COMMON CRITERIA PROTECTION PROFILE

EPASSPORT WITH BASIC ACCESS CONTROL AND ACTIVE AUTHENTICATION

Draft Version 1.0

TURKISH STANDARDS INSTITUTION

TABLE OF CONTENTS

1. INTRODUCTION

1.1 PP Reference

1.1.1 TITLE

Protection Profile for ePassport with Basic Access Control and Active Authentication

1.1.2 VERSION

Draft Version 1.0

1.1.3 AUTHOR

TURKISH STANDARDS INSTITUTION

1.1.4 PUBLICATION DATE

1.2 TOE OVERVIEW

1.2.1 TOE TYPE

The TOE is the composite smart card product consisting of:

- ePassport Application with BAC[1] and AA[2]
- Embedded OS
- Security IC Unique Identification Data and Configuration Data (optional)
- Secure IC Platform [Secure IC Hardware and IC Dedicated Software]
- Security Guidance Documentation

1.2.2 TOE USAGE AND MAJOR SECURITY PROPERTIES

The TOE is used as an ePassport's chip, as a proof of holder's identity. The TOE's usage is described below[3]:

- A state or an organisation issues an ePassport for the passport holder. The issuing state or organisation ensures the correctness of the data of genuine ePassport's.
- The receiving state trusts a genuine ePassport of an issuing state or organisation.

[1] BAC: Basic Access Control
[2] AA: Active Authentication
[3] From this PP's perspective physical properties of the ePassport that are used to verify the genuineness of the ePassport and the verification of the photograph printed on the ePassport belongs to the passport holder are out of scope.

- The ePassport holder's identity is verified by the receiving state by validating the genuineness of the valid ePassport and verification of the photo stored on the chip belongs to the passport holder[4]

The data structure of the ePassport is named as LDS and defined in [5]. The ePassport offers following security properties: the passive authentication, basic access control and active authentication are also defined in [5]. Passive Authentication is out of this PP's scope. They are ensured by PKI which is operated by states and organisations; key distribution network is maintained by ICAO and participant states and organisation.

The TOE offers following security properties:

- Write once access control to the LDS,
- Basic Access Control,
- Active Authentication,
- Security Management,
- Ability to detect the changes performed during TOE's delivery
- Protection against Physical Attacks,
- Protection against Side Channel Attacks,
- Protection against Environmental Stress Attacks.

1.2.3 REQUIRED NON-TOE HARDWARE/SOFTWARE/FIRMWARE

None

1.2.4 THE TOE LIFE-CYCLE

Life-cycle of the TOE can be divided into two main phases:

- ES Prior Phase
- ES Active System

Embedded operating system prior phase is described in the Security IC PP [6].

ES active phase is where the TOE's legitimate use is performed only through the interfaces provided by ES. ES active phase consists of five phases:

- Activation Phase
- Initialisation Phase
- Personalisation Phase
- Operational Phase
- Death Phase

In the activation phase, the TOE is received from the manufacturer and checked against if it is the genuine TOE. After the originality verification, the Activation Agent (acting on behalf of the Card Issuer) authenticates itself to the TOE, and the Initialisation and Personalisation authentication reference data are written to the TOE. Afterwards the TOE is taken to the initialisation phase.

[4] Additional biometric verification methods (the fingerprint and the iris) are out of the scope of this PP, since they are required to be protected by additional measure: Extended Access Control.

Initialisation phase is when the application specific data are written to the TOE. The phase when each card specific data is written to the TOE is personalisation phase. After the personalisation phase the TOE is taken to the operational phase, in the operational phase the TOE is assumed that it is hostile environment. Death phase is where the TOE stops normal functioning because of its internal secure state is corrupted or authentication attacks are performed during the activation, initialisation or personalisation phases.

1.2.5 THE TOE CONFIGURATIONS

There are two different TOE configurations that depend on the choice of embedded OS storage technology exist in this PP:

- The ROM Based
- The Flash Based

ROM Storage: This configuration requires the Embedded OS to be delivered prior to the manufacturing of the TOE. Embedded OS is stored in the ROM Memory of the TOE and rewrite is not possible.

