HM Government

Protection Profile for UK Dual-Interface Authentication Card

Version 1-0

10th July 2009

Reference: UNKT-DO-0002

Home Office
Identity & Passport Service

Home Office
UK Border Agency

Introduction

This document defines a Protection Profile to express security, evaluation and certification requirements based on Common Criteria (ISO 15408) for a UK-issued dual (contact and contactless) interface card containing a Machine-Readable Travel Document (MRTD), a Cardholder Authentication Application (CAA), and possibly other applications. This Protection Profile captures security requirements that are *in addition* to those contained in separate protection profiles for security ICs [IC PP] and Machine-Readable Travel Documents [MRTD PP], and is therefore intended to apply to products that are also certified against these PPs.

Home Office
Identity & Passport Service

Home Office
UK Border Agency

Summary of Amendments

Version 1-0 10 July 2009

First issued version.

0 Preface

0.1 Related Documents

[9303] ICAO Doc 9303, Sixth Edition, 2007. Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01, 2004, published by authority of the secretary general, International Civil Aviation Organization

This document is also updated by supplementary documents. The latest at the time of writing being:

Supplement to Doc 9303, Release 7, 19 November 2008, ISO/IEC JTC1 SC17 WG3/TF1 for ICAO-NTWG

[CC/1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, CCMB-2006-09-001, v3.1 Release 1, September 2006

[CC/2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2007-09-002, v3.1 Release 2, September 2007

[CC/3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2007-09-003, v3.1 Release 2, September 2007

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, May 2000

[CEM] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, CCMB-2007-09-004, v3.1 Release 2, September 2007

[JIL-AP] Application of Attack Potential to Smartcards, v2.5 Revision 1, April 2008, CCDB-2008-04-001

[MRTD PP] 'Machine Readable Travel Document with "ICAO Application", Extended Access Control', BSI-PP-0026, v1.2, 19th November 2007

[IC PP] Security IC Platform Protection Profile, Eurosmart, BSI-PP-0035, v1.0, 15 June 2007

Note that this PP is a version written for CC version 3.1. The previous version of the PP, written for CC version 2.3, is suitable as an alternative:

Smartcard IC Platform Protection Profile, Eurosmart, BSI-PP-0002, v1.0, July 2001.

[TR-03110] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, 21 February 2008, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI)

A reference of the form [*REF, n*] refers to section *n* of *REF*.

0.2 Glossary

Term	Meaning
Application	A unit of functionality and data that is loaded onto a smart card in order to meet one or more operational uses (e.g. identification and entitlement).
Authentication System	An external system that requests authentication of the person who presents a DIAC, to demonstrate that this person is the rightful Cardholder. The Authentication System communicates with the CAA to request the authentication, and provides a challenge value to the CAA. The CAA, after determining that the correct PIN has been supplied by the Cardholder, will provide a cryptographic response incorporating the challenge (this represents the 'Cardholder authenticated' status to the Authentication System). The Authentication System, on determining that the response is valid and correct, recognises the Cardholder as authenticated.
Blocking History	A Cardholder Authentication Application will enter a 'blocked' state when it receives a number of consecutive incorrect PIN values that exceeds a predefined threshold. When in the blocked state a CAA application will not respond to any requests for Cardholder authentication. The CAA leaves the blocked state (and therefore responds once more to Cardholder authentication requests) after it receives a valid 'unblock' message from a PIN Unblocking Authority. Over its operational lifetime, a CAA will therefore have a sequence of transitions between blocked and unblocked states, and this sequence constitutes the Blocking History of that instance of the CAA. In order to prevent replay attacks, an unblock message must be specific to a point in the Blocking History.
CAA	Cardholder Authentication Application – an application present on the DIAC in order to authenticate a person who presents the card as the rightful Cardholder. When a correct PIN is entered in response to a prompt from the CAA then the CAA will in turn provide a response to a challenge from an Authentication System, and this response message communicates the authenticated status of the Cardholder to the Authentication System.
Cardholder Authentication Application	See CAA.
DIAC	See Dual-Interface Authentication Card.

Term	Meaning
Dual-Interface Authentication Card	The TOE for this protection profile, which is a smart card having both contact and contactless interfaces, and carrying at least an MRTD application and a Cardholder Authentication Application as described in this PP.
EAC	Extended Access Control (see [TR-03110]).
Home Office	The UK Government department that sponsors and issues the DIAC. For these purposes the responsible agencies within the Home Office are the Identity and Passport Service and the UK Border Agency.
IC	Integrated Circuit
ICAO	International Civil Aviation Organisation – for the purposes of this document this refers to the organisation that is responsible for issuing and maintaining the specifications for machine-readable travel documents (e.g. [9303]).
MRTD	Machine-Readable Travel Document (see [9303]).
PIN	Personal Identification Number – a number allocated to a Cardholder to enable authentication of the Cardholder as the person identified by the details on the card (by entry of the PIN into an associated PIN-entry device at an Authentication System).
ST	Security Target – "an implementation-dependent statement of security needs for a specific identified TOE." ([CC/1])
TOE	Target of Evaluation – "a set of software, firmware and/or hardware possibly accompanied by guidance." ([CC/1]) The TOE for this protection profile is the DIAC.
TSF	TOE Security Functionality – "a set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs." ([CC/1])

For other Common Criteria (ISO 15408) terms see [CC/1], [CC/2], [CC/3], & [CEM].

For other terms related to machine-readable travel documents see [MRTD PP, 8] or [9303].

Table of Contents

1. Introduction

1.1 PP Reference Information

Title: Protection Profile for UK Dual-Interface Authentication Card

Version number: 1-0

Sponsoring Organisation: UK Identity and Passport Service

Technical editors: SiVenture

Certification Body: CESG

The minimum assurance level for this PP is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

1.2 Introduction to the Protection Profile

This protection profile describes the requirements for a UK-issued, dual-interface (contact and contactless) smart card containing at least two applications: a machine-readable travel document (ePassport) and a Cardholder Authentication Application (these applications are discussed in more detail in section 1.3.1). This is referred to here as the Dual-Interface Authentication Card (DIAC).

The security evaluation requirements for a machine-readable travel document are specified in [MRTD PP], and the DIAC follows the same lifecycle, but with extensions needed to cover the development, installation and personalisation of the additional application (CAA) covered in this PP (see section 1.3.2). The DIAC also has additional requirements for segregation of applications in the multi-application environment, and for the essential security properties of the Cardholder Authentication Application. The DIAC therefore requires and assumes conformance with [MRTD PP] as well as with this Protection Profile (this requirement is expressed as P.MRTD_PP in section 2.3.1).

