PLAID application specification

License Version 8.0 – Final

Contents

[PLAID application specification 1](#_Toc408582059)

[License Version 8.0 – Final 1](#_Toc408582060)

[1. Introduction 3](#_Toc408582061)

[2. PLAID Authentication Protocol 4](#_Toc408582062)

[3. Copyright 5](#_Toc408582063)

[4. Software Licensing Terms (License) 5](#_Toc408582064)

[4.1 License 5](#_Toc408582065)

[4.2 Intellectual Property Rights 6](#_Toc408582066)

[4.3 Disclaimer 6](#_Toc408582067)

[4.4 Indemnity 6](#_Toc408582068)

[4.5 Assignment and Novation 7](#_Toc408582069)

[4.6 Costs 7](#_Toc408582070)

[4.7 Miscellaneous 7](#_Toc408582071)

[4.8 Definitions and Interpretation 7](#_Toc408582072)

[5. Scope 7](#_Toc408582073)

[6. Normative References 8](#_Toc408582074)

[7. Terms and Definitions 8](#_Toc408582075)

[7.2 Card Holder 8](#_Toc408582076)

[7.3 Issuer 8](#_Toc408582077)

[7.4 ID-Leakage 8](#_Toc408582078)

[7.5 Man-in-the-middle attack 9](#_Toc408582079)

[7.6 Private data leakage 9](#_Toc408582080)

[7.7 Reflection attack 9](#_Toc408582081)

[7.8 Replay attack 9](#_Toc408582082)

[8. Symbols (and Abbreviated Terms) 9](#_Toc408582083)

[9. Revisions History 11](#_Toc408582084)

[10. Purpose 12](#_Toc408582085)

[11. Data Dictionary 12](#_Toc408582086)

[Table 2: Data Dictionary 12](#_Toc408582087)

[12. Authentication Protocol Description 14](#_Toc408582088)

[13. Key Sets 16](#_Toc408582089)

[14. Operational Modes 17](#_Toc408582090)

[15. Application Identification 17](#_Toc408582091)

[16. Command Set 18](#_Toc408582092)

[Table 3: Command Set 18](#_Toc408582093)

[17. Error Codes 18](#_Toc408582094)

[Table 4: PLAID Error Codes (Status Words) 18](#_Toc408582095)

[18. Key Diversification 19](#_Toc408582096)

[19. Session Key Generation 19](#_Toc408582097)

[Annex A: Reference Implementation (Informative) 20](#_Toc408582098)

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 authentication protocols currently available either proprietary or via existing formal standards. PLAID is designed to perform a high strength mutual authentication in the 150-300 millisecond range, (0.15 to 0.3 of a second), making it suitable for a range of mission critical contactless applications.

There are significant advantages in efficiency and reduction in costs if a common, non-proprietary and standardised authentication protocol of this type is available across common software, readers, building, key and card management systems particularly with multiple agencies or governments and their vendors supporting the exact 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 Australian and ISO/IEC standards.

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

Have PLAID evaluated by the most 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 is a step in the standardisation strategy. It provides any interested party with a formal, stabilised and prototyped version of PLAID (Version 8) which has both been reviewed by respected cryptographic organisations and has been load tested on a significant range of smartcards and devices over a four year period.

Version 8 incorporates various cryptographic enhancements in response to issues identified by the Australian Defence Signals Directorate (DSD), the US National Institute of Standards and Technology (NIST), a number of Independent cryptographic experts and consultants, a number of respected commercial cryptographic teams, as well as the internal Centrelink team. This version also incorporates enhancements and simplifications in support of a broader range of use cases raised by a number of US agencies and NIST in US workshops. Some of these changes are designed to enable support for ISO/IEC 24727 parts 3 and 6, which is emerging as an important requirement for any formal authentication protocol. PLAID version 8 will be formally registered by Centrelink under the ISO/IEC 24727-6 registration authority.

The specification of PLAID version 8 is the last version of this document supported 100% by Centrelink; future versions will be available as a formal Australian Standard (and probably subsequently as an ISO/IEC standard). Centrelink will continue to support reference implementations of the formal Australian and ISO/IEC Standard as required.

