

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Standards may also be withdrawn.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.

COPYRIGHT

© Standards Australia Limited

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968.

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

	<i>Page</i>
FOREWORD.....	4
1 SCOPE.....	5
2 OBJECTIVES OF PLAID.....	5
3 REFERENCED DOCUMENTS.....	6
4 TERMS AND DEFINITIONS	6
5 SYMBOLS (AND ABBREVIATED TERMS)	7
6 DATA DICTIONARY	8
7 AUTHENTICATION PROTOCOL DESCRIPTION	10
8 APPLICATION IDENTIFICATION	14
9 COMMAND SET	14
10 ERROR CODES (STATUS WORDS).....	15
11 KEY DIVERSIFICATION	15
12 SESSION KEY GENERATION	15
13 DEFAULT MODES.....	16
APPENDICES	
A TEST VECTORS.....	17
B IMPLEMENTATION UNDER ISO/IEC 24727	20
C REFERENCE IMPLEMENTATION.....	22
D FUNCTIONAL SPECIFICATION	23
E ID-LEAKAGE CONSIDERATIONS	24
F SUGGESTED KEY LENGTHS AND ALGORITHMS.....	25
G KEYSSET MANAGEMENT.....	26
H OPERATIONAL MODE MANAGEMENT	27
I PLAID SECURITY FEATURES.....	28
J COMPARISON OF PLAID TO ISO/IEC 9798 AUTHENTICATION MECHANISMS.....	31

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 protocols/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 detail);
- (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;

- (j) support countermeasures to ensure any device or devices inserting themselves in the middle of any session between the ICC and IFD cannot modify any session data without detection;
- (k) provide the ICC's PIN to the IFD only after completion of a mutual authentication and only in a hash form for comparison to an IFD generated PIN hash;
- (l) support a secure one-time session key negotiated between the ICC and IFD and suitable for subsequent secure session or secure messaging protocols;
- (m) support negotiation of multiple keysets such that keys may be allocated by purpose;
- (n) support spare unused keysets for planned or emergency key roll operations; and
- (o) support the authentication of different credential payloads to allow extensibility of the requirements of the IFD and schemes.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

ISO/IEC

- 7816 Identification cards—Integrated circuit cards
- 7816-3 Part 3: Cards with contacts—Electrical interface and transmission protocols
- 7816-4 Part 4: Organization, security and commands for interchange
- 7816-5 Part 5: Registration of application providers
- 8824 Information Technology—Abstract Syntax Notation One (ASN.1)
- 8824-1 Part 1: Specification of basic notation
- 9798 Information technology—Security techniques—Entity authentication
- 9798-2 Part 2: Mechanisms using symmetric encipherment algorithms
- 14443 Identification cards—Contactless integrated circuit cards—Proximity cards (all parts)
- 24727 Identification cards—Integrated circuit card programming interfaces
- 24727-3 Part 3: Application interface
- 24727-6 Part 6: Registration authority [to be published]

FIPS

- 197 AES Advanced Encryption Standard (AES)
- 180-1 Secure Hash Standard

ITU-T

- X.680 OSI Networking and System Aspects—Abstract Syntax Notation One

4 TERMS AND DEFINITIONS

For the purposes of this document, the following terms and definitions, apply.

4.1 Cardholder

The person to whom a PLAID capable ICC is issued and whose identity is the target of PLAID.

4.2 Clone

An exact digital copy of an existing ICC, RFID or tag, which is logically indistinguishable from the original by an IFD.

4.3 ID-Leakage

A constant subset of data that is static for each authentication exchange between a specific ICC and IFD.

NOTE: This subset (even when encrypted) could allow for identification of an individual ICC, and therefore indirectly the cardholder.

4.4 Issuer

The entity, system or role that issues a PLAID capable ICC and owns the PLAID keys.

4.5 Man-in-the-middle attack

An attack where an active emulator or similar device or devices insert themselves in the session between the real ICC and the IFD and maliciously modify data within the session in such a fashion that neither the ICC nor IFD detect the modified session.

4.6 Reflection attack

An attack where a host can be fooled into accepting a challenge as valid, where the challenge was previously generated by the host in a previous authentication.

4.7 Replay attack

An attack in which a valid data transmission from an ICC is able to be repeated by a different ICC or by an ICC emulator and appear to be an authentic session as viewed from an IFD.

5 SYMBOLS (AND ABBREVIATED TERMS)

For the purposes of this Standard, the following symbols and abbreviated terms apply.

