

Centrelink

Protocol for Lightweight Authentication of Identity (PLAID)

LOGICAL SMARTCARD APPLICATION SPECIFICATION PLAID Version 7.1

February 2009

Further information

Comments and requests for further information may be emailed to plaid@centrelink.gov.au

TABLE OF CONTENTS

1. Introduction.....	5
2. PLAID Authentication Protocol.....	6
3. Copyright.....	8
4. Software Licensing Terms (Licence).....	8
4.1 Licence.....	8
4.2 Intellectual Property Rights.....	9
4.3 Disclaimer.....	10
4.4 Indemnity.....	10
4.5 Assignment and Novation.....	10
4.6 Costs.....	10
4.7 Miscellaneous.....	10
4.8 Definitions and interpretation.....	11
5. Scope.....	12
6. Normative References.....	12
7. Terms and Definitions.....	13
8. Symbols (and Abbreviated Terms).....	14
9. Revisions History.....	15
10. Purpose.....	18
11. Data Dictionary.....	19
12. Authentication Protocol Description.....	21
13. Operational Modes and Key Sets.....	24
14. Application Identification.....	25
15. Command Set.....	25
16. Error Codes (Status Words).....	26
17. Key Diversification.....	27
18. Session Key Generation.....	27
19. Access Control System Record.....	27

Annex A:	Reference Implementation (Informative)	28
Annex B:	Functional Specification (Informative)	29
Annex C:	ID-Leakage Considerations (Informative)	31
Annex D:	Suggested Key Lengths and Algorithms (Informative).....	32

1. INTRODUCTION

PLAID (Protocol for Light weight Authentication of ID) is a smartcard authentication protocol developed by Centrelink, which is cryptographically stronger, faster and more private for contactless applications than most or all equivalent protocols currently available either commercially or via existing standards.

There are significant advantages in efficiency and reduction in costs if a common, non-proprietary and standardised protocol of this type is available across common software, readers, building, key and card management systems particularly should multiple agencies or governments and their vendors support the same protocol.

Centrelink, an Australian Government Statutory Agency, has a consequent strategic interest in obtaining commercial off the shelf (COTS) product using PLAID.

Since Centrelink obtains the greatest advantage by the broadest use of PLAID, Centrelink chooses to license the intellectual property developed by Centrelink to other agencies, government and commercial organisations on an open, free and non-discriminatory basis, and to propose it as a component of forward formal standards.

In order to facilitate the above, Centrelink has structured a program to;

- Have PLAID evaluated by both respected cryptographic organisations, as well as the broader cryptographic community.
- Generate interest and co-operation, from government agencies worldwide.
- Develop, propose, socialise, agree and implement standardisation strategies in consultation with these agencies and industry.
- Manage vendor access, feedback and licensing to ensure equality of access of PLAID intellectual property to all vendors and end-users that chose to support the protocol.
- Ensure Intellectual Property (IP) is not lost, diluted or accidentally transferred to any single party, and is available to all potential user communities under reasonable, non-discriminatory and free licensing arrangements.
- Encourage governments, their agencies, commercial end-users and vendors to implement PLAID within COTS product with the intention of using the scale of these implementations to drive down the cost and increase the availability of fit-for-purpose COTS product to all.

This specification forms an initial step in the standardisation strategy. It provides any interested party with a formal, stabilised and tested version of PLAID (Version 7) which has both been reviewed by respected cryptographic organisations and has been load tested on a significant range of smartcards and devices over a two year period.

This version incorporates various enhancements in response to issues identified by the Australian Defence Signals Directorate (DSD) and the US National Institute of Standards and Technology (NIST) as well as the internal Centrelink team.

This is the first version of PLAID to include a production licence which allows the re-distribution of PLAID IP without restriction and without the possibility of licence condition alteration. As such, manufacturers may choose to incorporate PLAID into their product offerings at no cost from this release.

2. PLAID AUTHENTICATION PROTOCOL

PLAID is a cryptographic and algorithmic method and associated source code which uses symmetric and/or asymmetric cryptography in a unique protocol to protect the communications between smartcard and terminal devices in such a way that strong authentication of objects on the smartcard 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 PLAID protocol uses standards based cryptography commonly available on most programmable smartcards, computer systems and embedded devices and is consequently highly portable to existing cards and devices.

The PLAID protocol is optimised for a fast mutual authentication between the smartcard and devices or middleware using either contact or contactless smartcard implementations. In optimal configurations, with high end cards and optimised environments, total transaction speeds range between 200 and 300 milliseconds (0.2-0.3 seconds). Slightly longer times are experienced when working with large access control objects such as biometric templates.

PLAID is highly resilient to the following threats:

- ID-leakage - the leakage of individually identifiable, unique or determinable data or characteristic of the smartcard or card holder during authentication.
- Private-data-leakage - availability of private data in the clear at interfaces accessible by other than the data owner or appropriately authorised parties.

- Replay attack - an attack in which a valid data transmission from a smartcard is able to be repeated by a different smartcard or by a smartcard emulator and appear to be an authentic session.
- Man-in-the-middle attack - an attack where an active emulator or similar device or devices insert themselves in the session between the real smartcard and the reader and maliciously modify data within the session in such a fashion that neither the smartcard nor reader detect the modified session.

PLAID supports either single or dual factor authentication, with support for authentication of the smartcard, the access control system record and (optionally) the cardholders PIN or biometric template.

PLAID version 7 supports the following additional features;

- Multiple key sets (255). Different keys may be used by purpose (i.e., perimeter, logical access, computer room and administrative key sets) and maintenance of keys is possible by rolling onto a spare un-used key set already stored on the smartcard.
- Multiple access control system records authenticated by purpose (255). Depending on the record required by the reader, the protocol will provide an authenticated record of just the type required for the particular environment. These records could for example be all of; a Weigand number; a US Federal FASC-N staff number; a FIPS 201 CHUID or Centrelink CSIC record; an ISO/IEC 7812 card number; a biometric template or any other numbering system required by the environment.
- A 256 bit AES session key is provided for the next smartcard operation. PLAID may be used as a bootstrap protocol to set up the card with a secure session to support subsequent higher level protocols or operations. This might for example be used to protect a public certificate accessed in the next operation from exposure of its otherwise publically available attributes.
- A usage counter is maintained by the card for analysis of successful authentications and comparison to back-office data in order to assist in identification of attempted attacks.
- A failed attempt counter is maintained by the smartcard for its analysis of failed authentications and to shut access to the application down in the instance of multiple failed authentications.