This document includes a production licence which allows the re-distribution of PLAID intellectual property 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. This licence will continue to be offered for implementations under both Australian and ISO/IEC standardisation processes.

1. PLAID Authentication Protocol

PLAID is a cryptographic and algorithmic method and associated source code which uses symmetric and asymmetric cryptography in a unique protocol to protect the communications between ICCs and terminal devices in such a way that strong authentication of objects on the ICC 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 150 and 300 milliseconds (0.15 - 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.

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.

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 8 supports the following new features;

Multiple operational modes (65,535). Different operational modes, identified by “OpModeID”, can be used to provide authenticated access control system records with varying content. 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; an ICAO credential; a RFC 4122 UUID record; an ISO/IEC 7812 card number; a PIV FASC-N or CHUID record; a biometric template or any other numbering system required by the environment.

Support for implementation under ISO/IEC 24727-6 through the use of ASN.1 compliant encoding.

ISO/IEC 24727-4 command and status word compliant. No proprietary commands or error status are utilised.

Various performance enhancements.

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 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 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.”

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.

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, ACS 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 made available by Centrelink to support this document. This implementation 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 with contacts

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

ITU-T X.680 – OSI Networking and System Aspects – Abstract Syntax Notation One

ISO/IEC 8824-1 – Information Technology – Abstract Syntax Notation One

1. Terms and Definitions

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

7.2 Card Holder

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

7.3 Issuer

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

7.4 ID-Leakage

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

7.5 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.

7.6 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.

7.7 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. Protocols that are symmetric in nature can be susceptible to this type of attack.

7.8 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) |
| AES | advanced encryption standard (as defined in FIPS-197) |
| AID | application identifier |
| AP | authentication protocol |
| APDU | application protocol data unit |
| ASN.1 | abstract syntax notation number 1 (as defined in ITU-T x.680) |
| CBC | cipher block chaining |
| COTS | commercial off the shelf |
| CRT | Chinese remainder theorem |
| DivDat | diversification data – salt data used in cryptographic operations |
| DOS | denial of service (attack) |
| 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 | A 2-byte value specifying which key set 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 specification to ICC |
| PIN | personal identification number |
| PKCS | public key cryptography standards |
| 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 |
| XOR | logical exclusive Or operation |

1. Revisions History

PLAID version 8.0 does not provide backwards compatibility to earlier versions. Consolidated details of the differences between PLAID version 8.0 and PLAID version 7.1 are set out in the table below.

| **Change** | **Rationale for change** |
| --- | --- |
| Various definitions and symbols and informative text | Consistency with other changes and with changing referenced standards. |
| The AES session key is generated by the hashing of RND1 and RND2.  Previous versions used the XOR operator. | An “adaptive nonce” attack could be performed on a compromised host. This host could generate a value for RND2 which complimented the ICC generated RND1, resulting in a predictable session key. |
| The response from the ICC to a Final Authenticate command should be encrypted using CBC.  Previous versions used ECB. | Repeating blocks of data will have identical corresponding cipher text in ECB mode, even when encrypted with a random session key. Biometric data may contain repeating blocks of data. |
| Removal of all “Try” and “Usage” counters and all associated metadata | The implementation of “Try” counters could make a PLAID implementation susceptible to DOS attacks. Additionally, the ability to lock a card through invalid attempts could lead to the determination of which key sets were present on the ICC.  The functionality of “Usage” counters is outside the scope of this authentication protocol. |
| Both KeySetID and OpModeID have been defined as 2 byte fields.  Previous versions used 1 byte for these fields. | A one-byte field for KeySetID (and to a lesser extent, OpModeID) may not be sufficient for large organisations with multiple units requiring unique keys sets which may be periodically “key-rolled”. |
| The key diversification algorithm has been changed to AESEncryptFAKEY(DivData).  Previous versions used: AESEncryptFAKEY(DivData,DivData,DivData,DivData). | No additional entropy is gained by repeating the DivData field four times. |
| Naming and symbol conventions adjusted | To support the standardisation process |
| Removal of all data from P1 and P2 of an APDU and use of generic CLA/INS fields | To assist in the standardisation of PLAID under ISO/IEC 24727 |
| Inclusion of ASN.1 representation of data in the APDU body. | To assist in the standardisation of PLAID under ISO/IEC 24727 |