The TOE for this PP is a dual-interface card, having both contact and contactless interfaces, whereas [MRTD PP] assumes only a contactless interface. Because the security of both interfaces is significant in this case, the DIAC also requires that the IC used has been certified to be conformant with the Security IC Platform Protection Profile [IC PP], with both interfaces included in the scope of the evaluation. Since [IC PP] does not specify requirements for cryptographic functions, the IC used for the DIAC is also required to include any cryptographic functions used for the DIAC that are implemented in hardware within the scope of this IC evaluation against [IC PP] (these requirements are expressed as P.IC_PP in section 2.3.2).

1.3 TOE Overview

1.3.1 Characteristics of the Card

The DIAC is a multi-application dual-interface smart card containing at least:

- An international machine-readable travel document (MRTD) application implementing Extended Access Control according to [TR-03110] and accessed only via the contactless interface. This application will be used both for national identity verification within the UK and for international travel within the EU.

- A Cardholder Authentication Application accessed only via the contact interface, and requiring the Cardholder to enter a PIN in order to enable the card to engage in a challenge-response protocol with a host system, thus authenticating the Cardholder. This application will be used as a means of establishing identity to UK government.

Other applications may also be present on the card, and there is therefore an essential requirement for segregation of applications so that no application has unauthorised access to the resources of any other application.

1.3.2 Card Lifecycle

The TOE lifecycle is essentially the same as that in [MRTD PP], which divides the lifecycle into 4 phases. These phases are listed below with the extensions needed to deal with the Cardholder Authentication Application (CAA).

- Phase 1 – Development: this is extended to include the development of the CAA.

- Phase 2 – Manufacturing: this is extended to include creation of the CAA

- Phase 3 – Personalisation of the MRTD: this is extended to include personalisation of the CAA, which will include writing any Cardholder-specific data for this application.

- Phase 4 – Operational Use: this is extended to include use and maintenance of the CAA (e.g. preparation and distribution of CAA ‘unblock’ messages).

Cryptographic keys for CAA and the Cardholder PIN value will be inserted into the TOE during one or more of these phases, and the relevant data and phases should be identified in Security Targets claiming conformance with this PP.

It will be decided by the Issuer, on the basis of the mapping of CAA application creation and personalisation to the phases above, which phases will be in the scope of the evaluation of an individual TOE.

1.4 Conformance Claims

This Protection Profile is conformant to the Common Criteria version 3.1 revision 2.

It is CC Part 2 conformant and CC Part 3 conformant.

The Protection Profile requires **demonstrable** conformance according to the definition in [CC/1, Annex D.2], for any ST or PP claiming conformance to this PP.

This PP does not claim conformance to any other PP. However, it assumes that it is used in conjunction with the Machine-Readable Travel Document Protection Profile [MRTD PP] and the Security IC Protection Profile [IC PP].

2. Security Problem Definition

Since the DIAC assumes that the TOE is also certified to be conformant with [MRTD PP] and [IC PP], parts of the security problem related to those Protection Profiles are not repeated here, however the requirement for conformance with these protection profiles is established by organisational security policies (see section 2.3). The security problem definition below focuses on the additional aspects of the security problem arising from the multi-application environment and the Cardholder Authentication Application.

2.1 Assets

The assets to be protected by the TOE are as follows.

- Application data

  The DIAC contains multiple applications, and each application must have control over its own data. The operating system itself will also have data that must not be accessible to the applications, and in this sense the operating system is considered as another application with its own 'application data'. Application data must be protected against unauthorised attempts to read, modify, or use[1] the data.

  For the CAA application in particular, the application data will include cryptographic keys used in the challenge-response protocol with the Authentication System (cf. section 4.1.4), keys used to protect unblocking messages (cf. section 4.1.5), any other keys used to protect PIN values, and the Cardholder's correct PIN value).

- 'Cardholder authenticated' status

  When a Cardholder has supplied a correct PIN during the current session[2], the Cardholder Authentication Application is used to communicate an 'authenticated' status to an external Authentication System. This 'authenticated' status is itself an asset that would be useful to an attacker.

2.2 Users & Subjects

Users of the TOE are either authorised human users, or external IT systems. Subjects are the active components of the TOE that act on behalf of users.

[1] "Use" of data here means that the data may be used without necessarily being known: for example, a private key might be used to sign data, imparting it with an undeserved appearance of authenticity, without the key being known.

[2] A session is defined for these purposes as, at a maximum, the period during which the DIAC remains inserted into a smart card reader. A session may also be shorter than this (e.g. a period between resets even though the card remains in the reader).

2.2.1 Human Users

Cardholder	The Cardholder is the rightful holder of the DIAC, for whom the Issuer personalised the card.
Issuer	The Issuer represents the organisations and individuals involved in personalising and issuing the DIAC[3]. In particular, this involves personalising and issuing the Cardholder Authentication Application.

2.2.2 External IT Systems

Authentication System	An external system that requests authentication of the person who presents a DIAC, to demonstrate that this person is the rightful Cardholder. The Authentication System communicates with the CAA to request the authentication, and provides a challenge value to the CAA. The CAA, after determining that the correct PIN has been supplied by the Cardholder, will provide a cryptographic response incorporating the challenge (this represents the 'Cardholder authenticated' status to the Authentication System). The Authentication System, on determining that the response is valid and correct, recognises the Cardholder as authenticated.
PIN Unblocking Authority	An external system that generates unblocking messages for CAAs that have been blocked due to exceeding the defined threshold for receipt of consecutive incorrect PIN values. The unblocking messages are cryptographically protected to enable the receiving CAA to recognise that they are authentic (i.e. that they originate from the PIN Unblocking Authority), fresh (i.e. that it has been produced for a specific instance of the CAA and to address a specific blocked state in the Blocking History of a specific CAA instance).

2.2.3 Subjects

Application	The DIAC contains at least two separate applications: the MRTD application and the Cardholder Authentication Application. The operating system may also be treated as an application in the context that it may authorise access to its own data to other applications (the operating system has, by definition, authorised access to all other applications' data).

[3] In this respect the Issuer may correspond in certain ways with the Personalisation Agent and/or Manufacturer defined for the MRTD in [MRTD PP, 3.1].

2.3 Organisational Security Policies

2.3.1 P.MRTD_PP MRTD security evaluation

The TOE is required to be certified for conformance with the Machine-Readable Travel Document Protection Profile [MRTD PP], or whatever equivalent may be approved by the UK Home Office at the time of card issuance.