Flash Storage: Flash Technology enables the embedded OS to be loaded after the TOE is manufactured. There is Flash Loader Software in the TOE within this configuration and provides functionality to load the embedded OS to the Flash Memory. There are several options to load the embedded OS; the manufacturer may load the embedded OS and disable flash loader prior to the delivery to the Card Issuer; or the TOE is delivered without ES and flash loader is active.

Starting from the lifecycles of the different configurations, differences for two configurations exist within this PP. Therefore any TOE that claims conformance to this PP has to state the embedded OS storage technology it supports in the PP conformance statement, whether ***ROM based*** or ***Flash Based***.

The TOE configuration differs in the way that how the embedded operating system is stored or loaded. Embedded operating system can be embedded during the manufacturing by using the Hard ROM masks which are prepared prior to the TOE manufacturing or may be loaded afterwards the manufacturing by a flash loader program if TOE is based on Flash Technology. Usage of Flash or ROM technology changes the lifecycle of the TOE and due to the flexibility the Flash Technology brings there are additional security concerns for the Flash based TOE's. For a TOE that is claiming conformance to this PP, which technology this TOE supports needs to be given in its security target.

Besides the configurations stated in this PP; additional threats, organisational security policies, TOE security objectives and security requirements can be added. Any other addition to the assumptions and environment security objectives requires consistency to other elements of the PP.

Note about the Configurations:

ROM based technology is simpler and the only difference between the ROM based and Flash based TOE is that Flash based TOE's have additional security items. Therefore first the SPD, SOs and SRs of ROM based technology are given afterwards if exist additional items for Flash based TOE are given.

2. CONFORMANCE CLAIMS

2.1 CC CONFORMANCE CLAIM

This Protection Profile claims conformance to the

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 1, September 2012

The

- Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

has to be taken into account

2.2 PP CLAIM

This PP does not claim conformance to any other PP.

2.3 PACKAGE CLAIM

This PP is conforming to assurance package EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC Part 3.

2.4 CONFORMANCE STATEMENT

The Protection Profile requires **strict** conformance for the ST or PP claiming conformance to this PP.

3. SECURITY PROBLEM DEFINITION

3.1 ASSETS AND ACTORS

3.1.1 ASSETS

The primary assets are the LDS, identity of the passport holder and originality of the TOE. The protection of the LDS against unauthorised modification and disclosure; protection of the anonymity of the passport holder and protection of the originality of the TOE are the key security concerns.

The secondary assets are: Unique IC Identification Data, Initialisation and Personalisation Agent Authentication Reference Data, Document Basic Access Keys, Active Authentication Private Key[5], TSF Code and TSF itself.

3.1.2 SUBJECTS AND EXTERNAL ENTITIES

Manufacturer (Composite Product): The roles of the IC Manufacturer, the ES Developer, the ePassport Application developer and the Composite Product Integrator are combined to the single subject within this PP. The TOE defined in the current PP is delivered to the ePassport issuer as a whole product including the ES and the Secure IC.

ePassport Issuer: The ePassport issuer performs all the legitimate security management roles; including activation agent, initialisation agent, personalisation agent, are assumed to be performed on behalf of ePassport issuer.

Activation Agent: The legitimate entity that performs the activation activities.

Initialisation Agent: The legitimate entity that performs the initialisation activities.

Personalisation Agent: The legitimate entity that performs the personalisation activities.

Terminal: The external entity that the TOE communicates with.

Inspection System: An inspection system is the system that verifies the authenticity of the ePassport by the passive authentication mechanism.

Basic Inspection System: It is the technical system that additionally applies the Basic Access Control and additionally may apply the Active Authentication mechanism.

ePassport Holder: ePassport holder is the legitimate holder of the TOE and the subject for whom the TOE is personalised for.

Attacker: The attacker is the entity who tries to undermine the security policies of the issuer state or the receiving state. Attacker is assumed to possess *enhanced basic attack potential*.

3.2 ORGANISATIONAL SECURITY POLICIES

P.BAC: The authentication of BIS, session key generation and secure messaging between the TOE and the BIS will be performed as stated in ICAO Doc 9303 [5].

[5] Active Authentication Public Key is included in the LDS.

P.AA: The active authentication mechanism will be performed as stated in ICAO Doc 9303 [5].

P.Security_Management: The TOE shall support Activation, Initialisation and Personalisation management functions and respective security management roles.