1. Purpose

This specification defines the PLAID version 8.0 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 8.0 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 2: Data Dictionary

| **Object Name** | **Purpose** | **Size Bytes** | **Data type** | **Comments** |
| --- | --- | --- | --- | --- |
| ACSRecord | Access Control System Record | varies | Alpha-Numeric | An Access Control System record for each supported Operational Mode Identifier for the purpose of authorisation 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 | 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(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. There are only 3 distinct key sizes allowable by AES. |
| KeySetID | Uniquely identify a keyset | 2 | Binary | One or more 2-byte identifiers sent in a list to the ICC in the Initial Authenticate command so as to determine and/or negotiate the key set to be used for authentication. |
| Minutiae | Fingerprint Minutiae data stored on-card | Variable | 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. |
| OpModeID | Operation Mode Identifier | 2 | Binary | An identifier sent to the ICC in the Final Authenticate command that determines which ACSRecord record is served up in the final authentication response from the ICC. |
| PIN | PIN | 8 | 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 1 | 16/24/32 | Binary | Random number generated by the smartcard using its TRNG. |
| RND2 | Random Number 2 | 16/24/32 | Binary | Random number generated by the IFD or back office system using a TRNG. |
| RND3 | Random Number 3 | 16/24/32 | Binary | String generated by the IFD and ICC separately calculation 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. There are only 3 distinct key sizes allowable by AES. |
| ShillKey | Shill Key (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. ShillKey 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. |

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.