	Logical concatenation of bit strings (Pipe)
AES	Advanced Encryption Standard (as defined in FIPS-197)
AID	Application IDentifier (as defined in ISO/IEC 7816 Part 4 and registered under Part 5)
AP	Authentication Protocol (as defined in ISO/IEC 24727-3)
APDU	Application Protocol Data Unit (as defined in ISO/IEC 7816-4)
ASN.1	Abstract Syntax Notation Number 1 (as defined in ISO/IEC 8824-1 and ITU-T X.680)
CBC	Cipher Block Chaining
CRT	Chinese Remainder Theorem
DivData	Diversification Data—Salt data used in cryptographic operations
DER	Distinguished Encoding Rules (as defined in ITU-T X.680)
DOS	Denial Of Service (attack)
ECB	Electronic Code Book
FA	Final Authenticate
IA	Initial Authenticate
ICC	Integrated Circuit Card, logically equivalent in this standard to PICC
IFD	InterFace Device
KeySetID	A 2 byte value specifying which Keyset the protocol will negotiate or use
LACS	Logical Access Control System

OAEP	Optimal Asymmetric Padding Scheme
OID	Object Identifier
OpModeID	A 2 byte value specifying which operational mode the protocol will use
PACS	Physical Access Control System
PICC	Proximity Integrated Circuit Card, logically equivalent in this standard to ICC
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PLAID	Protocol for Lightweight Authentication of IDentity
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir and Adleman Asymmetric cryptographic algorithm
SHA	Secure Hash Algorithm (as defined in FIPS 180-1)
SW	Status Word

6 DATA DICTIONARY

Table 1 sets out the size and details of PLAID data objects.

TABLE 1
DATA DICTIONARY

Object name	Purpose	Size, bytes	Data type	Comments
ACSRecord	Access control system record	Variable	Alpha-Numeric	An access control system record for each supported Operational Mode Identifier for the purpose of authorization by back office PACS or LACS access control systems. This record is mapped by the OpModeID to the particular back office numbering system the protocol is supporting. This record is returned by the final authenticate command response.
DivData	Symmetric key diversification data	8	Binary	A number (or salt) which is set at PLAID instantiation for use in the key diversification algorithm to ensure that loss of an individual card symmetric key cannot result in a breach of the system master keys. This salt is determined by the issuer and should preferably be both random and unique per PLAID invocation AND per system.
FAKey	Undiversified final authenticate key (AES)	16/24/32	Binary	An instance of a final authenticate key that is yet to be diversified against an ICC's diversification data. (See Note).
FAKey(DIV)	Diversified final authenticate key (AES)	16/24/32	Binary	An instance of a final authenticate key that has been diversified against an ICC's diversification data. The initialization vector (IV) shall be set to an array of zeros.

TABLE 1 (continued)

Object name	Purpose	Size, bytes	Data type	Comments
KeySetID	Uniquely identify a keyset	2	Binary	One or more two byte identifiers sent in a list to the ICC in the initial authenticate command so as to determine and/or negotiate the keyset to be used for authentication.
Minutiae	Fingerprint minutiae data stored on-card	Variable	Binary	Minutiae template is extracted as raw data and evaluated off-card by the IFD.
OpModeID	Operating mode identifier	2	Binary	An identifier sent to the ICC in the final authenticate command that determines which ACSRecord is served up in the final authentication response from the ICC.
PIN	PIN	Variable	Alpha-Numeric	The PIN Global to the ICC.
PINHash	PIN hash	20	Binary	The SHA1 hash value of the PIN which is served up in the final authentication response from the ICC.
RND1	Random number one	16/24/32	Binary	Random number generated by the ICC using its RNG.
RND2	Random number two	16/24/32	Binary	Random number generated by the IFD or back office system using a RNG.
RND3	Random number three	16/24/32	Binary	String generated by the IFD and ICC separately calculating SHA[RND1 RND2]
SecureICC	Secure the ICC	1	Binary	Flag to hold initial state of the PLAID application 0 = unsecured 1 = secured.
SessionKey	Session key	16/24/32	Binary	String generated by the IFD and ICC separately calculating RND3.
ShillKey	Shill key (RSA/AES)	Varies	Binary	A Shill key is randomly generated by the ICC during PLAID instantiation but is only known to the ICC. A shill key is generated for both the initial authenticate (RSA) and the final authenticate (AES) commands. Shill key is used by the ICC in place of the actual key when an inconsistency is detected, thereby removing any indication to a potential attacker that an inconsistency has been detected.
VersionNo	Version number	1	Binary	Implementation version number, starting at zero and incrementing by one for each release.

NOTE: FAKey is never used in its undiversified form for cryptographic operations therefore initialization vectors are not required.

7 AUTHENTICATION PROTOCOL DESCRIPTION

This clause sets out the steps involved in the PLAID mutual authentication involving a PACS or LACS use-case. Figure 1 illustrates this process.

The steps required to carry out a mutual authenticate using PLAID shall be as follows:

(a) *IA Command* [Step 1]

The IFD sends an Initial Authentication APDU request to the ICC in order to obtain the Diversification Data (DivData). The body of the APDU contains the complete list of authorized KeySetIDs (DER encoded) that will be acknowledged by the IFD. This list should be ordered with the preferred KeySetID first, followed by lesser preferred KeySetIDs.