P.IC_Unique_Identification_Data: The TOE should be uniquely identified by the Activation Agent.

ORGANISATIONAL SECURITY POLICY FOR THE FLASH LOADER CONFIGURATION

P.Embedded_OS_Load: The TOE should provide ES loading capability to the ePassport Issuer or the Manufacturer.

3.3 THREATS

3.1.1 EPASSPORT APPLICATION RELATED THREATS:

T.Anonymity_of_the_Holder: An attacker may try to establish communication to the TOE and obtain any information that may be linked to the identity of the passport holder.

T.Unauthorised_Access_to_the_LDS: An attacker may logically access (read or write) to the LDS.

T.Communication: An attacker may eavesdrop the communication between the BIS and the TOE to obtain the LDS.

T.Act_Life_BIS: An attacker may imitate BIS and try to get read access to the LDS.

T.Cloning: An attacker may read out the LDS and produce a cloned ePassport.

T.AA_Key_Disclose: An attacker may logically read the Active Authentication PrK.

3.1.2 ES RELATED THREATS

T.Unauthorised_Management: An attacker may illegitimately manage the TSF.

3.1.3 ATTACKS TO THE HARDWARE PLATFORM

The assets and the property of the asset which are the targets of the physical attacks to the platform are:

- Active Authentication Private Key (read),
- Activation Agent Authentication Reference Data read or manipulation,
- Initialisation and Personalisation Authentication Reference Data read or manipulation
- Document Basic Access Key read or manipulation
- Manipulation to the Authentication Failure Counters

- TSF Operation (manipulation or bypass)

The physical threats to the above assets are given below:

T.Probing_on_Data_Storage: An attacker may physically attack to the memories of the TOE to gain illicit access to the TSF data.

T.Probing_on_Data_Transfer: An attacker may probe the internals of the TOE to gain illicit access to the TSF data.

T.Manipulation_on_Data_Storage: An attacker may physically attack to the memories of the TOE to make changes to the TSF data.

T.Manipulation_on_Data_Transfer: An attacker may physically attack to the internals of the TOE to make changes to the TSF data that is transferred between internal parts of the TOE.

T.Manipulation_on_Execution: An attacker may physically attack to the TSF code operation to bypass the TSF.

T.Manipulation_on_RND: An attacker may physically attack to the random number entropy source to cause the TOE to generate random numbers with insufficient quality.

3.1.4 LEAKAGE AND EMISSION THREATS

T.Information_Leakage_Surface: An attacker may monitor and interpret the emissions emanated from the physical surface of the TOE to disclose the TSF data.

T.Information_Leakage_Side_Channel: An attacker may monitor the power consumption, timing of operation and other observables to interpret and get access to the TSF data.

3.1.5 ENVIRONMENTAL STRESS THREATS

T.Environmental_Stress_Application: Attacker may apply temperature, frequency, voltage outside of the standard operating conditions to force the TOE to malfunction.

3.1.6 FUNCTIONALITY ABUSE THREATS

T.Abuse_of_the_Test_Functions: Attacker may try to use the test functions to gain illicit access to the application data.

3.1.7 THREAT FOR THE FLASH LOADER CONFIGURATION

T.Abuse_of_the_Flash_Loader: Attacker may try to load an unauthentic ES to the ES by using the functionality of the Flash Loader. ***(Applies to the Flash based TOEs)***

3.4 ASSUMPTIONS

A.Personalisation_Agent: It is assumed that the personalisation agent ensures the correctness of the LDS and the Document Basic Access Keys. The personalisation agent generates and signs the Document Security Object correctly.

A.Passive_Authentication: It is assumed that the county signing certificate and private keys, document signer certificates and private keys are securely created, distributed and stored. Electronic signature creation and signature verification processes are functioning correctly.

A.BAC_Keys_Security: It is assumed that the countries generate the Document Basic Access Keys with sufficient strength.

A.Basic_Inspection_System: The Basic Inspection System which has privileges to create secure communication channel with the TOE and read the LDS through this channel and will act in responsive and secure manner. The session keys of the channel and the data read out through the channel will be protected accordingly.

A.Security_Management: The subjects that have the privileges of the security roles and the entities that create and write the authentication reference data and any confidential or integrity sensitive data acts responsively. Any authentication reference data that is created outside of the TOE or exported from the TOE is securely protected outside of the TOE.