PLAID Version 8 Authentication Protocol

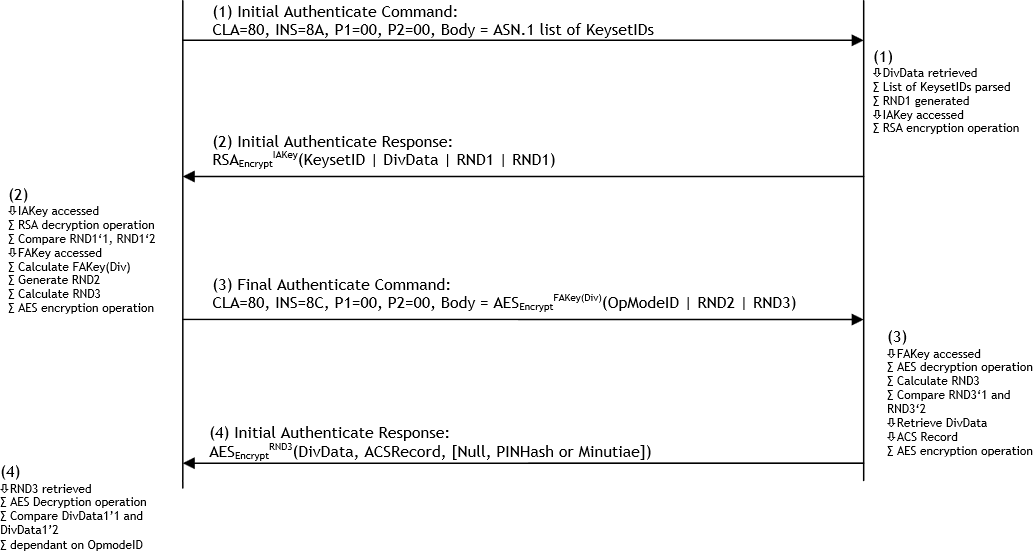


Figure 1 PLAID 8.0 Graphic Overview

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

1. IFD sends the Initial Authenticate command
   * The IFD sends an Initial Authenticate APDU request to the ICC in order to obtain the Diversification Data (DivData). The body of the APDU contains the complete list of authorised KeySetIDs (ASN.1 encoded) that will be acknowledged by the IFD. This list should be ordered with the preferred KeySetID first, followed by lesser preferred KeySetIDs.
     + Note: ASN1 encoding is only used in the body of the Initial Authenticate command as all other transactions are encrypted.
2. ICC responds to the IA command
   * The ICC parses the ASN.1 listing of KeySetIDs and retrieves the first IAKey found which matches a KeySetID supported by the ICC.
   * If none of the KeySetIDs identified in the ASN.1 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.
   * The ICC generates a random value (RND1) using a TRNG. The size of RND1 is identical to the key size of the selected AES cipher (16, 24 or 32 bytes).
   * The ICC retrieves the unique diversification data DivData.
   * The ICC creates the bit string STR1: KeySetID | DivData | RND1 | RND1.
   * The ICC computes the bit string ESTR1 where ESTR1 = RSAEncryptIAKey(STR1). This encryption only uses the modulus and public exponent of the IAKey. Padding (PKCS1.5 or OAEP) should be incorporated into the encryption.
   * The ICC transmits the ESTR1 string to the IFD.
3. The IFD responds to the IA response
   * The IFD calculates STR1 where STR1 = RSA Decrypt IAkey(ESTR1), using the first KeySetID identified in the ASN.1 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 ASN.1 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.
   * The IFD extracts the KeySetID from STR1 to confirm which key set is being used.
     + NOTE: This is necessary since the same asymmetric keys might be used in multiple KeySetIDs for large implementations.
   * The IFD extracts the card’s diversification data from STR1.
   * The IFD generates a random value (RND2) using a TRNG. The size of RND2 is identical to the key size of the selected AES cipher (16, 24 or 32 bytes).
   * The IFD calculates SHA[RND1**|**RND2], the result is denoted as RND3.
   * 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 step 3a/3b).
   * The IFD creates the bit string STR1: OpModeID | RND2 | RND3.
   * The IFD calculates ESTR2 where ESTR2 = AES Encrypt FAKey (Div) (STR2). The cipher mode for this operation must be CBC.
   * The IFD transmits the Final Authenticate string ESTR2 to the ICC.
4. The ICC responds to the FA command
   * The ICC calculates STR2 where STR2 = AES Decrypt FAKey (Div)(ESTR2). The FAKey (Div) to be used is referenced by the KeySetID used in step 2.
   * The ICC calculates RND3 as SHA [RND1|RND2] using RND1 generated in step 2 and RND2 extracted from STR2.
   * The ICC compares RND3 determined in step 4b 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.
   * The ICC retrieves the appropriate fields, based on the OpModeID extracted from STR2.
   * The ICC creates the bit string STR3: DivData | ACSRecord | (Null, PINHash and/or minutiae).
   * The ICC calculates ESTR3 where ESTR3 = AES Encrypt RND3(STR3). The cipher mode for this operation must be CBC.
   * The ICC transmits the Final Authenticate string ESTR3 to the IFD.
5. The IFD processes the credential
   * The IFD calculates STR3 where STR3 = AES Decrypt RND3(ESTR3).
   * The IFD compares the transmitted DivData with the IFD copy received in the Initial Authenticate command. Authentication fails if they do not match.
   * 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 card holder with the SHA PINHash retrieved from STR3. Authentication fails if they do not match.
   * 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.
   * 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.
   * 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. The cipher mode for this operation must be CBC.
6. Key Sets

This specification allows for up to 65535 key sets determined by the two byte KeySetID record. The ICC may therefore support a minimum of two and as many other key sets as is viable given the memory of the ICC. The specification also supports negotiation of key sets, where the IFD, in the Initial Authenticate command, gives the ICC a list of supported key sets, in preference order, and the ICC will utilise the most preferred key set of the set/s it has loaded.

This allows that different levels of trust and interoperability can be achieved depending on the business requirements of the implementation. These might be building, role or function based structuring of key sets, or some combination of these or other factors.

For example, an implementation might utilise the following Keysets:

**Administration** - Keyset = 0 for authentication for administration of the PLAID application only.

**Shared** - Keyset = 1 for authentication to shared public areas of a range of buildings – trusted persons could enter outer perimeter only.

**Physical Access** - Keyset = 2 for authentication to PACS systems within outer perimeter

**Computer room** - Keyset = 3 for authentication for computer room access and highly secure areas with separate PACS system.