It is noted that [MRTD PP] is based on Common Criteria version 2.3, whereas the current PP uses version 3.1. However, since assurance levels are accepted as being equivalent between the two versions, this does not raise any compatibility problems for the DIAC.

2.3.2 P.IC_PP IC security evaluation

The IC used in the TOE is required to be certified to be conformant with the Security IC Platform Protection Profile [IC PP], or whatever equivalent may be approved by the UK Home Office at the time of card issuance. Both contact and contactless interfaces and all hardware cryptographic functions used in the TOE are required to be in the scope of the evaluation against [IC PP][4].

It is noted that [IC PP] is based on Common Criteria version 3.1, but that an earlier version of that PP based on Common Criteria version 2.3 is also available (see section 0.1). Since assurance levels are accepted as being equivalent between the two versions of Common Criteria, either of these versions of [IC PP] is acceptable for the DIAC.

2.3.3 P.CAA_Personal_Data Data protection in the Authentication System

It is required that the Authentication System protects any of the Cardholder's personal data that it receives, against unauthorised disclosure, modification or use.

2.3.4 P.MRTD_Interface

It is required that the MRTD application is available only over the contactless interface of the DIAC.

2.4 Threats

The threats to the TOE are defined as follows.

[4] It is possible that the cryptographic functions may have been included in a different certification, such as the certification of an operating system, but not in the IC certification. In this case, the separate certification is acceptable provided that it covers the precise cryptographic functions used in implementing the CAA and any supporting functions examined during vulnerability analysis of the DIAC.

2.4.1 T.CAA_Chip_ID Tracking of chip

An attacker may use data provided by the CAA to trace the movements of the Cardholder from a distance. The attacker cannot read the data printed on the DIAC, and does not know in advance the details of the DIAC. (This threat extends T.Chip_ID in [MRTD PP] to cover data available from the CAA.)

2.4.2 T.App_Data_Breach Unauthorised access to application data

An application on the DIAC may gain unauthorised access to the executable code or data of another application on the DIAC.

2.4.3 T.CAA_CH_Masquerade Cardholder masquerade

An attacker may obtain 'Cardholder authenticated' status from the CAA, without correctly authenticating, in order to masquerade as the Cardholder.

2.4.4 T.CAA_Auth_Replay Replay of authentication status message

An attacker may replay to the Authentication System previous authentication details from the CAA in order to misleadingly appear to have 'Cardholder authenticated' status.

2.4.5 T.CAA_PIN_Search Exhaustive search for PIN value

An attacker may attempt to obtain 'Cardholder authenticated' status from the CAA by repeatedly entering possible PIN values for verification by the CAA.

2.4.6 T.CAA_Leakage Leakage of confidential CAA data

Confidential application data held by the CAA (such as private or secret keys, or the Cardholder's correct PIN value) may be revealed to an attacker via side channels (such as timing, power or electromagnetic emanations analysis) or by fault induction attacks. (This threat extends T.Information_Leakage and T.Malfunction in [MRTD PP] to cover secret data used by the CAA.)

2.5 Assumptions

2.5.1 A.CAA_Personalisation Personalisation of the CAA

It is assumed that the Cardholder Authentication Application is correctly and securely loaded and personalised on the DIAC. This includes loading the relevant keys and PIN value, as well as the personal details of the Cardholder. All of these details must be generated, stored and used (e.g. during the personalisation process) in ways that provide adequate protection against disclosure, modification or unauthorised use.

2.5.2 A.CAA_Operation Operation of the CAA infrastructure

It is assumed that the infrastructure for the Cardholder Authentication Application is correctly and securely operated. In particular, the following assumptions are made:

- 'unblock' messages are only issued under authorised circumstances, and applicable to the current point in the Blocking History of a target CAA instance
- the infrastructure will enable any required confirmation that a 'Cardholder authenticated' status received from a DIAC is not only fresh but current[5]
- applications on the DIAC will only be loaded or deleted under the control of the Home Office; any applications approved for load will be reviewed for their security impact on the DIAC, and appropriate measures put in place to preserve the authenticity and integrity of the reviewed application.

[5] The freshness of a 'Cardholder authenticated' status means that it applies to the relevant point in the history of the CAA, i.e. the point at which the Cardholder entered a correct PIN in response to the request from the CAA. For the status to be *current*, it must have been generated at the point in time appropriate to the need for the authentication context in which the status is being used (and not, for example, generated but not used previously and then received and used by the Authentication System in a different context).

3. Security Objectives

3.1 Security Objectives for the TOE

The Security Objectives for the TOE are defined as follows.

3.1.1 O.App_Interfaces Application interface restrictions

The MRTD application shall be available only over the contactless interface of the DIAC, and the CAA shall be available only over the contact interface of the DIAC.

3.1.2 O.App_Segregation Application Segregation

The DIAC shall provide segregation of applications such that no application can gain unauthorised access to the code or data of another application.

3.1.3 O.CAA_CH_Authentication CAA Cardholder authentication

The CAA shall require the Cardholder to enter a PIN assigned by the Issuer in order to achieve 'Cardholder authenticated' status. On receipt of the correct PIN value from the Cardholder, the CAA shall report the 'Cardholder authenticated' status to the Authentication System in a manner that demonstrates the authenticity and freshness of the status message[6].

3.1.4 O.CAA_PIN_failures CAA PIN failures restriction

After receiving a defined number of consecutive incorrect PIN values for authentication, the CAA shall enter a 'blocked' state in which it will not perform Cardholder authentication until after it has received a valid 'unblock' message. (The blocked state shall not affect the functionality of the MRTD application.) After receiving the 'unblock', the CAA shall return to its normal state and shall provide Cardholder authentication.

3.1.5 O.CAA_Leak_Protect CAA data leakage protection

The DIAC shall protect secret data (including private or secret keys, and the Cardholder's correct PIN value) from being revealed via side channels (such as timing, power or electromagnetic emanations analysis) or by fault induction attacks.

[6] The authenticity of the message means that it applies to the claimed Cardholder and originates from the claimed card. The freshness of the messages means that it applies to the relevant (i.e. current) point in the history of the CAA.

3.2 Security Objectives for the Operational Environment

3.2.1 OE.MRTD_PP MRTD PP certification requirement

The TOE shall be certified for conformance with the Machine-Readable Travel Documents Protection Profile [MRTD PP], or whatever equivalent may be approved by the UK Home Office at the time of card issuance.

3.2.2 OE.IC_PP IC PP certification requirement

The IC used in the TOE is required to be certified for conformance with the Security IC Platform Protection Profile [IC PP], or whatever equivalent may be approved by the UK Home Office at the time of card issuance. Both contact and contactless interfaces and all hardware cryptographic functions used in the TOE are required to be in the scope of the evaluation against [IC PP] [7].