4. SECURITY OBJECTIVES

4.1 SECURITY OBJECTIVES FOR THE TOE

4.1.1 APPLICATION SPECIFIC OBJECTIVES

OT.Anonymity: The TOE will not disclose any information that can link with the identity of the ePassport holder before BAC authentication takes place.

OT.BIS_Authentication: The TOE will have BIS authentication mechanism that is compliant with BAC authentication in [5].

OT.Secure_Communication: The TOE will securely communicate (protecting the integrity and confidentiality of the transmitted data) with BIS compliant with [5].

OT.LDS_Access_Control: The TOE will only allow personalisation and initialisation agents to write user data to the TOE. The TOE will allow read access of LDS only to the BIS. The TOE will not allow any write access to the TOE in operational phase.

OT.Active_Authentication: The TOE will have active authentication mechanism compliant with [5] to prove its originality.

OT.AA_PrK_Protection: The TOE will not allow read or write access to the active authentication private key in operational phase.

4.1.2 ES RELATED OBJECTIVES

OT.Security_Management: The TOE must have activation, initialisation and personalisation management functions and protect these functions from abuse. The TOE will not allow writing the TSF data to the unauthorised entities.

4.1.3 PROBING, MANIPULATION AND EMISSION THREATS:

OT.Phy_Data_Access_Control: The TOE must protect the data stored and processed on the TOE from unauthorized access through physical probing. Access to the memories should only be granted via logical interface which is controlled by the embedded operating system. Unauthorized physical access covers the physical probing which may be performed by an attacker.

OT.Data_Integrity: The TOE must detect the physical manipulation of the data stored on the TOE.

OT.Internal_TOE_Transfer_Confidentiality_Protection: The TOE must protect the confidentiality of the data transferred between internal parts of the TOE from probing.

OT.Internal_TOE_Transfer_Integrity_Protection: The TOE must protect the integrity of the transferred data between internal parts of the TOE.

OT.TSF_Operation_Protection: The TOE must have functionality to protect against any manipulation to the TSF operation.

OT.Random_Number_Generation_Protection: The TOE must have functionality to protect the number random number generation functionality.

4.1.4 ENVIRONMENTAL STRESS THREATS

OT.Environmental_Stress_Protection: The TOE must have mechanism(s) to protect the TSF from environmental stress.

4.1.5 LEAKAGE THREATS

OT.Side_Channel_Protection: The TOE must have protection against T.Information_Leakage_Side_Channel.

4.1.6 ABUSE OF THE FUNCTIONALITY

OT.Test_Functions_Disable_Mechanism: The TOE must have mechanism allowing the manufacturer to irreversibly disable the test functionality.

4.1.7 UNIQUE IDENTIFICATION

OT.Unique_ID_Storage: The TOE must have functionality to store Unique Identification Data. This data should only be writable by the manufacturer.

ADDITIONAL OBJECTIVES FOR THE FLASH LOADER CONFIGURATION

OT.Flash_Loader_Functionality: The TOE must have embedded operating system loading functionality.

OT.Flash_Loader_Authorization: The TOE must allow only authenticated entities to use the flash loader.

OT.Flash_Loader_Disable_Mechanism: The TOE must have mechanism allowing the manufacturer and/or the card issuer to irreversibly disable the flash loader functionality.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

OE.Personalisation_Agent: It is assumed that the personalisation agent ensures the correctness of the LDS and the Document Basic Access Keys. The personalisation agent generates and signs the Document Security Object correctly.

OE.Passive_Authentication: The country signing certificate and private keys, document signer certificates and private keys are securely created, distributed and stored. Electronic signature creation and signature verification processes are functioning correctly.

OE.BAC_Keys_Security: The countries will generate the Document Basic Access Keys with sufficient strength.

OE.Basic_Inspection_System: The Basic Inspection System which has privileges to create secure communication channel with the TOE and read the LDS through this channel and will act in responsive and secure manner. The session keys of the channel and the data read out through the channel will be protected accordingly. The Basic Inspection System will use the Active Authentication process.

OE.Security_Management: The subjects that have the privileges of the security roles and the entities that create and write the authentication reference data and any confidential or integrity sensitive data acts responsively. Any authentication reference data that is created outside of the TOE or exported from the TOE is securely protected outside of the TOE.