**Logical Access** - Keyset = 4 for authentication for system login, printer access, etc.

1. Operational Modes

This specification allows for up to 65535 operational modes determined by the two byte ACS record field sent to the ICC in the Final Authenticate command. Different values for the ACSRecord are subsequently authenticated and returned by the Final Authenticate response. This facility allows that a different and distinct ACS record can be passed to the IFD and backend systems depending on the business requirements for authorisation for the implementation.

For example, an implementation might utilise the following operational modes:

**New Buildings** - ACSRecord = 1 and results in a RFC 4122 based UUID string being returned for authorisation within new building systems.

**Old buildings** - ACSRecord = 2 and results in a 26 bit weigand string being returned for authorisation within older building systems.

**Logical Access** - ACSRecord = 3 and results in a RFC 4122 based UUID string being returned for authorisation to system login, printer access, etc.

**Computer room** - ACSRecord = 4 and results in a RFC 4122 based UUID string being returned for authorisation to computer room access and highly secure areas.

***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.

1. Application Identification

The PLAID application shall be selected either by;

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

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. These commands identify the structure that is transmitted from the IFD to the ICC.

Note: Some implementations may need to use “Envelope” command as specified in ISO/IEC7816-4. For these scenarios, the PLAID operation identifier can be moved from the INS to the body of the APDU, and the INS byte replaced with the value 0xC2.

Table 3: Command Set

| **Operation** | **CLA** | **INS** | **P1 Value** | **P2 Value** | **Body** | **Comments** |
| --- | --- | --- | --- | --- | --- | --- |
| Initial Authenticate | 0x80 | 0x8A | 0x00 | 0x00 | ASN.1 | Only available when card application security state is “PLAID\_SECURED”.  The ASN.1 includes the list of KeySetIDs that will be trusted. |
| Final Authenticate | 0x80 | 0x8C | 0x00 | 0x00 | OpModeID, RND2, RND3 | Only available when card application security state is “PLAID\_SECURED” and the corresponding “INITIAL AUTHENTICATE” command has been successfully completed. |
| Set Data | 0x80 | 0xDB | 0x00 | 0x00 | ASN.1 | Only available when card is state is “PLAID\_UNSECURED” or “FINAL\_AUTHENTICATE” in Administration mode has been successfully completed.  The ASN.1 contains the tag and value for the field to be set. |
| Get Data | 0x80 | 0xCB | 0x00 | 0x00 | ASN.1 |  |

1. Error Codes

In order to protect from ID leakage, and to minimise useful information available to an attacker, an inconsistency or error during a PLAID authentication shall not generate standard ISO/IEC 7816-4 error codes as these indicate that an inconsistency or failed attempt has occurred. Instead, the ICC shall use the ShillKey to complete the operation and return a status word of SW\_OK.

The following ISO/IEC 7816-4 error codes shall however be returned by the PLAID application during PLAID instantiation or if a poorly formatted APDU has been received.

Table 4: PLAID Error Codes (Status Words)

| **Error Code Name** | **Status Word Value** | **Origin** |
| --- | --- | --- |
| SW\_OK | 0x9000 | ISO/IEC |
| SW\_WRONG\_LENGTH | 0x6700 | ISO/IEC |
| SW\_COMMAND\_NOT\_ALLOWED | 0x6986 | ISO/IEC |
| SW\_INS\_NOT\_SUPPORTED | 0x6D00 | ISO/IEC |

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 (DivData)*

1. Session Key Generation

PLAID results in the generation of an AES session key that may optionally be used for subsequent communications with the ICC. The size of this session key is determined by the key size of the AES cipher selected. Currently there are only 3 legitimate key sizes supported by AES (16, 24 or 32 bytes only). 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) = SHA [RND1|RND2o]*

Annex A: Reference Implementation (Informative)

A reference implementation for PLAID 8 will be made available to assist in the comprehensive understanding of how to implement this specification.

The reference implementation may be downloaded from the following link:

[GovDex](https://www.govdex.gov.au)

Select **Centrelink PLAID** from the list of Public GovDex Communities.