AS 5185—2010

Australian Standard®

Protocol for Lightweight Authentication of IDentity (PLAID)

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 8 September 2010.
This Standard was published on 14 October 2010.

The following are represented on Committee IT-012:

- Attorney General's Department
- Australia Post
- Australian Association of Permanent Building Societies
- Australian Government Information Management Office (AGIMO)
- Australian Industry Group
- Australian Information Industry Association
- Australian Payments Clearing Association
- Council of Small Business Organisations of Australia
- New Zealand Defence Force
- Reserve Bank of Australia

Additional Interests:

- Australian Computer Society
- Centrelink
- Lockstep
- Queensland Transport

This Standard was issued in draft form for comment as DR AS 5185.

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 the 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Standards may also be withdrawn.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®

Protocol for Lightweight Authentication of IDentity (PLAID)

First published as AS 5185—2010.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 0 7337 9690 6

PREFACE

This Standard was prepared by a working group of Australian members from the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, 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.

INTELLECTUAL PROPERTY

Standards Australia draws attention to the fact that it is claimed that compliance with this document may involve the use of intellectual property concerning PLAID.

Standards Australia takes no position concerning the evidence, validity and scope of such an intellectual property right.

The holder of the right has assured Standards Australia that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect the licence provided is perpetual, irrevocable, world-wide, non-exclusive, royalty free and no-charge. The statement of the holder of this intellectual property right is registered with Standards Australia. Information may be obtained from:

Commonwealth of Australia acting through the Commonwealth Services Delivery Agency also known as 'Centrelink' or such other agency as may from time to time, administer the PLAID Licence on behalf of the Commonwealth of Australia. Contact details are as follows:

Attn: Centrelink PLAID
PO Box 7788
Canberra M.C. ACT 2910

Email: PLAID@centrelink.gov.au
Licence: https://www.plaid.gov.au

Attention is drawn to the possibility that some of the elements of this document may be the subject of intellectual property rights other than those identified above. Standards Australia shall not be held responsible for identifying any or all such rights.

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 wishes to thank Centrelink for their financial support in helping to develop this Standard.

CONTENTS

Page

FOREWORD

PLAID (Protocol for Lightweight Authentication of IDentity) is an ICC (smartcard) authentication protocol, which is cryptographically strong, fast and private and designed to expressly support contactless applications. The protocol is designed to fill the gap in standardized protocols between existing tag and RFID based technologies which do not utilize cryptography but are fast, and PKI based authentication, which can be very strong cryptographically, but slower, and unsuitable for many contactless use-cases.

It is based on a cryptographic and algorithmic method, which uses both symmetric and asymmetric cryptography in a unique hybrid protocol to protect the communications between ICCs and terminal devices. This is done in such a way that strong authentication of the ICC and credentials on it is possible in a fast and highly secure fashion without the exposure of card or cardholder identifying information or any other information which is useful to an attacker.

The protocol is designed to perform a high strength mutual authentication in less than 300 milliseconds (0.3 of a second) using off-the-shelf PICCs/ICCs, making it suitable for a range of mission critical contactless applications.

PLAID uses standards-based cryptography commonly available on most programmable ICCs, computer systems and embedded devices and is consequently highly portable to a wide range of existing cards and devices.

Support is provided for either single or dual factor authentication, including support for authentication of the ICC, the access control system record and (optionally) the cardholder's PIN or biometric template.

Prior to publication of this Standard, there were no standardized and non-proprietary ICC specific authentication protocols designed for 'tap-n-go' use-cases using ISO/IEC 14443 and ISO/IEC 7816 capable ICCs.

The majority of unattended physical access systems utilize contactless technologies, which fit the following two classes of protocol/ciphers:

(a) Active tag, RFID and ISO/IEC 14443 series UID-based protocols which respond with a fixed and theoretically unique number using an unsecured protocol. This class of protocols, where the unique identifier is not cryptographically protected, and is available in the clear, are subject to simple clone or replay attacks. Attacks of this kind may be mounted using off-the shelf devices.

(b) ISO/IEC 14443 series standards-based protocols and ciphers using a proprietary authentication protocol and/or cryptographic cipher. Significant weaknesses have been demonstrated in mainstream proprietary ciphers and proprietary authentication protocols which have been exposed in recent years including algebraic attack of the cipher.

The need for a strong standardized and non-proprietary authentication protocol using standardized ciphers has become urgent in the Physical Access Control Systems (PACS) sector, where significant elements of Australian national infrastructure are currently exposed.

PLAID includes all necessary components required for it to be a capable replacement for the class of technologies (a) and (b) above for PACS and LACS implementation on ICCs meeting ISO/IEC 14443 and ISO/IEC 7816. It provides for strong authentication of both the ICC and credential data secured by the ICC in a highly secure fashion without the exposure of ICC or cardholder identifying information or any other private information which is useful to an attacker.

STANDARDS AUSTRALIA

Australian Standard
Protocol for Lightweight Authentication of IDentity (PLAID)

1 SCOPE

This Standard sets out an authentication protocol suitable for use in physical and logical access control systems based on ICCs and related systems which support the standards based AES, RSA and SHA ciphers.

This Standard specifies PLAID and its implementation in sufficient detail to allow any two or more implementations to be interoperable. It does not address how implementations share cryptographic keys, access control system credential record structures and biometric template formats.

NOTES:

1 Appendix A provides information for implementers on Test Vectors.

2 Appendices B to J provide informative commentary for implementers and will assist developers, architects and security evaluators.

(a) Appendix B: Implementation under ISO/IEC 24727.

(b) Appendix C: Reference implementation.

(c) Appendix D: Functional specification.

(d) Appendix E: ID-Leakage considerations.

(e) Appendix F: Suggested key lengths and algorithms.

(f) Appendix G: Keyset management.

(g) Appendix H: Operational mode management.

(h) Appendix I: PLAID security features.

(i) Appendix J: Comparison of PLAID to ISO/IEC 9798 authentication mechanisms.

2 OBJECTIVES OF PLAID

PLAID addresses the following objectives, and should—

(a) be broadly suitable for PACS and LACS use-cases using COTS products;

(b) be available as intellectual property without discrimination under a perpetual, irrevocable, worldwide, non-exclusive, royalty free and no-charge licence;

(c) support PACS tap-n-go speed requirements using COTS ICCs (see Appendix F for details);

(d) support interface neutrality for contact or contactless usage;

(e) support standardized cryptographic ciphers commonly deployed on ICC and IFD devices and available in the public domain;

(f) not expose any individually identifiable, unique or determinable data or characteristic of the ICC or cardholder during authentication;

(g) not expose private data in the clear at any interface;

(h) not generate or utilize any repeatable data that could allow another ICC, or ICC emulator, to successfully frame a replay attack;

(i) not be symmetric in protocol architecture so as to protect from reflection attacks;