3. COPYRIGHT

No part of PLAID or its source code may be reproduced, digitised, stored in a retrieval system, communicated to the public or caused to be seen or heard in public, made publicly available or publicly performed, offered for sale or hire or exhibited by way of trade in public or distributed by way of trade in any form or by any means, electronic, mechanical or otherwise without either the written permission of the Commonwealth represented by the Commonwealth Service Delivery Agency (Centrelink) or as **licensed under the Software Licence Terms below.**

4. SOFTWARE LICENSING TERMS (LICENCE)

The Protocol for Lightweight Authentication of ID (PLAID) described in this document is a cryptographic and algorithmic method and associated source code which uses symmetric and/or asymmetric cryptography in a unique protocol to protect the communications between smartcard and terminal devices in such a way that strong authentication of objects on the smartcard 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.

This Licence takes effect on and from the date the User first uses; accesses; downloads; reproduces; or otherwise deals with PLAID and/or its source code.

The User acknowledges and agrees that having access to PLAID and its source code is valuable to the User and in consideration for the 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 this Licence on behalf of the Commonwealth of Australia) providing PLAID to the User on the terms of this Licence, the User accepts and agrees to be bound by its terms.

The User acknowledges that any act of accessing, downloading, copying or using, PLAID and/or its source code will each bind the User to the terms of this Licence.

4.1 Licence

Subject to the terms of this Licence, the Commonwealth of Australia grants to the User a perpetual, irrevocable, world-wide, non-exclusive, royalty free and no-charge licence to use, reproduce, communicate, sub-license and distribute PLAID and/or its source code. The licence in this clause includes the right to incorporate PLAID into any Product developed by the User.

The User must, when reproducing or communicating PLAID and/or its source code, ensure that the following words (or words to the same effect) appear concurrently with PLAID and/or its source code, or any reproduction in a material form of PLAID or any part of it, or as part of any licence for any Product which incorporates or uses PLAID:

“All intellectual property rights in the Protocol for Lightweight Authentication of ID (PLAID) and/or its source code are owned by the Commonwealth of Australia. PLAID and/or its source code is used, copied, accessed, downloaded or reproduced by [insert name of User] under licence from the Commonwealth of Australia. The licence provided is perpetual, irrevocable, world-wide, non-exclusive, royalty free and no-charge, but all users of PLAID, its source code or any product using or incorporating these must include this statement in any reproduction of PLAID or its source code or any product using or incorporating PLAID. Use of this item is at the user's own risk, and the Commonwealth of Australia makes no warranties or representations about PLAID and/or its source code and/or any product using or incorporating the same, including about their quality or fitness for purpose.”

4.2 Intellectual Property Rights

The Intellectual Property Rights in PLAID and its source code remain the exclusive property of the Commonwealth of Australia.

This Licence does not include or constitute any Moral Rights consent or waiver. The User must not commit any act which constitutes a breach of an author's Moral Rights in respect the Intellectual Property Rights except where that author has given a Moral Rights consent that meets the requirements of the Copyright Act 1968 (Cth) or without the Commonwealth of Australia's written approval.

The User:

must obtain any third party consents necessary in relation to this Licence; and
warrants that it will not in exercising its rights under this Licence infringe the Intellectual Property Rights of any third parties.

4.3 Disclaimer

The Commonwealth of Australia provides no warranty and accepts no responsibility in respect of PLAID and/or its source code or the Intellectual Property Rights that it licenses in this Licence. The Commonwealth of Australia provides PLAID and/or its source code on an "as is" basis, without warranties or conditions of any kind, either express or implied, including without limitation any warranties or conditions of title, non-infringement, merchantability or fitness for a particular purpose. The User agrees that it is solely responsible for determining the appropriateness of using or redistributing PLAID and/or its source code and assume any risks associated with the exercise of the permissions under this Licence.

The User agrees that the Commonwealth of Australia is not liable for any direct, indirect, incidental, special or consequential damages, or damages for loss of profits, revenue, data or use, incurred by it or any third party as a result of its use of PLAID and/or its source code.

4.4 Indemnity

In no event and under no legal theory, whether in tort (including negligence), contract or otherwise, unless required by applicable law or as agreed to in writing, will the Commonwealth of Australia be liable to the User for damages, including any direct, indirect, special, incidental or consequential damage of any character arising as a result of this Licence or out of the use or inability to use PLAID or its source code, even if the Commonwealth of Australia has been advised of the possibility of such damages.

The User agrees to permanently indemnify the Commonwealth of Australia from and against any and all claims, liabilities, damages, losses or expenses and costs in respect of the User's use of PLAID and/or its source code.

4.5 Assignment and Novation

The User must not transfer, assign or novate its rights under this Licence.

4.6 Costs

The User must pay its own costs in relation to this Licence and any document related to this Licence.

4.7 Miscellaneous

The Commonwealth of Australia can modify the terms of this Licence at any time, by posting a notice and a copy of the new Licence terms on its website, but the Commonwealth of Australia may not change the perpetual, irrevocable, world-wide, non-exclusive, royalty free and no-charge nature of the licence granted to the User, or the User's right to use, reproduce, communicate, sub-license and distribute PLAID and/or its source code under the Licence.

This Licence contains everything the parties have agreed in relation to the matters it deals with.
This Licence is governed by the law of Australian Capital Territory, Australia.

4.8 Definitions and interpretation

In this Licence capitalised terms have the meaning specified in this clause.

Licence means these terms and conditions including the licence granted under the Licence.

