Centrelink PLAID version 7 (Nov 2008)

Logical SmartCard Application Specification

**Contents**

[1. Introduction 2](#_Toc407107415)

[2. PLAID Authentication Protocol 3](#_Toc407107416)

[3. COPYRIGHT 4](#_Toc407107417)

[4. Software Licensing Terms (License) 4](#_Toc407107418)

[4.1 License 5](#_Toc407107419)

[4.2 Intellectual Property Rights 5](#_Toc407107420)

[4.3 Disclaimer 5](#_Toc407107421)

[4.4 Indemnity 6](#_Toc407107422)

[4.5 Assignment and Novation 6](#_Toc407107423)

[4.6 Costs 6](#_Toc407107424)

[4.7 Miscellaneous 6](#_Toc407107425)

[4.8 Definitions and interpretation 6](#_Toc407107426)

[5. Scope 7](#_Toc407107427)

[6. Normative References 7](#_Toc407107428)

[7. Terms and Definitions 7](#_Toc407107429)

[7.1 ACS record (ACSrecord) 7](#_Toc407107430)

[7.2 Card Holder 7](#_Toc407107431)

[7.3 Diversification Data (DivDat) 7](#_Toc407107432)

[7.4 Issuer 8](#_Toc407107433)

[7.5 ID-Leakage 8](#_Toc407107434)

[7.6 Keyset Identifier (KeySetID) 8](#_Toc407107435)

[7.7 LACS record 8](#_Toc407107436)

[7.8 Man-in-the-middle attack 8](#_Toc407107437)

[7.9 Operational mode identifier 8](#_Toc407107438)

[7.10 PACS record 8](#_Toc407107439)

[7.11 Private data leakage 8](#_Toc407107440)

[7.12 Replay attack 8](#_Toc407107441)

[8. Symbols (and abbreviated terms) 8](#_Toc407107442)

[logical exclusive or operator (XOR) 8](#_Toc407107443)

[9. Purpose 10](#_Toc407107444)

[10. Data Dictionary 10](#_Toc407107445)

[Table 1: Data Dictionary 10](#_Toc407107446)

[11. Authentication Protocol Description 12](#_Toc407107447)

[12. Operational Modes and Key Sets 14](#_Toc407107448)

[13. Application Identification 15](#_Toc407107449)

[14. Command Set 15](#_Toc407107450)

[Table 2: Command Set 15](#_Toc407107451)

[15. Error Codes (Status Words) 16](#_Toc407107452)

[Table 3: PLAID Error Codes (Status Words) 16](#_Toc407107453)

[16. Key Diversification 17](#_Toc407107454)

[17. Session Key Generation 17](#_Toc407107455)

[18. States Of The Application 17](#_Toc407107456)

[19. Access Control System Record 18](#_Toc407107457)

[Annex A: Reference Implementation (Informative) 18](#_Toc407107458)

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.

1. 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.

1. 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.**

1. Software Licensing Terms (License)

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.

* 1. License

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.”

* 1. 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.

* 1. 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.

* 1. 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.

* 1. Assignment and Novation

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

* 1. Costs

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

* 1. 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.

* 1. 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.

1. 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.

1. 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

1. Terms and Definitions

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

* 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.

* 1. 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.

* 1. 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.

* 1. Issuer

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

* 1. 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.

* 1. Keyset Identifier (KeySetID)

An identifier which uniquely identifies a key set.

* 1. LACS record

Logical access control system record, see ACS record.

* 1. 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.

* 1. Operational mode identifier

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

* 1. PACS record

Physical access control system record, see ACS record.

* 1. 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.

* 1. 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.

1. Symbols (and abbreviated terms)

| **Symbol** | **Meaning** |
| --- | --- |
| | | 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 |
| DivDat | diversification data |
| 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 |
| PLAID | protocol for lightweight authentication of identity |
| POM | 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 |

1. Purpose

This specification defines the PLAID version 7 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 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.

