AS 4860—2007

Australian Standard®

Knowledge-based identity authentication—Recognizing Known Customers

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 June 2007.
This Standard was published on 12 July 2007.

The following 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 Electrical and Electronic Manufacturers Association
- Australian Information Industry Association
- Certification Forum of Australia
- Consumers' Federation of Australia
- Council of Small Business Organisation of Australia
- Department of Defence (Australia)
- Department of Social Welfare, New Zealand
- Government Communications Security Bureau, New Zealand
- Internet Industry Association
- NSW Police
- New Zealand Defence Force
- Reserve Bank of Australia

This Standard was issued in draft form for comment as DR 07082.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that 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Standards may also be withdrawn.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 that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting **www.standards.org.au**

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at **mail@standards.org.au**, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard®

Knowledge-based identity authentication—Recognizing Known Customers

First published as AS 4860—2007.

Published by Standards Australia GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 8284 1

PREFACE

This Standard was prepared by the Australian members of the Joint Standards Australia/Standards New Zealand Committee, IT-012, Information Security. After consultation with stakeholders in both countries, Standards Australia and Standards New Zealand decided to develop this as an Australian, rather than an Australian/New Zealand Standard.

Security of electronic access to facilities and services often depends on the ability to remotely authenticate the identity of people. Authentication is a complex topic and a number of standards exist to facilitate the design of authentication solutions. For example:

(a) ISO 10181-2* specifies an authentication framework for open systems interconnection.

(b) AS 4539.1.1† specifies an authentication architecture relevant to public key infrastructure.

(c) ISO/IEC 7498‡ specifies a model and mechanisms for entity authentication.

(d) AS 4590§ specifies syntax for identity attributes.

This Standard is relevant to provisioning electronic access to facilities (e.g. provisioning remote access to web services) within an authentication framework and provides requirements that allow organizations to share authenticated knowledge about a person's identity for the purposes of provisioning electronic access to services and facilities, while protecting that person's privacy.

Appendix A is normative and describes the access control lifecycle model that is relevant to the scope of this Standard. Appendix B is informative and gives an example of identity assurance classification levels. Appendix C is informative and discusses the use of common identity authentication credentials by more than one relying party. Appendix D is informative and summarizes the requirements in this Standard that provide privacy protection.

The terms 'normative' and 'informative' have been used in this Standard to define the application of the appendix to which they apply. A 'normative' appendix is an integral part of a Standard, whereas an 'informative' appendix is only for information and guidance.

Standards Australia gratefully acknowledges the financial assistance and technical input from the Australian Government Information Management Office (AGIMO) into the development of this Standard.

---

* ISO 10181-2:1996, Information technology—Open Systems Interconnection—Security frameworks for open systems: Authentication framework—Part 2

† AS 4539.1.1—2002, Information technology—Public Key Authentication Framework (PKAF) related Standards Part 1.1: General—PKAF architecture

‡ ISO/IEC 7498 (all parts) Information technology—Open Systems Interconnection—Basic Reference model

§ AS 4590—2006, Interchange of client information

CONTENTS

Page

FOREWORD

Electronic access to services and facilities is common in a variety of situations, for example:

(a) Electronic access by people to on-line enterprise applications doing their job.

(b) Electronic access by people to on-line web services over the internet for a variety of personal purposes.

(c) Electronic access by people to buildings using an electronic access card.

(d) Electronic identity authentication when people access services with the assistance of service-provider staff.

Electronic access to services and facilities is often convenient and efficient. However, prevention of fraud and other crime arising from misrepresentation of the identity of users is a major challenge to providers of services and managers of facilities with electronic access. This challenge is typically met by applying identification standards (concerning who people are) and identity authentication standards (concerning assurance that a person is who they claim to be) when people apply for access to services and facilities.

In some cases, identity authentication standards are mandated by regulations. In other cases, they are determined in an ad hoc manner by the provider of services or the manager of facilities. Whatever approach is taken, the provisioning process can be expensive, repetitive, inconvenient, and time consuming when it is necessary to be sure a person is who they say they are.

Sometimes a person, whether acting as an individual or as a representative of an organization, has to undertake identity authentication processes requiring authentication of Evidence of Identity on many occasions to meet similar requirements for different purposes. This Standard specifies requirements for organizations to share authenticated knowledge about a person's identity for the purpose of provisioning electronic access to services and facilities. These requirements potentially minimize the inconvenience and cost of provisioning electronic access while protecting the privacy of the people involved.

This Standard makes no assumptions about the relationship between the person with electronic access capabilities and the organizations that provide the services and facilities that are accessed; for example, users may be employees, customers, or have some other type of relationship with the service or facility provider.

This Standard does not assume or prescribe any particular technologies for the implementation of systems to authenticate a person's identity. Thus, for example, this Standard could be used in association with systems that use static passwords, one-time pass-codes, Public Key Infrastructure (PKI), and/or biometric authentication techniques.

STANDARDS AUSTRALIA

Australian Standard

Knowledge-based identity authentication—Recognizing Known Customers

1 SCOPE, OBJECTIVE AND APPLICATION

1.1 Scope

This Standard specifies requirements for using pre-existing, authenticated knowledge about a person's identity held by one organization to streamline provisioning of electronic access to services and facilities by other organizations. These requirements relate to the access control lifecycle model specified in Appendix A.

This Standard provides an alternative to repeating identity authentication checks requiring authentication of Evidence of Identity when applying for access to electronic services where it is possible to rely on authentication of Evidence of Identity performed at an earlier time.

The following are excluded from the scope of this Standard.

(a) System-to-system access where a person is not associated with each instance of electronic access.

(b) Determination of those identity attributes that are necessary to identify a Customer.

(c) Syntax for identity attributes.

(d) Telecommunications protocols for interactions between Customers, Known Customer Organizations, and other Relying Parties.

(e) Requirements for Evidence of Identity and authentication of Evidence of Identity.

(f) Criteria concerning whether or not a relationship history is satisfactory.

(g) The choice of type of identity authentication credential.

(h) Requirements for management of identity authentication credentials (including issue, re-issue, change).

(i) Criteria for a Relying Party to decide whether or not identity information held by a Known Customer Organization and identity authentication credentials assigned by a Known Customer Organization meet their needs.

(j) Operations in Relying Parties concerning a Customer's access that take place after completion of access provisioning.

(k) Other services that Known Customer Organizations may provide to Relying Parties.

(l) Requirements for certification of compliance with the requirements of this Standard.

(m) Requirements for accreditation of Known Customer Organizations to provide the services specified in this standard.

(n) Procedures to be followed to report fraud or suspected fraud.

1.2 Objective

The objective of this Standard is to provide a convenient and cost-efficient way for people to apply on-line for electronic access to services and facilities when another trusted organization has previously authenticated their identity and assigned identity authentication credentials to them.