Intellectual Property Rights means any and all copyrights, patents, patent applications, trademarks, service marks, trade names, registered designs, unregistered design rights, copyright, know how, trade secrets, domain names, internet addresses, rights in confidential information, and all and any other intellectual property rights, whether registered or unregistered, and including all applications and rights to apply for any of the same, now or in the future.

Moral Rights means rights of integrity of authorship, rights of attribution of authorship, rights not to have authorship falsely attributed, and rights of a similar nature conferred by statute that exist, or may come to exist, anywhere in the world.

Product means any product or other material developed by or on behalf of the User, including any software, hardware or design, and whether or not intended for commercial distribution.

User means the entity that accesses, uses, reproduces, downloads or otherwise deals with PLAID.

5. SCOPE

The scope of this document is to describe the PLAID authentication protocol in sufficient detail to allow any two or more implementations to be interoperable given that the implementations independently agree on the PLAID keys used and the values of keys, as well as the ACS record structures and any biometric template formats supported.

This document does not address key management, record structures or biometric templates as these are logically described in other standards or specifications or should be determined by implementers.

Further to this scope, and to assist in interoperability, a reference implementation is available to support this document. This implementation is coded in Java Card for the ICC and C for the IFD and is freely available from the Commonwealth of Australia via Centrelink as both source and objects code under the same licence applicable to this document and set out in section 4.

6. NORMATIVE REFERENCES

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- ISO/IEC 7816 Parts 3, 4, Identification cards – Integrated circuit cards
- ISO/IEC 14443 (all parts), Information technology – Identification cards - Contactless integrated circuit(s) cards - Proximity cards
- ISO/IEC 18033 (all parts), Information technology – Security techniques – Encryption algorithms
- FIPS 197 AES - Announcing the Advanced Encryption Standard
- FIPS 180 SHA - Introducing the Secure Hash Standard

7. TERMS AND DEFINITIONS

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

7.1 ACS record (ACSrecord)

A unique record per Card Holder and Operational Mode that is authenticated by the PLAID AP for the purpose of PACS or LACS access.

7.2 Card Holder

The person to whom a PLAID capable smartcard is issued by the Issuer and whose identity is the target of the PLAID Authentication Protocol.

7.3 Diversification Data (DivDat)

A number which the Issuer sets that is unique per smartcard for use by the key diversification algorithm to ensure that breach of an individual card symmetric key cannot result in a breach of the systems master keys.

7.4 Issuer

The entity, system or role which issues a PLAID capable smartcard and owns the PLAID keys.

7.5 ID-Leakage

A constant subset of data that is static for each authentication exchange between a specific ICC and an IFD. This subset (even when encrypted) could allow for identification of an individual smartcard, and therefore indirectly the cardholder. This attribute can be a superset of private-data-leakage.

7.6 Keyset Identifier (KeySetID)

An identifier which uniquely identifies a key set.

7.7 LACS record

Logical access control system record, see ACS record.

7.8 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.

7.9 Operational mode identifier (OpModeID)

An identifier sent to the ICC in the in the P1 parameter of the Initial Authenticate command that determines which PACS/LACS record type is served up by the final authentication step.

7.10 PACS record

Physical access control system record, see ACS record.

7.11 Private-data-leakage

The availability of private data in the clear at interfaces accessible by other than the data owner or appropriately authorised parties. This attribute is a subset of ID-Leakage.

7.12 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.

8. SYMBOLS (AND ABBREVIATED TERMS)

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

	logical concatenation of bit strings (Pipe)
⊕	logical exclusive or operator (XOR)
AES	advanced encryption standard (as defined in FIPS-197)
AID	application identifier
AP	authentication protocol
APDU	application protocol data unit
COTS	commercial off the shelf
CRT	Chinese remainder theorem
DivDat	diversification data
ECB	electronic code book
FA	final authenticate
IA	initial authenticate

ICC	integrated circuit card, logically equivalent in this specification to PICC
IFD	interface device
KeySetID	number specifying which key set the protocol will use
LACS	logical access control system
OID	object identifier
OpModeID	number specifying which operations mode the protocol will use
PACS	physical access control system
PICC	proximity integrated circuit card, logically equivalent in this specification to ICC
PIN	personal identification number
PKCS	public key cryptography standards
PLAID	protocol for lightweight authentication of identity
ROM	read only memory
RSA	Rivest, Shamir and Adleman asymmetric cryptographic algorithm
SHA	secure hash algorithm (as defined in FIPS-180)
SW	status word
TRNG	true random number generator

9. REVISIONS HISTORY

PLAID version 7.1 provides minor backward compatible extensions to PLAID version 7. All of these extensions are designed to ensure precise definition of function and logic and optimisations implemented in the PLAID version 7.1 reference implementation source code. Consolidated details of the differences to previous versions are set out in the table below

Table 1 Changes between version 7.0 and 7.1

Revision Ref No	Change	Rationale for change	Document Locations

7.1.1	New Section and Explanatory Paragraph	New section and paragraph setting out an overview of changes	This section, Revisions History
7.1.2	Add new options to FA Command to distinguish between one, and two factor PIN or biometric based authentication	<p>For a one factor (default) authentication, there is no sense in passing the PIN hash if it is not going to be used by the IFD. In this circumstance the FA payload only needs to include the diversification data and the ACS record.</p> <p>For a two factor authentication the FA payload needs to additionally include the PIN hash.</p> <p>For a biometric based two factor authentication minutia data is required rather than PIN hash.</p> <p>This change discriminates between these scenarios using the P2 parameter of the FA command and the PLAID ICC application should adjust the payload based on the scenario.</p> <p>This options also improves performance and security since sending superfluous payload information no longer occurs</p> <p>Modified and new P2 definitions for the FA command are:</p> <p>FA_1FACTOR = 0x00 (Default)</p> <p>FA_2FACTOR_PIN = 0x01</p> <p>FA_2FACTOR__MINUTIAE = 0x02</p>	<p>Four new rows in section 11, table 2, Data dictionary. New definition for “Minutiae” and three new FA_xxx objects defined</p> <p>One modified and two new rows under the FA Command in section 15, command set table 3</p> <p>Two new rows for Minutiae under the set and get data Command in section 15, command set table 3</p>
7.1.3	Removed the LUCount	This field was designed to be used to	LUCount