OE.Test_Functions_Disable: The manufacturer must ensure that for every TOE before delivery, test functionality has been disabled.

OE.Unique_Identification: The manufacturer must use the unique ID storage mechanism of the TOE properly. The manufacturer must ensure that IDs written to the TOEs are unique.

ADDITIONAL OBJECTIVES FOR THE FLASH LOADER CONFIGURATION

OE.Flash_Loader_Disable: Depending on the life-cycle of the TOE, whether the manufacturer or the card issuer must ensure that any TOE that will be delivered; the flash loader functionality had been disabled.

4.3 SECURITY OBJECTIVES RATIONALE

4.3.1 SECURITY OBJECTIVES RATIONALE TABLE

	OT.Anonymity	OT.BIS_Authentication	OT.Secure_Communication	OT.LDS_Access_Control	OT.Active_Authentication	OT.AA_PrK_Protection	OT.Security_Management	OT.Phy_Data_Access_Control	OT.Data_Integrity	OT.Internal_TOE_Transfer_Confidentiality_Protection	OT.Internal_TOE_Transfer_Integrity_Protection	OT.TSF_Operation_Protection	OT.Random_Number_Generation_Protection	OT.Environmental_Stress_Protection	OT.Side_Channel_Protection	OT.Test_Functions_Disable_Mechanism	OT.Unique_ID_Storage	OE.Personalisation_Agent	OE.Passive_Authentication	OE.BAC_Keys_Security	OE.Basic_Inspection_System	OE.Security_Management	OE.Test_Functions_Disable	OE.Unique_Identification
1. P.BAC		✓	✓																				
2. P.AA					✓																		
3. P.Security_Management							✓																
4. P.IC_Unique_Identification_Data																	✓						✓
5. T.Anonymity_of_the_Holder	✓																						
6. T.Unauthorised_Access_to_the_LDS				✓																			
7. T.Communication			✓																		✓		
8. T.Act_Life_BIS		✓																		✓			
9. T.Cloning					✓																✓		
10. T.AA_Key_Disclose						✓																	
11. T.Unauthorized_Management							✓															✓	
12. T.Probing_on_Data_Storage								✓															
13. T.Probing_on_Data_Transfer										✓													
14. T.Manipulation_on_Data_Storage								✓	✓														
15. T.Manipulation_on_Data_Transfer										✓	✓												
16. T.Manipulation_on_Execution												✓											
17. T.Manipulation_on_RND													✓										
18. T.Information_Leakage_Surface										✓													
19. T.Information_Leakage_Side_Channel															✓								
20. T.Environmental_Stress_Application														✓									
21. T.Abuse_of_the_Test_Functions																✓						✓	
22. A.Personalisation_Agent																		✓					
23. A.Passive_Authentication																			✓				
24. A.BAC_Keys_Security																				✓			
25. A.Basic_Inspection_System																					✓		
26. A.Security_Management																						✓	

Table 1: Security Objectives Rationale

Additional Rationale for the Flash Loader Configuration

1.	P.Embedded_OS_Load	OT.Flash_Loader_Functionality
2.	T.Abuse_of_the_Flash_Loader	OT.Flash_Loader_Authorization, OT.Flash_Loader_Disable_Mechanism, OE.Flash_Loader_Disable

Table 2: Additional Rationale for the Flash Loader

4.3.2 SECURITY OBJECTIVES JUSTIFICATION

— **P.BAC**

The OT.BIS_Authentication and OT.Secure_Communication define the BIS authentication and secure communication between the BIS and the TOE as stated in P.BAC. OT.BIS_Authentication and OT.Secure_Communication cover the policy.

Security Objectives: OT.BIS_Authentication, OT.Secure_Communication

— **P.AA**

The OT.Active_Authentication reflect the P.AA as it is.

Security Objective: OT.Active_Authentication

— **P.Security_Management**

The OT.Security_Management cover the P.Security_Management.

Security Objective: OT.Security_Management

— **P.IC_Unique_Identification_Data**

OT.Unique_ID_Storage enables the TOE to have ID storage capability and OE.Unique_Identification requires that manufacturer creates a unique identification data for the TOE and writes it to the TOE before delivery to the card issuer. So OT.Unique_ID_Storage and OE.Unique_Identification cover the P.IC_Unique_Identification_Data

Security Objectives: OT.Unique_ID_Storage, OE.Unique_Identification

— **P.Embedded_OS_Load**

OT.Flash_Loader_Functionality covers the policy P.Embedded_OS_Load.