1. Data Dictionary

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

Table 1: Data Dictionary

| **Purpose**  | **Object Name**  | **Size Bytes**  | **Data type**  | **Comments**  |
| --- | --- | --- | --- | --- |
| Access Control System Record  | ACSrecord  | varies  | Alpha-Numeric  | The data returned by the Final Authenticate command. The exact structure of this data is determined by the implementation.  |
| Symmetric Key Diversification Data  | DivDat  | 8  | Binary  | Diversification data fixed at card issuance via a random method and guaranteed unique by the issuance system for any one scheme.  |
| PIN  | PIN  | 8  | Alpha-Numeric  | The PIN Global to the ICC.  |
| IN Hash  | PINhash  | 20  | Binary  | When retrieving the PIN value, the SHA-1 hash value of the PIN is the only value transmitted.  |
| Logical Usage Counter  | LUcount  | 2  | Binary  | Logs total successful logical authentications for all KeySetIDs other than the Administrative key set.  |
| Logical Usage Counter for the Admin Key Set  | LUcountAdm  | 2  | Binary  | Logs total successful logical authentications for the Administrative key set.  |
| Logical Try Counter  | LTcount  | 1  | Binary  | Logs failed logical authentication attempts for all KeySetIDs other than the Administrative key set. Reset to zero with successful attempt.  |
| Logical Try Counter for the Admin Key Set  | LTcountAdm  | 1  | Binary  | Logs failed logical authentication attempts for the Administrative KeySetID. Reset to zero with successful attempt.  |
| Initial Authenticate Key  | IAkey(KeySetID)  | 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.  |
| Administrative Initial Authenticate Key  | IAkey(KeySetID)  | 32  | Binary  | Administrative IAkey where KeySetID is always decimal zero.  |
| Final Authenticate Key  | FAkey(KeySetID)  | 32  | Binary  | An AES symmetric key shared by the smartcard and by the host system. One instance of FAkey will exist for each KeySetID.  |
| Administrative Final Authenticate Key  | FAkey(KeySetID)  | 32  | Binary  | Administrative FAkey where KeySetID is always decimal zero.  |
| Diversified Final Authenticate Key  | FAkey(DIV)  | 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.  |
| Key Set Identifier  | KeySetID  | 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.  |
| Administrative Key Set Identifier  | KeySetID  | 1  | Binary, Value=0 decimal  | Key set identifier for the administrative key set, which must exist and be key set decimal zero.  |

1. 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.

(The original image isn’t readable, so the original needs to be found so it can be copied over in a readable way. It also needs to have an alt-text explanation of what it shows.)

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
	1. 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.
	2. 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
	1. The ICC responds with the ICC normal response to the ATR/ATQ command.
	2. 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
	1. The IFD sends an IA request to the ICC in order to obtain the Diversification Data (DivDat).
	2. 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
	1. The ICC retrieves the cryptographic key value as identified by the KeySetID value in P2 of the IA command.
	2. 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.
	3. The ICC Generates a random value (RND1) using its TRNG.
	4. The ICC Creates the bit string STR1: (DivDat) | RND1 | RND1.
	5. The ICC Computes the bit string ESTR1 where ESTR1 = RSA Encrypt IAkey (STR1).
	6. Note that the ICC shall incorporate only the modulus and the public exponent values to perform the encryption.
	7. The ICC Transmits the ESTR1 string to the IFD.
5. The IFD responds to the IA response
	1. The IFD calculates STR1 where STR1 = RSA Decrypt IAkey(ESTR1).
	2. 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.
	3. The IFD extracts the cards diversification data from STR1.
	4. The IFD generates a random 256-bit value (RND2) using its TRNG.
	5. The IFD calculates RND1⊕RND2; the result is denoted as RND3.
	6. The IFD uses the diversification data (DivDat) and calculates the diversified final authenticate key FAkey(Div) where FAkey(Div) = AES Encrypt FAkey(DivDat, DivDat, DivDat, DivDat).
	7. The IFD generates the bit string denoted STR2 where STR2 = RND2 | RND3.
	8. The IFD calculates ESTR2 where ESTR2 = AES Encrypt FAkey(Div) (STR2).
	9. The IFD transmits the final authenticate string ESTR2 to the ICC.
6. The ICC responds to the FA command
	1. The ICC calculates STR2 where STR2 = AES Decrypt FAkey(Div) (ESTR2).
	2. The ICC Calculates RND1⊕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.
	3. The ICC updates the internal LUcount.
	4. The ICC calculates the PIN hash from the ICC global PIN.
	5. Based on the OpModeID flag set in P1 of the IA command, the ICC retrieves the appropriate PLAID ACSrecord from secure memory.
	The ICC concatenates the string STR3 where STR3 = DivDat | LUcount| PIN Hash| ACSrecord.
	6. The ICC Calculates ESTR3 where ESTR3 = AES Encrypt RND3(STR3).
7. The ICC Transmits ESTR3 to the IFD.
	1. The IFD processes the credential
	2. The IFD calculates STR3 where STR3 = AES Decrypt RND3(ESTR3).
	3. The IFD compares the transmitted DivDat with the IFD copy received in the Initial Authenticate command. Authentication fails if they do not match.
	4. If PIN authentication is required then the IFD has 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.
	5. 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.
	6. 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.
8. 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).