	from the FA payload returned by the ICC	correlate the usage of the card with the usage recorded by backend systems and need not be collected for each authentication. This field can be retrieved after the PLAID authentication has been completed through a “GET DATA” command when an audit is required.	concatenation removed from step 6F of section 12 and from related Figure 1
7.1.4	Remove VersionNo from Set Data command set	Version number should be set at ICC application instantiation and should only be readable after this point.	Remove VersionNo row from Set Data command set in Section 15, table 3
7.1.5	Add new status word (error message) SW_OUT_OF_KEYSTORES	This status word allows an implementation to handle the situation where all of the key slots allocated by the implementation on an ICC have been populated with keys, and an administrator attempts to add a new key. The new SW is : SW_OUT_OF_KEYSTORES = 0x69F7	New row added to section 16, table 4
7.1.6	Remove three status words (error messages) SW_DATA_INVALID SW_INCORRECT_P1P2 SW_CONDITION_NOT_SATISFIED	These error messages have been found to be unnecessary since a failure induced by an attacker should NOT be provided with information confirming a failure. The correct response to an attack is to return seemingly good but incorrect data and for the ICC application to “play along” with the attacker.	Row removed from section 16, table 4
7.1.7	Change value of status word values (error messages)	Values chosen for status words were consistent with ISO/IEC 14443-3 but not to ISO/IEC 7816-3 which mandates status word values must start with	Values modified in section 16, table 4

		<p>either a 6 or a 9 hexadecimal value.</p> <p>The values are changed to:</p> <p>SW_PLAID_LOCKED = 0x69F1</p> <p>SW_PLAID_TERMINATED = 0x69FD</p>	
7.1.8	Remove section “States of the Application”	This section has been moved from this specification to the documentation associated with the reference implementation as the content was implementation specific.	Remove section “States of the Application”
7.1.9	Section 12, Figure 1 PLAID 7.1 Graphic Overview updated	Diagram updated and supporting text boxes numbered to improve clarity	Diagram updated
7.1.10	Section 18, Session Key Generation	Second paragraph, second sentence , deleted words “of the key“ since correctly it is actually the data that is padded	Deleted words “of the key“
7.1.11	Add informative annex regarding key lengths and algorithms	Informative annex added to clarify the requirement to specify key lengths and algorithms and algorithm options	Add Annex “Suggested Key Lengths and Algorithms”

10. PURPOSE

This specification defines the PLAID version 7.1 authentication protocol including all elements required to create an operational implementation of the AP. The specification is intended as the reference documentation required for implementers to build generic and interoperable PLAID version 7.1 ICCs, IFDs and systems. This document is intended to stand in place of formal standards documentation until such time as formal standardisation is complete, at which point this document will be withdrawn, and a reference to the formal standard provided in its place.

11. DATA DICTIONARY

The following table sets out the size and details of PLAID data objects;

Table 2 Data Dictionary

Object Name	Purpose	Size Bytes	Data type	Comments
ACSrecord	Access Control System Record	varies	Alpha-Numeric	The data returned by the Final Authenticate command. The exact structure of this data is determined by the implementation.
DivDat	Symmetric Key Diversification Data	8	Binary	Diversification data fixed at card issuance via a random method and guaranteed unique by the issuance system for any one scheme.
FA_1Factor	Final authenticate default command option (one factor)	8	Binary	When the FA command P2 value is set to 0x00 the command returns the binary concatenation DivDat ACSrecord
FA_2Factor_PIN	Final authenticate two factor factor with PIN command option	8	Binary	When the FA command P2 value is set to 0x01 the command returns the binary concatenation DivDat ACSrecord PINhash
FA_2Factor_Minutiae	Final authenticate two factor with minutiae command option	8	Binary	When the FA command P2 value is set to 0x02 the command returns the binary concatenation DivDat ACSrecord Minutiae
FAkey(DIV)	Diversified Final Authenticate Key	32	Binary	The current Final Authenticate key that has been diversified based on the appropriate key set and key diversification algorithm and per ICC diversification data.
FAkey(KeySetID)	Administrative Final Authenticate Key	32	Binary	Administrative FAkey where KeySetID is always decimal zero.
FAkey(KeySetID)	Final Authenticate Key	32	Binary	An AES symmetric key shared by the smartcard and by the host system. One instance of FAkey will exist for each KeySetID.
IAkey(KeySetID)	Administrative Initial Authenticate Key	32	Binary	Administrative IAkey where KeySetID is always decimal zero.
IAkey(KeySetID)	Initial Authenticate Key	32	Binary	An RSA Key pair used to secure the Initial Authenticate command. One instance of IAkey will exist for each KeySetID with the public key stored on the ICC and the private key stored on the IFD or back office.
KeySetID	Administrative Key Set Identifier	1	Binary, Value=0 decimal	Key set identifier for the administrative key set, which must exist and be key set decimal zero.
KeySetID	Key Set Identifier	1	Binary, Range 1-255 decimal	Key set identifier provided by the IFD to the ICC to support multi-issuer and multi-key set environments.

