol element. If support is claimed, the element shall be treated as if it were specified as mandatory support, and the sub-elements, if present, shall be supported as specified. Implementations claiming to perform processing of certificates shall ignore the protocol element and continue processing of the certificate.
- (c) *Conditional (c)* Implementations shall support the protocol element under the conditions specified. If the conditions are met, the protocol element shall be treated as if it were specified as mandatory support. If these conditions are not met, the protocol element shall be treated as if it were specified as optional support (unless otherwise stated).
- (d) *Not applicable (–)* This element is not applicable in the particular context in which this classification is used.

7.2 Dynamic capability

Only one classification is used to specify dynamic conformance (i.e., behaviour).

This is *Required (r)*. The information for this protocol element must be populated upon certificate generation.

8 IDENTIFICATION OF THE IMPLEMENTATION

8.1 Identification of PICS

Item	Question	Response
1	Date of statement (DD/MM/YYYY)	
2	PICS serial number	
3	System conformance statement cross reference	

8.2 Identification of implementation and/or system

Item	Question	Response
1	Implementation name	
2	Implementation version	
3	Machine name	
4	Machine version	
5	Operating system name	
6	Operating system version	
7	Special configuration	
8	Other information	

8.3 Identification of system supplier and/or test laboratory client

Item	Question	Response
1	Organization name	
2	Contact name(s)	
3	Address	
4	Telephone number	
5	Telex number	
6	Fax number	
7	E-mail address	
8	Other information	

8.4 Identification of the certificate

Item	Question	Response
1	Title, reference number and date of publication of the Standard	
2	Certificate Version Number	

8.5 Global statement of conformance

Item	Question	Response	Comments
1	Are all mandatory base standards requirements implemented?		See note

NOTE: Answering 'No' to this Section indicates non-conformance to the information object specification. Unsupported mandatory capabilities are to be identified in the IO-ICS, with an explanation of why the implementation is non-conformant.

9 PAA SIGNATURE CERTIFICATE

Item	Protocol element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	signed	m	mr	m	mr			
2	toBeSigned	m	mr	m	mr			
3	version	m	mr	m	mr			
4	serialNumber	m	mr	m	mr			
5	signature	m	mr	m	mr			See note
6	issuer	m	mr	m	mr			
7	validity	m	mr	m	mr			
8	notBefore	m	mr	m	mr			
9	notAfter	m	mr	m	mr			
10	subject	m	mr	m	mr			
11	subjectPublicKeyInfo	m	mr	m	mr			
12	algorithm	m	mr	m	mr			
13	subjectPublicKey	m	mr	m	mr			
14	issuerUniqueIdentifier	o	o	m	o			
15	subjectUniqueIdentifier	o	o	m	o			
16	extensions	o	o	m	mr			
17	algorithmIdentifier	m	m	m	mr			See note
18	encrypted	m	m	m	mr			

NOTE: Population of the 'parameter' sub-field is not recommended, as the values in this field will be ignored.

9.1 Algorithm identifier

Item	Protocol element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	algorithm	m	m	m	mr			
2	parameters	m	m	m	mr			See note

NOTE: The parameters p, q and g shall be present in the PAA certificate (see AS 4539.1.2.3).

9.2 Extensions

Item	Protocol element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	extnID	m	m	m	mr			See note
2	critical	m	m	m	mr			d(false)
3	extnValue	m	m	m	mr			

NOTE: The support requirements for PAA certificate extensions are listed in Clause 9.2.1.