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).

1. 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.

1. 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 2: Command Set

| **Operation**  | **CLA**  | **INS**  | **Object**  | **P1 Value**  | **P2 Value**  | **Lc/Le**  | **Comments**  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Initial Authenticate  | 0x80  | 0x8A  | IA  | <OpModeID>  | <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  | 0x00  | 0x00  | Lc=0x40  | Only available when card application security state is “PLAID\_SECURED” and the corresponding “INITIAL AUTHENTICATE” command has been successfully completed.  |
| 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) (0x00) until the length is equal |
| ACSrecord  | 0x02  | 0x00  | Lc=Variable per scheme  |
| PIN  | 0x03  | 0x00  | Lc=0x20  |
|  |  |  | 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”.  |
| VersionNo | 0x05 | 0x00 | Lc=0x10 |
| IAkey | 0x07 | <KeySetID> | Lc=0x20 |
| FAkey | 0x08 | <KeySetID> | Lc=0x20 |
| LTcount | 0x0A | 0x00 | Lc=0x10 |
| Get Data | 0x80 | 0xCB | DivDat | 0x01 | 0x00 | Le=0x10 | 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.  |
| ACSrecord | 0x02 | 0x00 | Le=Variable per scheme |
| PINhash | 0x03 | 0x00 | Le=0x20 |
| VersionNo | 0x05 | 0x00 | Le=0x10 |
| LTcount | 0x0A | 0x00 | Le=0x10 |
| LTcountAdm | 0x0B | 0x00 | Le=0x10 |
| LUcount | 0x0C | 0x00 | Le=0x10 |
| LUcountAdm | 0x0D | 0x00 | Le=0x10 |

1. 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 3: PLAID Error Codes (Status Words)

| **Error Code Name**  | **Status Word Value**  | **Origin**  |
| --- | --- | --- |
| SW\_WRONG\_LENGTH | 0x6700 | ISO/IEC 7816-4 |
| SW\_DATA\_INVALID | 0x6984 | ISO/IEC 7816-4 |
| SW\_CONDITION\_NOT\_SATISFIED | 0x6985 | ISO/IEC 7816-4 |
| SW\_COMMAND\_NOT\_ALLOWED | 0x6986 | IISO/IEC 7816-4 |
| SW\_INCORRECT\_P1P2 | 0x6A86 | ISO/IEC 7816-4 |
| SW\_INS\_NOT\_SUPPORTED | 0x6D00 | ISO/IEC 7816-4 |
| PLAID\_LOCKED | 0xF1F1 | This specification |
| PLAID\_TERMINATED | 0xFDFD | This specification |

1. 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)*

1. 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 of the key may be required up to the next block. The process used to generate the session key is as follows:

*SessionKey (RND3) = RND1*⊕*RND2*

1. States Of The Application

This specification requires the following states to be supported for the PLAID on-card application:

UNSECURED

* + Initial state of the smartcard after the applet has been instantiated on the smartcard. The personalisation of the application and cryptographic key load should be performed on secure equipment immediately after this state becomes available on the card.

SECURED

* + “Idle” state of the card. The transition from “UNSECURED” is irreversible.

IA\_< KeySetID>\_COMPLETED

* + The IA command has been completed for an operational keyset mode.

IA\_ADMINISTRATION\_COMPLETED

* + The IA command has been completed in administration mode.

FA\_< KeySetID>\_COMPLETED

* + The Final Authentication command has been completed for an operational keyset mode.

FA\_ADMINISTRATION\_COMPLETED

* + The Final Authentication command has been completed in administration mode.

PLAID\_LOCKED

* + If the LTcount object exceeds the maximum allowed value then the application is placed in this state.

PLAID\_TERMINATED

* + If the LTcountAdm object exceeds the maximum allowed value then the application is placed in this state and, all keys are erased and all operations are disabled.
1. 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 OpModeID 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 [GovDex](https://www.govdex.gov.au) and select **Centrelink PLAID** from the list of Public GovDex Communities.