Object Name	Purpose	Size Bytes	Data type	Comments
LTcount	Logical Try Counter	1	Binary	Logs failed logical authentication attempts for all KeySetIDs other than the Administrative key set. Reset to zero with successful attempt.
LTcountAdm	Logical Try Counter for the Admin Key Set	1	Binary	Logs failed logical authentication attempts for the Administrative KeySetID. Reset to zero with successful attempt.
LUcount	Logical Usage Counter	2	Binary	Logs total successful logical authentications for all KeySetIDs other than the Administrative key set.
LUcountAdm	Logical Usage Counter for the Admin Key Set	2	Binary	Logs total successful logical authentications for the Administrative key set.
Minutiae	Fingerprint Minutiae data stored on-card	Variable up to 224 bytes	Binary	Minutiae template is extracted as raw data and evaluated by the IFD. At this version we are looking to understand if this is sufficient data for operational systems. We are explicitly seeking comment as to whether additional minutiae data should be designed into the specification or whether minutiae should be by individual finger etc.
OpModelID	Administrative Operating Mode Identifier	1	Binary, Value=0 decimal	Operating mode identifier for the administrative mode, which must exist and be set to decimal zero.
OpModelID	Operating Mode Identifier	1	Binary, Range 1-255 decimal	Operating mode identifier provided by the CAD to the ICC to support multiple operating modes.
PIN	PIN	8	Alpha-Numeric	The PIN Global to the ICC.
PINhash	PIN Hash	20	Binary	When retrieving the PIN value, the SHA-1 hash value of the PIN is the only value transmitted.
RND1	Random Number one	32	Binary	Random number generated by the smartcard using its TRNG.
RND2	Random Number two	32	Binary	Random number generated by the IFD or back office system using a TRNG.
RND3	Random Number three	32	Binary	String generated by the IFD and ICC separately calculating $RND1 \oplus RND2$.
SecureICC	Secure the ICC	1	Binary	Flag to hold initial state of the PLAID application 0=unsecured 1=secured.
SessionKey	Session Key	32	Binary	String generated by the IFD and ICC separately calculating RND3.
VersionNo	Version number	1	Binary	Implementation version number, starting at zero and incrementing by one for each release.

12. AUTHENTICATION PROTOCOL DESCRIPTION

The following is a step-by-step description of the steps involved in the PLAID mutual authentication involving a PACS or LACS record.

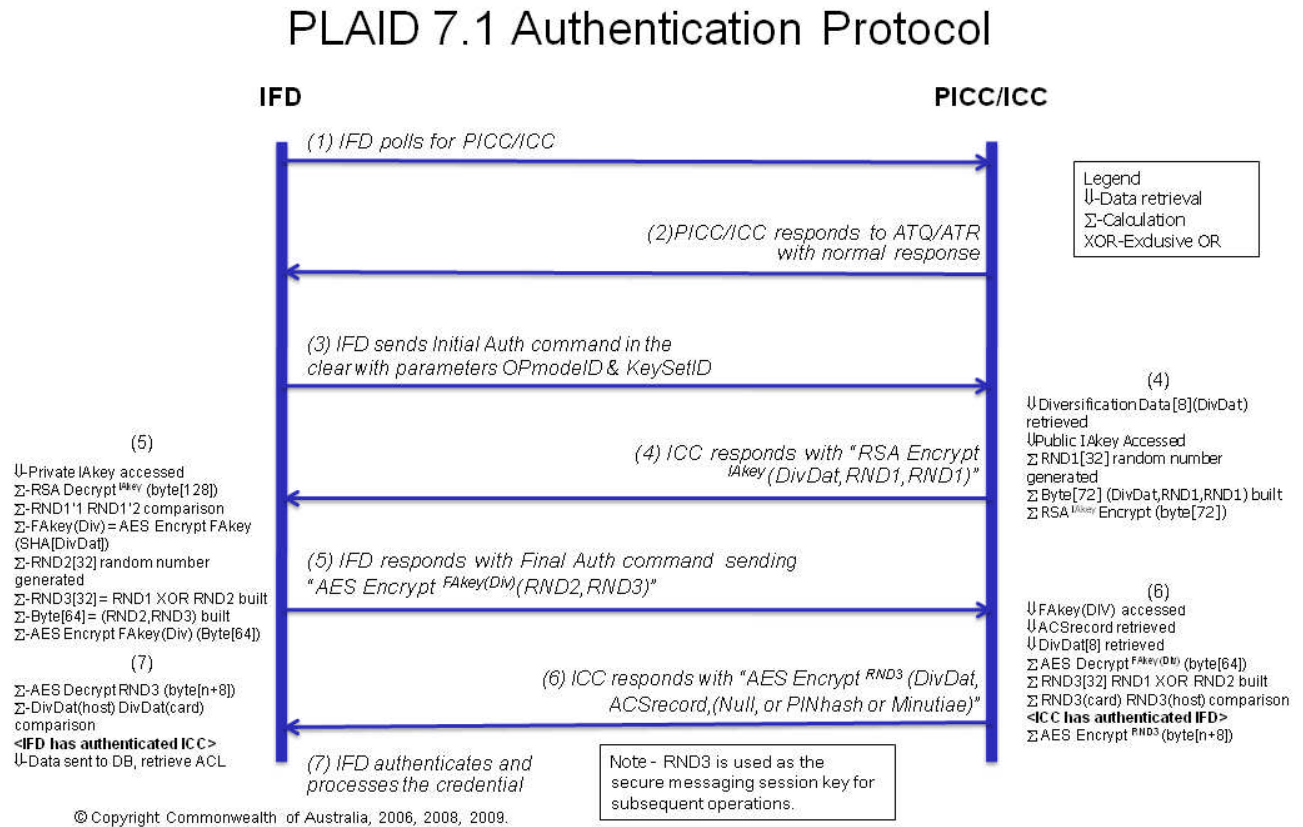


Figure 1 PLAID 7.1 Graphic Overview

The following sets out the explicit steps required in order to carry out a mutual authenticate using the PLAID Authentication Protocol

1) IFD begins polling

- In the case of contactless PICC the IFD polls for the PICC, waits for card presence, completes the ISO/IEC 14443-3 anti-collision procedure and then sends the answer to query (ATQ) command.
- In the case of contact cards, the IFD application shall determine ICC presence from the reader. Once the ICC is present the application shall send the answer to reset (ATR) command according to ISO/IEC 7816-4.

2) ICC responds to ATR/ATQ

- The ICC responds with the ICC normal response to the ATR/ATQ command.
- If the PLAID application is NOT the ICC default application then the ISO/IEC 7816-4 select application command shall be called by the IFD.

3) IFD sends the IA command

- a) The IFD sends an IA request to the ICC in order to obtain the Diversification Data (DivDat).
- b) The IA request incorporates the OpModeID value (in P1) and KeySetID value (in P2) identifying respectively which information the device is expecting to be returned and which cryptographic key set should be used to perform the authentication.

