Australian Standard™

Information technology—Public Key Authentication Framework (PKAF) related Standards

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

Standards Australia

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 18 April 2001 and published on 15 May 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 Standards may also be withdrawn.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 00343.

Australian Standard™

Information technology—Public Key Authentication Framework (PKAF) related Standards

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

First published as AS 4539.1.2.3—2001.

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

ISBN 0 7337 3899 0

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 committee that it be produced as an Australian Standard.

The objective of this Standard is to specify the Profile for the Certificate Revocation (CRL) for use in the Public Key Authentication Framework (PKAF) CMI. The structure for the CRL is defined in the 1997 version of ITU-T X.509 / ISO/IEC 9594-8.

The AS 4539 series of Standards is as follows:

AS		
4539		Information technology—Public Key Authentication Framework (PKAF)
4539.1.2.2	Part 1.2.2	General—PICS Proforma for digital signature certificates
4539.1.2.3	Part 1.2.3	General—PICS Proforma for Certificate Revocation Lists (CRL) (this Standard)
4539.1.3	Part 1.3	General—X.509 supported algorithms profile
4539.2.1	Part 2.1	Assurance framework—Certification Authorities

Parts of the AS 4539 series of Standards under development are:

Part 1.1	General—PKAF architecture
Part 1.2.1	General—X.509 Certificate and Certification Revocation Lists (CRL) profile

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-012/4/1 in the production of this document. In particular the following organizations had significant input:
Adacel Technologies
Australian Stock Exchange
Authentic8
Baltimore
Centrelink
Defence Signal Directorate
Department of Communications, Information Technology & the Arts
DSTC
Eracom
Ernst & Young
Gadens Lawyers
Health Insurance Commission
Office for Government Online
Office of Information Technology N.S.W.
Pacific Research
Price Waterhouse
QANTAS
Quadriga Consulting Group
Rotek
Security Consulting Services
Spyrus Consulting Services
Telstra
WESTPAC Banking Corporation

CONTENTS

STANDARDS AUSTRALIA

Australian Standard

Information technology—Public Key Authentication Framework (PKAF) related Standards

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

1 SCOPE

This Standard specifies the Profile for the Certificate Revocation (CRL) for use in the Public Key Authentication Framework (PKAF) CMI.

NOTE: The structure for the CRL 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 9594-8 is required to complete a copy of the PICS Proforma provided in Sections 8 to 10 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)
4539.1.3	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).