3.2.3 OE.CAA_Personalisation CAA secure personalisation

The Issuer shall ensure that the Cardholder Authentication Application is correctly and securely loaded and personalised on the DIAC. This includes loading the relevant keys and PIN value, as well as the personal details of the Cardholder. All of these details shall be generated, stored and used (e.g. during the personalisation process) in ways that provide adequate protection against disclosure, modification or unauthorised use.

3.2.4 OE.CAA_Personal_Data Secure handling of CAA personal data

The Authentication System and its operators shall protect any of the Cardholder's personal data that it receives against unauthorised disclosure, modification or use.

3.2.5 OE.CAA_Operation Secure operation of the CAA infrastructure

The infrastructure for the Cardholder Authentication Application shall be correctly and securely operated. In particular:

- 'unblock' messages shall only be issued under authorised circumstances, and applicable to the current point in the Blocking History of a target CAA instance
- the infrastructure shall enable any required confirmation that a 'Cardholder authenticated' status received from a DIAC is not only fresh but current[5]
- applications on the DIAC shall only be loaded or deleted under the control of the Home Office; any applications approved for load shall be reviewed for their security impact on

[7] As noted for P.IC_PP in section 2.3.2, it is possible that the cryptographic functions may have been included in a different certification, such as the certification of an operating system, but not in the IC certification. In this case, the separate certification is acceptable provided that it covers the precise cryptographic functions used in implementing the CAA and any supporting functions examined during vulnerability analysis of the DIAC.

the DIAC, and appropriate measures shall be put in place to preserve the authenticity and integrity of the reviewed application.

3.3 Security Objectives Rationale

P.MRTD_PP is addressed by OE.MRTD_PP, which specifically requires that the DIAC must also be certified to be conformant with [MRTD PP] or an approved equivalent. Note that some threats in the current PP are related to threats in [MRTD PP][8]:

- T.CAA_Chip_ID extends T.Chip_ID in [MRTD PP] to cover data available from the CAA which might also be used to track a Cardholder

- T.CAA_Leakage extends T.Information_Leakage and T.Malfunction in [MRTD PP] to cover the application of side channel and fault induction attacks to secret data used by the CAA.

P.IC_PP is addressed by OE.IC_PP, which specifically requires that the DIAC must also be certified to be conformant with [IC PP] or an approved equivalent. Note that some threats in the current PP are related to threats in [IC PP], in particular T.CAA_Leakage extends T.Leak-Inherent, T.Leak-Forced, and T.Malfunction in [IC PP][8].

P.CAA_Personal_Data is addressed by OE.CAA_Personal_Data, which specifically requires protection of the relevant personal data in the operation of the Authentication System.

P.MRTD_Interface is addressed by O.App_Interfaces, which ensures that the MRTD application is only available over the contactless interface of the DIAC.

T.CAA_Chip_ID is addressed by O.App_Interfaces, which ensures that the CAA is only available by using the contact interface of the DIAC. This means that an attacker cannot trace the movements of the Cardholder by using the CAA from a distance.

T.App_Data_Breach is addressed by O.App_Segregation, which requires that the TOE provides segregation between applications such that unauthorised access from one application to the code or data of another is not permitted.

T.CAA_CH_Masquerade is addressed by O.CAA_CH_Authentication, which sets a basic requirement for Cardholder to enter a correct PIN value before ‘Cardholder authenticated’ status is granted by the CAA.

[8] The threats identified in the rationale for P.MRTD_PP represent those threats for which the additional presence of the CAA introduces new potential sources of vulnerabilities that would not have been considered during an evaluation against [MRTD PP]. In particular, the CAA adds the potential for different identification data that might be used to track a user – hence the spirit of T.Chip_ID in [MRTD] needs to be extended with T.CAA_Chip_ID here. CAA also adds different embedded software, using different secret data, and hence provides the potential for new sources of side channel and fault induction attacks – hence T.Information_Leakage and T.Malfunction in [MRTD] need to be extended with T.CAA_Leakage. Other threats in [MRTD PP] relating to physical attacks on the chip, such as T.Abuse_Func and T.Phys_Tamper are generic threats: their assessment against the original PP does not depend on the embedded software that operates on the device. Hence these threats do not need to be extended in this PP. A similar argument applies to threats in [IC PP].

T.CAA_Auth_Replay is also addressed by O.CAA_CH_Authentication, which requires that the message conveying the 'Cardholder authenticated' status to the Authentication System implements a method to demonstrate freshness of the message – hence any replayed message would be detected by the Authentication System.

T.CAA_PIN_Search is addressed by O.CAA_PIN_failures, which requires that the DIAC limits the number of consecutive failed authentication attempts that it will accept. OE.CAA_Operation ensures that unblock messages (that could allow an attacker to continue entering PIN attempts by unblocking the application whenever it blocks) are suitably controlled.

T.CAA_Leakage is addressed by O.CAA_Leak_Protect, which requires the DIAC to implement suitable countermeasures against side channel and fault induction attacks[9].

A.CAA_Personalisation is addressed by OE.CAA_Personalisation, which specifically requires correct and secure personalisation of the CAA.

A.CAA_Operation is addressed by OE.CAA_Operation, which specifically requires correct and secure operation of the CAA infrastructure.

The table below summarises the mappings to security objectives in the rationale above.

Assumption, Threat or Organisational Security Policy	Security Objective
P.MRTD_PP	OE.MRTD_PP
P.IC_PP	OE.IC_PP
P.CAA_Personal_Data	OE.CAA_Personal_Data
P.MRTD_Interface	O.App_Interfaces
T.CAA_Chip_ID	O.App_Interfaces
T.App_Data_Breach	O.App_Segregation
T.CAA_CH_Masquerade	O.CAA_CH_Authentication
T.CAA_Auth_Replay	O.CAA_CH_Authentication
T.CAA_PIN_Search	O.CAA_PIN_failures OE.CAA_Operation
T.CAA_Leakage	O.CAA_Leak_Protect

[9] In general this will require the CAA to follow guidance for programmers provided for the operating system and/or the IC.