4) ICC responds to the IA command

- a) The ICC retrieves the cryptographic key value as identified by the KeySetID value in P2 of the IA command.
- b) Authentication fails if the key is not found, in which case an equivalent but random string is returned, without ANY indication of the error condition.
- c) The ICC Generates a random value (RND1) using its TRNG.
- d) The ICC Creates the bit string STR1: (DivDat) | RND1 | RND1.
- e) The ICC Computes the bit string ESTR1 where $ESTR1 = \text{RSA Encrypt}^{IAkey}(STR1)$.
- f) Note that the ICC shall incorporate only the modulus and the public exponent values to perform the encryption.
- g) The ICC Transmits the ESTR1 string to the IFD.

5) The IFD responds to the IA response

- a) The IFD calculates STR1 where $STR1 = \text{RSA Decrypt}^{IAkey}(ESTR1)$.
- b) The IFD compares the two copies of RND1 - Authentication fails if they do not match, in which case an equivalent but random string is returned, without ANY indication of the error condition.
- c) The IFD extracts the cards diversification data from STR1.
- d) The IFD generates a random 256-bit value (RND2) using its TRNG.
- e) The IFD calculates $RND1 \oplus RND2$; the result is denoted as RND3.
- f) The IFD uses the diversification data (DivDat) and calculates the diversified final authenticate key $FAkey(Div)$ where $FAkey(Div) = \text{AES Encrypt}^{FAkey}(DivDat, DivDat, DivDat, DivDat)$.
- g) The IFD generates the bit string denoted STR2 where $STR2 = RND2 | RND3$.
- h) The IFD calculates ESTR2 where $ESTR2 = \text{AES Encrypt}^{FAkey}(Div)(STR2)$.
- i) The IFD transmits the final authenticate string ESTR2 to the ICC.

6) The ICC responds to the FA command

- a) The ICC calculates STR2 where $STR2 = \text{AES Decrypt}^{FAkey}(Div) (ESTR2)$.
- b) The ICC Calculates $RND1 \oplus RND2$ and compares it with RND3. Authentication fails if they do not match, in which case an equivalent but random string is returned, without ANY indication of the error condition.
- c) The ICC updates the internal LUcount.
- d) The ICC calculates the PIN hash from the ICC global PIN.
- e) Based on the OpModelID flag set in P1 of the IA command, the ICC retrieves the appropriate PLAID ACSrecord from secure memory.
- f) The ICC concatenates the string STR3 where $STR3 = DivDat \mid ACSrecord \mid$ (then either null or PIN Hash or Minutiae depending on the P2 value of the FA command).
- g) The ICC Calculates ESTR3 where $ESTR3 = \text{AES Encrypt}^{RND3}(STR3)$.
- h) The ICC Transmits ESTR3 to the IFD.

7) The IFD processes the credential

- a) The IFD calculates STR3 where $STR3 = \text{AES Decrypt}^{RND3}(ESTR3)$.
- b) The IFD compares the transmitted DivDat with the IFD copy received in the Initial Authenticate command. Authentication fails if they do not match.
- c) If PIN authentication is required then the IFD will have the cardholders PINhash in STR3 and compares a SHA-1 hash of the PIN from the card holder with the SHA-1 PINhash retrieved from STR3. Authentication fails if they do not match.
- d) If biometric authentication is required then the IFD has the cardholders Minutiae in STR3 and should biometrically compare minutiae from the card holder with minutiae retrieved from STR3. Authentication fails if they do not match.
- e) The ACSrecord is extracted from STR3 and can now be considered to have been authenticated. The ACSrecord can now be passed to whichever back office system is appropriate to open a door or to be part of a further logon process.
- f) Further authentication protocols or card access protocols may optionally use the generated session key RND3 as a secure messaging or encryption key in subsequent sessions.

13. OPERATIONAL MODES AND KEY SETS

This specification allows for up to 255 key sets. For each key set, the value for IAkey and FAkey can be different. This allows that different levels of trust can be applied depending on the business requirements of the implementation. These might be building, role or function based, or some combination of these or other factors.

This specification allows for up to 255 operational modes. For each mode, the ACS record returned in the final authenticate can be different, and allows that a distinct ACS record can then be passed to the IFD or backend systems depending on the business requirements of the implementation.

For **example**, a system might utilise the following key sets and/or operational modes:

Old buildings - only authenticates weigand number for older buildings

New Buildings - authenticates using ISO/IEC 7812 based numbering

Administration - modify the cards PLAID contents such as off-line keys or ACS records

Logical Access - access to system login, printer access, etc

Physical Access - perimeter access

Computer room - computer room access and highly secure areas

Offline - physical network connection is not possible

Shared - shared public areas of government buildings - trusted persons can enter outer perimeter

Note: there may or may not be a one-one correspondence between OpModeID and KeySetID in any one implementation. For instance; during transition there may be a single KeySetID utilised for building access, but new buildings might use one OpModeID whilst old buildings use another in order to transition from their use of the older weigand based numbering.

There is always an administrative key set and operational mode; these are denoted by the value contained in OpModeID and KeySetID being set to decimal zero for the related objects; KeySetID, OpModeID, IAkey(KeySetID) and FAkey(KeySetID).

14. APPLICATION IDENTIFICATION

The PLAID application shall be selected either by;

- making the PLAID authentication application the default application;
- calling the AID registered by the Australian Commonwealth (Centrelink) directly at "A0 00 67 6D 61 66"; or
- registering an appropriate AID for a specific scheme.

PLAID supports multiple implementations under different AIDs, therefore more than one implementation may be supported per card or reader as long as the appropriate AID is explicitly called or set as the default AID.

15. COMMAND SET

The following are the specific commands required to comply with this specification. These commands are based on commands specified in ISO/IEC 7816 part 4 including the provision within the standard for the introduction of new commands for specific purposes such as PLAID. Within ISO/IEC 7816-4 there is provision for the passing of parameters via the P1 and P2 structures. The P1 structure is used to pass the operational mode parameter and the P2 structure is utilised to pass the key-set identifier from the IFD to the ICC. These parameters are sent in the clear by the IFD in the Initial Authenticate command.

