Australian Standard™

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

Part 1.1: General—PKAF architecture

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 25 March 2002 and published on 15 May 2002.

The following interests are represented on Committee IT-012:

Attorney Generals 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

Government Communications Security Bureau, New Zealand

New Zealand Defence Force

New South Wales 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 Standards may also be withdrawn.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 01239.

Australian Standard™

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

Part 1.1: General—PKAF architecture

First published as AS 4539.1.1—2002.

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

ISBN 0 7337 4496 6

PREFACE

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

After consultation with stakeholders in both countries, Standards Australia and Standards New Zealand decided to develop this Standard as an Australian Standard, rather than an Australian/New Zealand Standard.

The objective is to describe the high level architecture of the Public Key Authentication Framework (PKAF) and to facilitate the interoperability of Certificate Management Systems within the Australian PKAF.

This Standard is Part 1.1 of the AS 4539 series dealing with the PKAF, which are published in the following parts:

AS 4539 Information technology—Public Key Authentication Framework (PKAF)

- Part 1.1: General—PKAF architecture (this Standard)
- Part 1.2.1: General—X.509 certificate and Certification Revocation Lists (CRL) profile
- Part 1.2.2: General—PICS Proforma for digital signature certificates
- Part 1.2.3: General—PICS Proforma for Certificate Revocation Lists (CRL)
- Part 1.3: General—X.509 supported algorithms profile
- Part 2.1: Assurance framework—Certification authorities

CONTENTS

STANDARDS AUSTRALIA

Australian Standard

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

Part 1.1: General—PKAF architecture

1 SCOPE

This document describes the architecture to provide a scheme where a digital signature (with an associated public/private key pair) will be linked to a particular distinguished name by a chain of Public-key Certificates.

The ownership of, and right to use, the distinguished name is outside the scope of this Standard.

The creation of Public-key Certificates for authorization, privilege management, delegation of authority, confidentiality or key management purposes is outside the scope of this Standard.

The internal design of Certification Authorities is outside the scope of this Standard.

2 REFERENCES

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
4539.1.3	Part 1.3: General—X.509 supported algorithms profile
4539.2.1	Part 2.1: Assurance framework—Certification authorities
MP 59	Naming and addressing in the Australian OSI environment
ITU-T	
Rec.X.509	ISO/IEC 9594-8:2000 Information Technology—Open Systems Interconnection—The Directory: public-key and attribute certificate frameworks

3 DEFINITIONS

For the purposes of this Standard the following definitions apply:

3.1 OSI directory Public-key and Attribute Certificate frameworks

The following terms are defined in ITU-T Rec. X.509 | ISO/IEC 9594-8:

(a) Authority.

(b) Authority Certificate.

(c) Attribute Certificate.

(d) CA-certificate.

(e) Certificate Policy.

(f) Certificate Revocation List (CRL).

(g) Certificate.