Assumption, Threat or Organisational Security Policy	Security Objective
A.CAA_Personalisation	OE.CAA_Personalisation
A.CAA_Operation	OE.CAA_Operation

4. Security Requirements

4.1 Security Functional Requirements

The security functional requirements are structured as follows:

- Application interface restrictions: the requirements to use the MRTD application only over the contactless interface and the CAA only over the contact interface are expressed as information flow rules (FDP_IFC.1/App_IF and FDP_IFF.1/App_IF)

- Application segregation: this is expressed as an access control rule (FDP_ACF.1/Multi-App), with a management function in FMT_MOF.1/Multi-App to represent any ability to authorise inter-application access authorisation

- CAA functional requirements: these are divided into 3 aspects:

    - PIN entry for Cardholder authentication (FIA_UAU.1/CAA)

    - Freshness and authenticity of the Cardholder authentication response message (FDP_DAU.1/CAA)

    - CAA blocking (FIA_AFL.1/CAA),

- Side channel protection for the CAA (FDP_IFC.1/CAA)

- Fault-induction protection for the CAA (FPT_FLS.1/CAA and FRU_FLT.2/CAA).

In the statements of security functional requirements, the requirement text is taken from [CC/2], and the following conventions are adopted:

- Where SFRs have been completed, the convention in [MRTD PP] is used: completion text is underlined and the original SFR operation text is recorded in a footnote

- Where refinements have been made that change the *text* of an SFR, these are indicated by using bold font. Other refinements (to the meaning of the SFR) are described under a '*Refinement'* heading.

4.1.1 Application interface restrictions

FDP_IFC.1/App_IF	**Subset information flow control**
Hierarchical to:	No other components.
Dependencies:	FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/App_IF The TSF shall enforce the Application Interface SFP[10] on

- subjects: MRTD application, CAA
- objects: interface used for communication with external entities
- operations: all communication between the MRTD application and external entities, and between CAA and external entities[11].

FDP_IFF.1/App_IF	**Simple security attributes**
Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/App_IF The TSF shall enforce the Application Interface SFP[12] based on the following types of subject and information security attributes:

- subjects: MRTD application, CAA
- information: all data communicated between the MRTD application and external entities, and between the CAA and external entities
- attributes: interface used for communication with external entities[13].

FDP_IFF.1.2/App_IF The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- communications between external entitiesand the MRTD application shall take place only over the contactless interface (and not the contact interface) of the DIAC
- communications between external entitiesand the CAA shall take place only over the contact interface (and not the contactless interface) of the DIAC[14].

FDP_IFF.1.3/App_IF The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

[10] [assignment: *information flow control SFP*]

[11] [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]

[12] [assignment: *information flow control SFP*]

[13] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

[14] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]

FDP_IFF.1.4/App_IF The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorise information flows*].

FDP_IFF.1.5/App_IF The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].

Application Note:

The communications in FDP_IFF.1.2/App_IF relate to communications with external entities and do not include any authorised communications between applications (or between an application and the operating system) on the card (such communications would use internal communications channels mediated by the operating system).

4.1.2 Application Segregation

The following SFRs express the requirement that an application's data should only be accessible to another application if there has been an authorisation step that allows this[15].

FDP_ACC.1/Multi-App	**Subset access control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/Multi-App The TSF shall enforce the Application Segregation SFP[16] on

- subjects: Applications
- objects: all application data
- operations: all[17].

FDP_ACF.1/Multi-App	**Security attribute based access control**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/Multi-App The TSF shall enforce the Application Segregation SFP[18] to objects based on the following:

[15] The mechanism for authorisation is not specified here in order not to unnecessarily constrain implementations.

[16] [assignment: access control SFP]

[17] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

- subjects: Applications
- information: all application data
- attributes: owner of the data[19].

FDP_ACF.1.2/Multi-App The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- access for any operation, by any application to code or data owned by another application shall only be possible if the accessing application has been explicitly authorised for access to the code or data for the operation concerned[20].

FDP_ACF.1.3/Multi-App The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4/Multi-App The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Application Note:

Every item of data shall have an application owner (the owner of an application's code is taken to be the application itself). The method of authorisation should be identified in a Security Target in an Application Note.

FMT_MOF.1/Multi-App	**Management of security functions behaviour**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1/Multi-App The TSF shall restrict the ability to enable[21] the **function** 'authorisation of an application to access the code or data of another application'[22] to [assignment: *the authorised identified roles*].

[18] [assignment: access control SFP]

[19] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

[20] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

[21] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[22] [assignment: *list of functions*]

Application Note:

An implementation of the DIAC may use 'static' properties in the implementation of application segregation. For example, the implementation might prevent *any* access to the code or data of another application. In this case the final assignment of a role in FMT_MOF.1/Multi-App in the ST may be completed with 'None'. The role might alternatively be an off-card role that is not represented by a user or subject defined in this PP (see section 2.2), in which case the ST should add the relevant role as an additional type of user or subject (this applies even if the role is only active during initial creation of the TOE and has no separate role during the operational lifetime of the DIAC).

4.1.3 PIN entry for Cardholder authentication

The SFR below deals with the use of the CAA to provide Cardholder authentication by means of PIN entry. The usual use of this SFR in CC would be as a precursor to giving a user access to other TOE functions, but in this case the authentication is provided by the TOE as a service, and hence the first part of the SFR does not require the TOE to prevent access to other operations before authentication using the CAA (indeed, it must not prevent access to other functions such as the MRTD authentication functions). A refinement is added to the SFR text since this iteration of the SFR applies only to the CAA (a separate use of FIA_UAU.1 is found in [MRTD PP]).

FIA_UAU.1/CAA	**Timing of authentication**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1/CAA The TSF shall allow any TOE operation except provision of a PIN check response by the CAA[23] on behalf of the user to be performed before the user is authenticated **by the Cardholder Authentication Application**.

FIA_UAU.1.2/CAA The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note:

This SFR refers to the use of a PIN verification check by the CAA, which then provides a 'Cardholder authenticated' message intended for the Authentication System, rather than for the TOE. Hence any TOE operation is allowed before PIN authentication, except for an operation that would send a response indicating the result of a PIN check operation. For the purposes of FIA_UAU.1.2/CAA therefore, the only TSF-mediated action remaining is the provision of a PIN check response.

[23] [assignment: list of TSF mediated actions]

4.1.4 Freshness and authenticity of Cardholder authentication response

FDP_DAU.1/CAA	Basic Data Authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_DAU.1.1/CAA The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of PIN verification responses from the Cardholder Authentication Application[24].

FDP_DAU.1.2/CAA The TSF shall provide the Authentication System[25] with the ability to verify evidence of the validity of the indicated information.

Refinement:

"Validity" in this case means the authenticity of the message (to prove that the response comes from a specific, genuine CAA) and freshness (to prove that the message applies to the relevant (i.e. current) point in the history of the CAA).

4.1.5 Cardholder Authentication Application blocking

This SFR deals with the blocking of the CAA after a number of consecutive PIN verification failures.

