Australian Standard™

Information technology—Public Key Authentication Framework (PKAF)

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

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 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 Standards may also be withdrawn.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 00050.

Australian Standard™

Information technology—Public Key Authentication Framework (PKAF)

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

First published as AS 4539.1.2.1—2001.

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

ISBN 0 7337 3730 7

PREFACE

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

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 Version 3 (V3) certificates and Version 2 (V2) Certificate Revocation Lists (CRL).

This Standard is Part 1.2.1 one of a series which, when complete, will consist of the following:

AS
4539 Information technology—Public Key Authentication Framework (PKAF)
Part 1.2.1: General—X.509 certificate and Certificate Revocation Lists (CRL) profile (this Standard)
Part 1.2.2: PICS Proforma for digital signature certificates and CRL
Part 1.2.3: Genral—PICS Proforma for Certificate Revocation Lists (CRL)
Part 1.3: General—X.509 supported algorithms profile
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/12/4/1 in the production of this document. In particular the following organizations:

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

INTRODUCTION

This Standard facilitates the interoperability of certificate management systems within the Australian PKAF.

X.509 Version 3 (V3) certificates contain the identity and attribute data of a subject using a base certificate with applicable extensions. The base certificate contains such information as the version number of the certificate, the certificate's identifying serial number, the signature algorithm used to sign the certificate, the issuer's distinguished name, the validity period of the certificate, the distinguished name of the subject and the subject's public key. To this base certificate is appended numerous certificate extensions. This Standard describes those extensions and stipulates which extensions are required for PKAF-compliant implementations.

STANDARDS AUSTRALIA

Australian Standard

Information technology—Public Key Authentication Framework (PKAF)

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

1 SCOPE

This Standard specifies the PKAF profile for X.509 Version 3 (V3) Certificates and Version 2 (V2) Certificate Revocation List (CRL). Implementation guidance is provided for certificate generation entities (e.g., Certification Authority [CA]) and certificate processing entities.

2 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

3 DEFINITIONS

3.1 Certificate definitions

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

3.2 Conformance definitions

Conformance definitions given in ISO/IEC 9646, ie. those for conformance, mandatory requirement, optional requirement, and conditional requirement apply.

3.3 PAA certificate

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

3.4 PCA certificate

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