Table 3 Command Set

Operation	CLA	INS	Object	P1 Value	P2 Value	Lc/Le	Comments
Initial Authenticate	0x80	0x8A	IA	<OpModelID>	<KeySetID>	N/A N/A	Only available when card application security state is "PLAID_SECURED"
Administrative Initial Authenticate	0x80	0x8A	IA	0x00	0x00	N/A	Only available when card application security state is "PLAID_SECURED" and when administrative KeySetID(0) is selected
Final Authenticate	0x80	0x8C	FA_1FACTOR	0x00	0x00	Lc=0x40	Only available when card application security state is "PLAID_SECURED" and the corresponding "INITIAL AUTHENTICATE" command has been successfully completed.
			FA_2FACTOR_PIN	0x00	0x01	Lc=0x40	
			FA_2FACTOR_MINUTIAE	0x00	0x02	Lc=0x40	
Set Data	0x80	0xDB	DivDat	0x01	0x00	Lc=0x10	Only available when card is state is "PLAID_UNSECURED" or "FINAL_AUTHENTICATE" and after Administration has been successfully completed. The length of the APDU body must be padded with null(s)
			ACSrecord	0x02	0x00	Lc=Variable per scheme	
			PIN	0x03	0x00	Lc=0x20	

Operation	CLA	INS	Object	P1 Value	P2 Value	Lc/Le	Comments
			SecureICC	0x04	0x00	Lc=0x10	(0x00) until the length is equal to the specified Lc when the ICC is in the state "PLAID_UNSECURED". The data value of the command must be encrypted with the session key when the smartcard is in the state "PLAID_SECURED".
			Minutiae	0x06	0x00	Lc=0xE0	
			IAkey	0x07	<KeySetID>	Lc=0x20	
			FAkey	0x08	<KeySetID>	Lc=0x20	
			LTcount	0x0A	0x00	Lc=0x10	
Get Data	0x80	0xCB	ACSrecord	0x02	0x00	Le=Variable per scheme	Only available when card security state is "PLAID_SECURED" and "FINAL_AUTHENTICATE" (User or Administration) has been successfully completed. Note: The smartcard response will be encrypted with the session key Note: The decrypted response will be padded with null(s) (0x00) up to the length specified in Lc.
			PINhash	0x03	0x00	Le=0x20	
			VersionNo	0x05	0x00	Le=0x10	
			Minutiae	0x06	0x00	Le=0xE0	
			LTcount	0x0A	0x00	Le=0x10	
			LTcountAdm	0x0B	0x00	Le=0x10	
			LUcount	0x0C	0x00	Le=0x10	
			LUcountAdm	0x0D	0x00	Le=0x10	

16. ERROR CODES (STATUS WORDS)

In addition to the standard error status conditions supported by ISO/IEC 7816 and ISO/IEC 14443, the following are the status words required in order to support the full range of PLAID error conditions.

Table 4 PLAID Error Codes (Status Words)

Error Code Name	Status Word Value	Origin
SW_WRONG_LENGTH	0x6700	ISO/IEC 7816-4
SW_COMMAND_NOT_ALLOWED	0x6986	ISO/IEC 7816-4
SW_INS_NOT_SUPPORTED	0x6D00	ISO/IEC 7816-4
PLAID_LOCKED	0x69F1	This specification
PLAID_TERMINATED	0x69FD	This specification
SW_OUT_OF_KEYSTORES	0x69F7	This specification

17. KEY DIVERSIFICATION

PLAID utilises key diversification to ensure that the system remains secure should an individual ICC be compromised and its secret keys determined. The algorithm used to diversify the FAkey is as follows:

$$FAkey (DIV) = AES\ Encrypt^{FAkey}(DivDat, DivDat, DivDat, DivDat)$$

18. SESSION KEY GENERATION

PLAID results in the generation of a 256 bit (32 byte) session key in the final steps.

It is then possible for all subsequent communications between the ICC and the IFD or back office to have the body of the APDU encrypted with this key within a secure messaging session. Since AES uses 128 bit (16 byte) blocks for encryption/decryption, padding may be required up to the next block. The process used to generate the session key is as follows:

$$SessionKey (RND3) = RND1 \oplus RND2$$

19. ACCESS CONTROL SYSTEM RECORD

The detailed structure of the ACS record or credential shall be determined by the issuers' specific specification or standards and use case. This is outside the scope of this specification.

PLAID supports multiple concurrent types of ACS record which are selected via the OpModelID parameter.

Since multiple ACS records may be stored and selected, these may for example include existing record numbers such as weigand building access numbers (for transition purposes), biometric templates or any other appropriate or standardised personnel number/s or strings which require authentication.

ANNEX A: *REFERENCE IMPLEMENTATION (INFORMATIVE)*

A reference implementation is available to assist in the comprehensive understanding of how to implement this specification.

The reference implementation may be downloaded from the following URL;

<https://www.govdex.gov.au> and select **Centrelink PLAID** from the list of Public GovDex Communities.

ANNEX B: FUNCTIONAL SPECIFICATION (INFORMATIVE)

The following are the functional requirements for PLAID version 7. The authentication protocol shall;

- **Speed** - result in a complete exchange between the ICC and IFD in less than 0.4 seconds. (Using optimal ICC and IFD devices and assuming keys are cached in the IFD and the credential payload does not overflow a single APDU),
- **Standard algorithms** -Utilise COTS cryptographic algorithms commonly employed and available on ICC and IFD devices and in public domain libraries,
- **ID-Leakage** - have no individually identifiable, unique or determinable data or characteristic of the ICC or card holder transmitted during authentication. Note: This does not apply to the IFD since the location and characteristics of the IFD are generally public knowledge,
- **Private-data-leakage** - have no availability of private data in the clear at any interface,
- **Replay attack** - not generate or utilise any repeatable data that could allow another ICC or ICC emulator to successfully frame a replay attack,
- **Man-in-the-middle attack** - utilise countermeasures which 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,
- **PIN authentications** - provide the ICCs 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. Should a PIN not be required, such as for low security perimeter access, the hash data should be able to be disregarded,
- **Session key generation** - provide a secure 256 bit one-time session key negotiated between the ICC and IFD and suitable for subsequent secure session or secure messaging protocols,
- **Multiple key sets** - support multiple keysets such that keys may be allocated by purpose, such as different perimeters or higher or lower security zones. Additionally the protocol shall support spare un-used key-sets for planned or tactical key roll operations,

- **Multiple credential payloads** - support the authentication of different credential payloads or credential data depending on the requirement of the IFD and the scheme. Payload size shall be extensible up to 1 Kbyte,
- **Authentication failure and velocity countermeasures** - support counters to assist in the identification of attacks and their velocity and to destroy all keys in the case of attack.