FIA_AFL.1/CAA	Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/CAA The TSF shall detect when [assignment*: number less than or equal to 9*][26] unsuccessful authentication attempts occur related to PIN verification by the Cardholder Authentication Application [27].

FIA_AFL.1.2/CAA When the defined number of unsuccessful authentication attempts has been surpassed[28], the TSF shall block the Cardholder Authentication Application and prevent

[24] [assignment: list of objects or information types]

[25] [assignment: list of subjects]

[26] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

[27] [assignment: list of authentication events]

[28] [selection: met, surpassed]

further PIN verification attempts until after the receipt of an authentic, fresh 'unblock' message[29].

Application Note:

Only the CAA is blocked when the threshold is exceeded: the MRTD application, for example, shall be unaffected. The 'unblock' message shall be authentic in the sense that the card can prove that it comes from a genuine PIN Unblocking Authority, and fresh in the sense that the CAA can prove that the message applies to the current point in its own Blocking History (and therefore has not been replayed, nor was it originally intended for a different instance of the CAA).

4.1.6 Side channel protection for CAA

Side channels represent ways in which the PIN value, or a cryptographic key value (or other confidential data item), may be gained by an attacker because of correlations between the value of the data item and some observable activity of the DIAC. Typically the observations are related to time taken for processing, power consumed, or electromagnetic radiation emitted.

Since OE.IC_PP requires that the underlying IC has been certified against [IC PP] (including relevant cryptographic algorithms) then some of the side channel protection will have been assessed at the IC level. However, the inclusion of this SFR in the current PP is necessary because some side channel attacks are specific to the software being executed.

In [MRTD PP], the danger of side channels is dealt with using the (part 2 extended) SFR FPT_EMSEC.1 for two specific assets: the Personalization Agent Authentication Key and the Chip Authentication Private Key. For the DIAC, protection needs to be applied to at least the PIN value and CAA (non-public) keys introduced to meet other SFRs in this PP (e.g. for proving the authenticity of PIN verification responses as in section 4.1.4 and PIN unblock messages as in section 4.1.5). The extension in the current PP is made using an approach similar to that of [IC PP]: an information flow policy is defined that requires that confidential data is only to be revealed when (and if) the TOE intends to communicate it – hence any leakage of confidential data would be in breach of the requirement.

FDP_IFC.1/CAA	**Subset information flow control**
Hierarchical to:	No other components.
Dependencies:	FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/CAA The TSF shall enforce the CAA Data Confidentiality Policy[30] on all confidential CAA data when they are processed or transferred internally by the TOE[31].

[29] [assignment: list of actions]

[30] [assignment: *information flow control SFP*]

The CAA Data Confidentiality Policy is defined as follows:

CAA Data Confidentiality Policy: CAA data required to remain confidential (in order for the CAA to successfully implement the SFRs) shall not be accessible from the TOE except when (and if) the TOE software decides to communicate the data via an external interface. The protection shall be applied to confidential data only but without reference to attributes controlled by the TOE software.

Application Note:

The confidential data for the CAA would typically include the Cardholder PIN value, and non-public cryptographic keys to support the freshness and authenticity of both PIN verification check responses (see FDP_DAU.1/CAA in section 4.1.4) and PIN unblock messages (see FIA_AFL.1/CAA in section 4.1.5).

4.1.7 Fault-induction protection for CAA

Confidential data items may be compromised by inducing faults in the operation of the DIAC, so that software execution leads to the secret value being exposed as a result of the faulty behaviour, whether directly (e.g. because the secret value is erroneously transmitted unencrypted over an interface) or indirectly (e.g. where mathematical analysis of erroneous encryption results may enable the unencrypted value to be found).

The following SFRs are used in the same way as in [IC PP], and require protection against fault-induction attacks to be extended to cover the Cardholder Authentication Application.

The essence of the approach is (as described in [IC PP, 6.1]) that FPT_FLS.1 ensures that when the TOE is taken outside its usable limits then it fails securely, while FRU_FLT.2 ensures that when operating within its usable limits then the TOE will handle induced faults (which might include voltage, frequency, or laser-induced faults) securely.

Since OE.IC_PP requires that the underlying IC has been certified against [IC PP] then much of the routine fault-resistance will have been assessed for the IC. However, the inclusion of these SFRs in the current PP is necessary because some fault induction attacks are specific to the software being executed (CAA in this case[32]).

FPT_FLS.1/CAA	**Failure with preservation of secure state**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1/CAA The TSF shall preserve a secure state when the following types of failures occur: exposure to operating conditions which may not be tolerated according to the

[31] [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]

[32] [MRTD PP] also includes FPT_FLS.1 applied to the MRTD application.

requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur[33].

FRU_FLT.2/CAA	**Limited fault tolerance**

Hierarchical to: FRU_FLT.1 Degraded fault tolerance

Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.2.1/CAA The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1)[34].

Application Note:

The Security Target shall define and describe the secure state that is maintained when failures (as defined in both FPT_FLS.1 and FRU_FLT.2) occur.

4.2 Security Functional Requirements Rationale

4.2.1 SFR Dependencies Rationale

The following dependencies arise from the SFRs used:

SFR	Dependencies	Rationale Statement
FDP_IFC.1/App_IF	FDP_IFF.1	Met by FDP_IFF.1/App_IF
FDP_IFF.1/App_IF	FDP_IFC.1	Met by FDP_IFC.1/App_IF
	FMT_MSA.3	Since no attributes used in the SFR are managed or changed (the interface used is implicit), the dependency on FMT_MSA.3 is not necessary.
FDP_ACC.1/Multi-App	FDP_ACF.1	Met by FDP_ACF.1/Multi-App
FDP_ACF.1/Multi-App	FDP_ACC.1	Met by FDP_ACC.1/Multi-App
	FMT_MSA.3	Since no attributes used in the SFR are managed or changed (the ownership attribute is implicit), the dependency on FMT_MSA.3 is not necessary.