NOTES:

- 1 DER encoding is only used in the body of the Initial Authenticate command as all other transactions are encrypted.
- 2 The formal ASN.1 representation of the IA command is:
 - >> PLAID – {iso(1) member-body (2) au (36) AS5185(5185)PLAID(1)}
 - >> Definitions Implicit Tags:
 - >> BEGIN
 - >> KeySetID: OCTET STRING (Size 2)
 - >> KeySetIDSequence: Sequence of KeySetID
 - >> END

(b) *IA Command Evaluation* [Step 2]

- (i) The ICC parses the DER listing of KeySetIDs and retrieves the first IAKey found which matches a KeySetID supported by the ICC.
- (ii) If none of the KeySetIDs identified match a key stored by the ICC then the ICC responds using a random byte string encrypted with the ShillKey, thereby preventing any indication that an error has occurred.

(c) *IA Response* [Step 3]

- (i) The ICC generates a random value (RND1) using a RNG. The size of RND1 is identical to the key size of the selected AES cipher (16, 24 or 32 bytes).
- (ii) The ICC retrieves the unique diversification data DivData.
- (iii) The ICC creates the bit string STR1: KeySetID || DivData || RND1 || RND1.
- (iv) The ICC computes the bit string ESTR1 where $ESTR1 = \text{RSA}_{\text{Encrypt}}^{\text{IAKey}}(\text{STR1})$. This encryption only uses the modulus and public exponent of the IAKey. Padding (PKCS1.5) should be incorporated into the encryption.
- (v) The ICC transmits the ESTR1 string to the IFD.

(d) *IA Response Evaluation* [Step 4]

- (i) The IFD calculates STR1 where $\text{STR1} = \text{RSA}_{\text{Decrypt}}^{\text{IAKey}}(\text{ESTR1})$, using the first KeySetID identified in the list. The IFD compares the two copies of RND1 to confirm that decryption was successful. If the decryption was unsuccessful then the IFD attempts decryption using the next KeySetID identified in the list. This continues until the decryption is successful or until all available KeySetIDs have been attempted. Authentication fails if all KeySetIDs have been used and decryption fails.

- (ii) The IFD extracts the KeySetID from STR1 to confirm which Keyset is being used.
NOTE: This is necessary since the same Asymmetric keys might be used in multiple KeySetIDs for large implementations.
- (iii) The IFD extracts the ICC diversification seed data DivData from STR1.
- (e) *FA Command* [Step 5]
 - (i) The IFD generates a random value (RND2) using a RNG. The size of RND2 is identical to the key size of the selected AES cipher (16, 24 or 32 bytes).
 - (ii) The IFD calculates SHA [RND1||RND2]; the result is denoted as RND3.
 - (iii) The IFD uses the diversification data (DivData) and calculates the diversified final authenticate key where $FAKey(Div) = AES_{Encrypt}^{FAKey}(DivData)$. The FAKey to be used is referenced by the KeySetID identified as successful in the IA Response evaluation.
 - (iv) The IFD creates the bit string STR1: OpModeID || RND2 || RND3.
 - (v) The IFD calculates ESTR2 where $ESTR2 = AES_{Encrypt}^{FAKey(Div)}(STR2)$. The cipher mode for this operation must be CBC.
 - (vi) The IFD transmits the Final Authenticate string ESTR2 to the ICC.
- (f) *FA Command Evaluation* [Step 6]
 - (i) The ICC calculates STR2 where $STR2 = AES_{Decrypt}^{FAKey(Div)}(ESTR2)$. The FAKey (Div) to be used is referenced by the KeySetID used in the IA Response.
 - (ii) The ICC calculates RND3 as SHA [RND1||RND2] using RND1 generated in the FA Command step and RND2 extracted from STR2.
 - (iii) The ICC compares RND3 above with the RND3 extracted from STR2. If a mismatch occurs then the ICC responds using a random byte string encrypted with the ShillKey, thereby preventing any indication that an error has occurred.
- (g) *FA Command Response* [Step 7]
 - (i) The ICC retrieves the appropriate fields, based on the OpModeID extracted from STR2.
 - (ii) The ICC creates the bit string STR3: DivData || ACSRecord || (Null, PINHash and/or minutiae).
 - (iii) The ICC calculates ESTR3 where $ESTR3 = AES_{Encrypt}^{RND3}(STR3)$. The cipher mode for this operation must be CBC.
 - (iv) The ICC transmits the Final Authenticate string ESTR3 to the IFD.
- (h) *FA Response Evaluation* [Step 8]
 - (i) The IFD calculates STR3 where $STR3 = AES_{Decrypt}^{RND3}(ESTR3)$.
 - (ii) The IFD compares the transmitted DivData with the IFD copy received in the IA Response. Authentication fails if they do not match.
 - (iii) If PIN authentication is required then the IFD will have the cardholders PINHash in STR3 and compares a SHA hash of the PIN from the cardholder with the SHA PINHash retrieved from STR3. Authentication fails if they do not match.