ANNEX C: ID-LEAKAGE CONSIDERATIONS (INFORMATIVE)

ID-Leakage may occur in passive or active forms. Passive leakage is where unique per card or per scheme data is available simply by recording the session between IFD and ICC/PICC. Active leakage can occur where specific tools or viruses scan the ICC/PICC for useful identification or private data at likely addresses on the card.

Passive attacks are relatively easily eliminated by the methods used by PLAID, subject to appropriate initialisation of the ICC as discussed below.

Active attacks may be impractical to fully eliminate, since most existing specifications require some freely available information to be available at predictable ICC/PICC addresses, and resolving this is well beyond the scope of this specification. The discussion below provides some options for consideration in order to minimise the impact of active ID-Leakage

C1: PASSIVE ID-LEAKAGE

In order to remove possible passive ID-Leakage when implementing PLAID, the following additional checks should be considered as part of the pre-personalisation set up of a PLAID ICC/PICC.

- a) In the case of contactless PICC the UID generated by the PICC for the ISO/IEC 14443-3 anti-collision procedure should be specified to use the “random” option of ISO/IEC 14443-3. This generally needs to be set prior to card personalisation or in some cases at manufacture.
- b) In implementations where ID-Leakage of any form cannot be tolerated, care may need to be taken to ensure the ATR/ATQ response does not contain unique per-card or per-scheme identifying data, particularly in the ISO/IEC 7816-3,4 historical bytes. Any such data which must be set may be best set to null values. This generally needs to be set prior to card personalisation or in some cases at manufacture.
- c) Check for any possible session dialogue with other applications on the ICC, particularly any which are set as the default application.

C2: ACTIVE ID-LEAKAGE

- a) Check the status and session dialogue of all applications on the card, particularly generic or diagnostic applications from the manufacturer which may be instantiated in the Read Only Memory (ROM) mask, and may or may not be formally documented or normally disclosed by the manufacturer.
- b) Administrative functions such as card management are generally carried out using a contact reader. Many ICC/PICCs can differentiate programmatically between contact and contactless interfaces, and can refuse access to selected applications from the contactless interface. Consider switching off access to administrative applications from contactless interfaces, particularly ones which store unique card identification information such as the GlobalPlatform card manager.

ANNEX D: SUGGESTED KEY LENGTHS AND ALGORITHMS (INFORMATIVE)

It is intended that PLAID may be implemented with different key lengths and cryptographic algorithms and their modes and options. These may change over time and may be dependent on end use application and the interoperability and performance requirements of different communities of interest. Communities of interest may choose lower bit length options in order to obtain faster transaction times or vice versa for higher security.

Where interoperability is a requirement it is important that the community of interest clearly specify the specific algorithms, modes, options and key length requirements in their specifications.

There is always a trade off between key length, cryptographic options and speed, which will also vary by the particular technology used in both the IFD and ICC.

The Centrelink Reference Implementation uses RSA 1024 with PKCS1.5 padding and AES 256 in ECB mode; however the following combinations have been reviewed and found suitable on current generation ICCs and IFDs. Other combinations may well be suitable depending on end-use and transaction time requirements.

Table 5 Suggested Key Lengths and Algorithms

Ref	Symmetric Algorithm	Key length (bits)	Mode	Asymmetric algorithm	Key length (bits)	Padding	Options	Target transaction time (ms)
1	AES	256 ⁽¹⁾	ECB ⁽²⁾	RSA	1024	PKCS1.5 ⁽³⁾	CRT ⁽⁴⁾	300
2	AES	256 ⁽¹⁾	ECB ⁽²⁾	RSA	1536	PKCS1.5 ⁽³⁾	CRT ⁽⁴⁾	400
3	AES	256 ⁽¹⁾	ECB ⁽²⁾	RSA	1984	PKCS1.5 ⁽³⁾	CRT ⁽⁴⁾	480
4	AES	256 ⁽¹⁾	ECB ⁽²⁾	RSA	2048 ⁽⁵⁾	PKCS1.5 ⁽³⁾	CRT ⁽⁴⁾	500 ⁽⁶⁾

Notes to table 5:

1. Little performance difference was found between the key length options for AES, therefore only AES 256 is considered.
2. Cipher Block Chaining (CBC) mode is normally recommended for AES cryptographic operations. However, each AES block within a PLAID transaction contains sufficient

entropy for there to be no need to link the cipher blocks and ECB provides a performance advantage.

3. Optimal Assymmetric Encryption Padding (OAEP) would normally be the padding scheme for RSA cryptographic operations. However, PLAID doesn't expose the modulus or any other RSA primitive, therefore there is no currently identified benefit in using OAEP over PKCS1.5 padding. There is a significant performance advantage in using PKCS1.5 padding.
4. Chinese Remainder Theorem (CRT) may be optionally used to improve the speed of the RSA operation performed by the IFD subject to all secret parameters being stored securely on a SAM or HSM device.
5. Where cards do not support "extended APDU" an additional APDU is returned by the FA command once RSA key lengths exceed 255 bytes or 2040 bits. There is a consequent and significant performance reduction as a result of this additional APDU. The target time here assumes cards supporting extended APDUs.
6. Transaction times greater than 500ms may be too slow for viable contactless use.