[33] [assignment: list of types of failures in the TSF]

[34] [assignment: list of type of failures]

SFR	Dependencies	Rationale Statement
FMT_MOF.1/Multi-App	FMT_SMR.1	The mechanism for authorising access between applications addressed by FMT_MOF.1/Multi-App need not involve roles explicitly recognised by the TSF (as implied in FMT_SMR.1.2). Hence FMT_SMR.1 may not be appropriate and is not included in this PP. An ST author may chose to include it, or to make the authorisation role clear in the ST by some other means.
	FMT_SMF.1	The only management function addressed by FMT_MOF.1/Multi-App is authorisation for access between applications, and this is sufficiently stated and defined by FMT_MOF.1/Multi-App itself and by FDP_ACC.1/Multi-App.
FIA_UAU.1/CAA	FIA_UID.1	The dependency on FIA_UID.1 is not relevant to this instance of the SFR because identification of the Cardholder is implicit in their presentation of the card, and by the fact that the card only holds a single Cardholder PIN reference value.
FDP_DAU.1/CAA	None	
FIA_AFL.1/CAA	FIA_UAU.1	Met by FIA_UAU.1/CAA
FDP_IFC.1/CAA	FDP_IFF.1	As in [IC PP, para 253] the dependency on FDP_IFF.1 is not met, but neither is it necessary in this case. The specification of FDP_IFF.1 would not capture the nature of the security functional requirement nor add any detail. As stated in the CAA Data Confidentiality Policy referred to in FDP_IFC.1 there are no attributes necessary. The security functional requirement for the TOE is sufficiently described using FDP_IFC1 and its CAA Data Confidentiality Policy (FDP_IFC.1).

SFR	Dependencies	Rationale Statement
FPT_FLS.1/CAA	None	
FRU_FLT.2/CAA	FPT_FLS.1	Met by FPT_FLS.1/CAA

4.2.2 SFRs and Objectives Rationale

O.App_Interfaces is implemented by the requirements of FDP_IFC.1/App_IF and FDP_IFF.1/App_IF which require that the MRTD application can only be accessed using the contactless interface, and that the CAA can only be accessed using the contact interface.

O.App_Segregation is implemented by FDP_ACC.1/Multi-App and FDP_ACF.1/Multi-App, which require segregation of application code and data so that access to code or data is only possible if it has been specifically authorised by the owning application. Restriction of the ability to authorise inter-application access (or expression of the absence of any such access mechanism) is specified in FMT_MOF.1/Multi-App.

O.CAA_CH_Authentication is implemented by FIA_UAU.1/CAA and FDP_DAU.1/CAA, which define the need for authentication of the Cardholder (by PIN entry) before issuing a message that represents the Cardholder as authenticated. FDP_DAU.1/CAA ensures that the 'Cardholder authenticated' status conveyed by the DIAC can be recognised by an Authentication System as authentic and fresh.

O.CAA_PIN_failures is implemented by FIA_AFL.1/CAA, which require that the application (and hence the CAA Cardholder authentication function) is blocked if a threshold of consecutive authentication failures is exceeded. The blocked status is reversed on receipt of an authentic and fresh 'unblock' message.

O.CAA_Leak_Protect is implemented by FDP_IFC.1/CAA to protect against side channel attacks on the CAA confidential data, and by FPT_FLS.1/CAA and FRU_FLT.2/CAA to protect against fault-induction attacks on the CAA.

The mapping of objectives to SFRs is summarised in the table below.

Security Objective	SFRs
O.App_Interfaces	FDP_IFC.1/App_IF FDP_IFF.1/App_IF
O.App_Segregation	FDP_ACC.1/Multi-App FDP_ACF.1/Multi-App FMT_MOF.1/Multi-App
O.CAA_CH_Authentication	FIA_UAU.1/CAA FDP_DAU.1/CAA

Security Objective	SFRs
O.CAA_PIN_failures	FIA_AFL.1/CAA
O.CAA_Leak_Protect	FDP_IFC.1/CAA FPT_FLS.1/CAA FRU_FLT.2/CAA

The table below shows how each SFR is derived from a security objective:

SFR	Objectives
FDP_IFC.1/App_IF	O.App_Interfaces
FDP_IFF.1/App_IF	O.App_Interfaces
FDP_ACC.1/Multi-App	O.App_Segregation
FDP_ACF.1/Multi-App	O.App_Segregation
FMT_MOF.1/Multi-App	O.App_Segregation
FIA_UAU.1/CAA	O.CAA_CH_Authentication
FDP_DAU.1/CAA	O.CAA_CH_Authentication
FIA_AFL.1/CAA	O.CAA_PIN_failures
FDP_IFC.1/CAA	O.CAA_Leak_Protect
FPT_FLS.1/CAA	O.CAA_Leak_Protect
FRU_FLT.2/CAA	O.CAA_Leak_Protect

4.3 Security Assurance Requirements

The Security Assurance Requirements for the evaluation of the TOE are those of EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 (all as defined in [CC/3]).

The full list of assurance requirements is therefore as follows:

Security Target evaluation according to ASE requirements for EAL4

> ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1

Lifecycle Support	
Lifecycle Definition	ALC_LCD.1
CM Capabilities	ALC_CMC.4
CM Scope	ALC_CMS.4
Tools and Techniques	ALC_TAT.1
Development Security	ALC_DVS.2
Delivery	ALC_DEL.1
Development	
Architectural Design	ADV_ARC.1
Functional Specification	ADV_FSP.4
TOE Design	ADV_TDS.3
Implementation	ADV_IMP.1
Tests	
Functional Tests	ATE_FUN.1
Coverage	ATE_COV.2
Depth	ATE_DPT.2
Independent Testing	ATE_IND.2
Guidance Documents	
Preparative User Guidance	AGD_PRE.1
Operational User Guidance	AGD_OPE.1
Vulnerability Assessment	
Vulnerability Analysis	AVA_VAN.5

4.3.1 Refinements of the Security Assurance Requirements

AVA_VAN.5 is refined below (in section 4.3.1.1) in order to include a confirmation that the DIAC provides some controls over the loading and deleting of applications on the TOE, limiting the capability to authorised users (or external IT systems). This property is not critical to the TOE[35], but is desirable, and as part of a general analysis of possible vulnerabilities in the TOE it is appropriate to include an extra activity to confirm the presence of controls[36].

[35] The application segregation required by FDP_ACF.1/Multi-App ensures that even if a malicious application were to be installed then it could not compromise the rest of the TOE, and deletion of the MRTD application or CAA would not compromise the security of either system.

[36] The controls over load and delete are not included in the SFRs for the TOE because the criticality of the functionality (and the impact of any potential vulnerabilities) do not merit the full range of evaluation deliverables and activities under ADV, ATE, etc, nor that the controls should necessarily resist High attack potential.

It is noted that in evaluating the requirements of this PP the evaluators may discover properties of the TOE that might represent vulnerabilities concerning other security requirements of the MRTD (or even of the IC platform). Any such discoveries should be reported in the Evaluation Technical Report, and this is formally noted in a further refinement to AVA_VAN.5.

4.3.1.1 Refinement of AVA_VAN.5

AVA_VAN.5 Advanced methodical vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description
ADV_FSP.2 Security-enforcing functional specification
ADV_TDS.3 Basic modular design
ADV_IMP.1 Implementation representation of the TSF
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.5.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.5.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.5.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.5.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.5.3E The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.5.4E The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing High attack potential.

Refinement:

The term “vulnerability analysis” in AVA_VAN.5.3E shall be taken to include, in addition to the normal work units defined in [CEM], the following evaluator activities:

- The evaluators shall confirm, by examination of ADV_FSP deliverables, that the TOE provides the ability to limit any ability to load or delete applications to authorised users

only. The result of this confirmation (including an identification and brief description of the relevant mechanisms) shall be recorded in the Evaluation Technical Report.

- The evaluators shall demonstrate via testing that unauthorised applications cannot be loaded and that unauthorised attempts to delete loaded applications do not succeed. These tests shall be recorded in the Evaluation Technical Report in a manner consistent with tests carried out for ATE_IND.2.3E.

- The evaluators shall also record in the Evaluation Technical Report any properties discovered during evaluation of the DIAC that represent vulnerabilities concerning other security requirements of the MRTD (or even of the IC platform).

Application Note:

The evaluators' work on testing the loading and deleting of applications is intended to utilise an amount of effort consistent with the use of only the ADV_FSP level of deliverable analysis required in the refinement of AVA_VAN.5 above.

4.4 Security Assurance Requirements Rationale

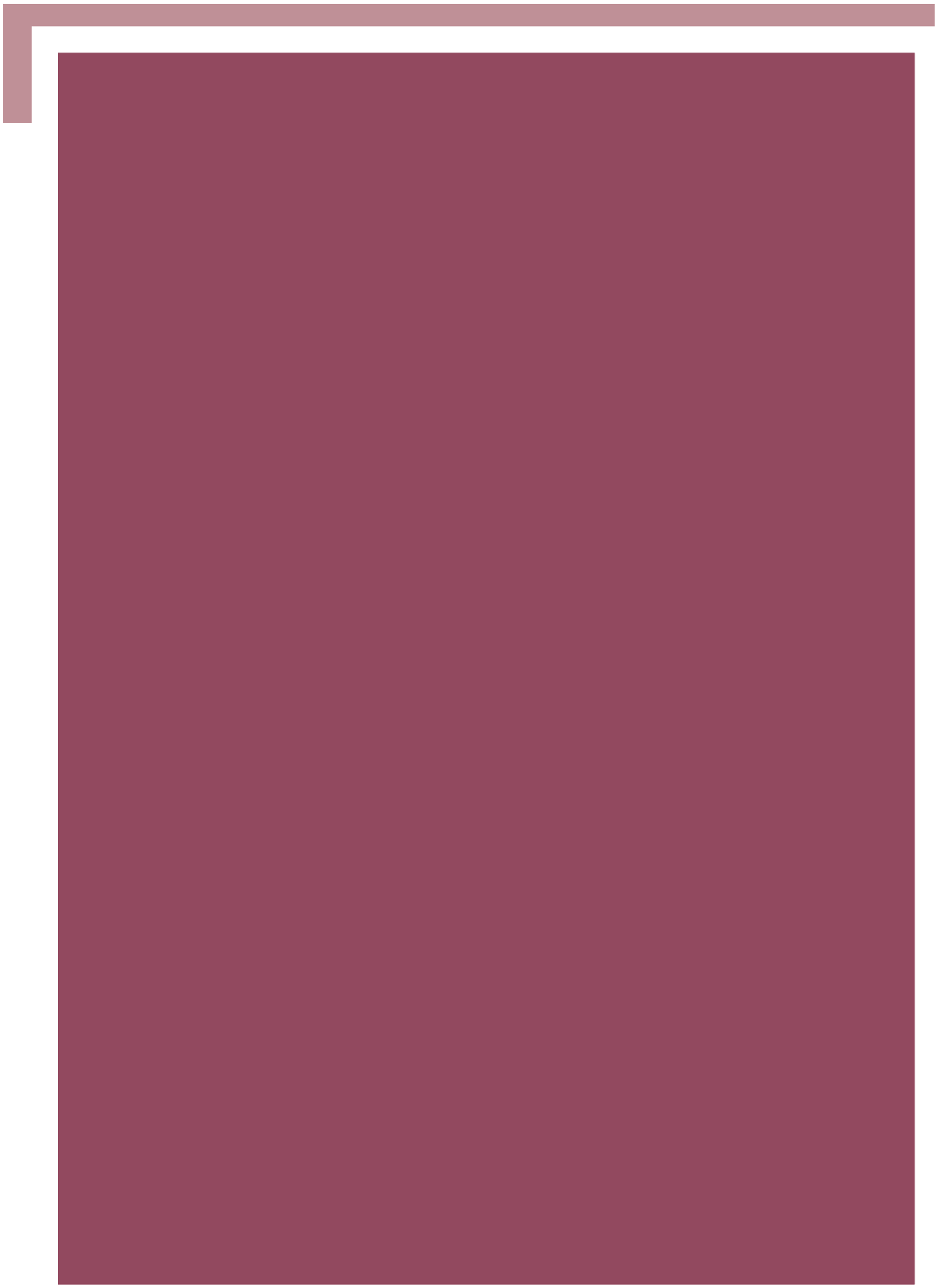
The assurance level chosen for this PP is consistent with the assurance levels and augmentations in [MRTD PP] and [IC PP][37]. This represents a level that maximises the assurance to be gained from good commercial engineering practices at an economically feasible level for this type of TOE.

In addition to the basic EAL4 level, the augmentations are added to increase the assurance gained in areas that are particularly important for this type of TOE:

- ALC_DVS.2 recognises the importance of the secure handling of personal data held on the card, and ensures consistency with the requirements for the MRTD application (ALC_DVS.2 has no dependencies)

- AVA_VAN.5 reflects the uncontrolled environment in which the DIAC is deployed, and hence the exposure to attackers with High attack potential.

[37] [MRTD PP], which was written in conformance to Common Criteria version 2.3, includes the augmentation AVA_MSU.3 which was present in Common Criteria version 2.3 but is not available in version 3.1 because it has been subsumed into the AGD and AVA_VAN requirements. It also includes ADV_IMP.2 in order to ensure that the implementation representation of the entire TSF is available to the evaluators. Under Common Criteria version 3.1 this requirement is included in ADV_IMP.1 and hence the augmentation to ADV_IMP.2 is not required in the current PP.



Home Office
Identity &
Passport Service

Home Office
UK Border Agency