Security Objective: OT.Flash_Loader_Functionality

- **T.Anonymity_of_the_Holder**

The OT.Anonymity prevents the leakage of any information that can be linked to the epassport holder and so cover the threat.

Security Objective: OT.Anonymity

- **T.Unauthorised_Access_to_the_LDS**

OT.LDS_Access_Control defines who can access to the LDS and prevents from any unauthorised access to the LDS.

Security Objectives: OT.LDS_Access_Control

- **T.Communication**

OT.Secure_Communication and OE.Basic_Inspection_System together perform the secure communication between the TOE and the BIS and protect the communication channel from eavesdropping and manipulation attacks.

Security Objectives: OT.Secure_Communication, OE.Basic_Inspection_System

- **T.Act_Life_BIS**

OT.BIS_Authentication provides the authentication of the BIS and protects from attacks BIS masquareding attacks. OE.BAC_Keys_Security provides the security of the authentication reference data used to authenticate the BIS.

Security Objectives: OT.BIS_Authentication, OE.BAC_Keys_Security

- **T.Cloning:**

Active authentication mechanism prevents the TOE from cloning. OE.Basic_Inspection_System uses the mechanism to verify the originality of the TOE and OT.Active_Authentication enables the mechanism in the TOE.

Security Objectives: OT.Active_Authentication, OE.Basic_Inspection_System

- **T.AA_Key_Disclose:**

OT.AA_PrK_Protection protects the active authentication key from attacker accessing through the logical interface.

Security Objectives: OT.AA_PrK_Protection

- **T.Unauthorized_Management:**

OT.Security_Management puts the management functions and management roles and necessary authentication mechanisms in place. OE.Security_Management protects the authentication reference data of the authentication mechanisms. So the objectives OT.Security_Management and OE.Security_Management address the threat.

Security Objectives: OT.Security_Management, OE.Security_Management

- **T.Probing_On_Data_Storage**

OT.Phy_Data_Access_Control protects the data stored and processed on the TOE from physical probing; and so the objective OT.Phy_Data_Access_Control counters the threat T.Probing_On_Data_Storage.

Security Objective: OT.Phy_Data_Access_Control

- **T.Probing_on_Data_Transfer**

OT.Internal_TOE_Transfer_Confidentiality_Protection protects the confidentiality of the transferred data between internals of the TOE; and so it covers the threat T.Probing_on_Data_Transfer.

Security Objective: OT.Internal_TOE_Transfer_Confidentiality_Protection

- **T.Manipulation_on_Data_Storage**

OT.Data_Integrity protects the integrity of the data stored and processed on the TOE from physical manipulation. And the OT.Phy_Data_Access_Control protects against reading the data, prevents the attacker knowing the physical location and content of the data. So with OT.Phy_Data_Access_Control, even if OT.Data_Integrity does not exist; an attacker may manipulate the data and can not foresee the changes he or she makes. OT.Data_Integrity and OT.Phy_Data_Access_Control cover this threat.

Security Objective: OT.Phy_Data_Access_Control, OT.Data_Integrity

- **T.Manipulation_on_Data_Transfer**

OT.Internal_TOE_Transfer_Integrity_Protection protects the integrity of the data transferred between internal parts of the TOE from physical manipulation. And the OT.Internal_TOE_Transfer_Confidentiality_Protection prevents the attacker from compromising the data in transfer so making reasonable changes is not possible. So with OT.Internal_TOE_Transfer_Confidentiality_Protection, even if OT.Internal_TOE_Transfer_Integrity_Protection does not exist; an attacker may manipulate the data and can

not foresee the changes he or she makes. OT.Internal_TOE_Transfer_Confidentiality_Protection and OT.Internal_TOE_Transfer_Integrity_Protection cover this threat.

Security Objectives: OT.Internal_TOE_Transfer_Integrity_Protection, OT.Internal_TOE_Transfer_Confidentiality_Protection

- **T.Manipulation_on_Execution**

OT.TSF_Operation_Protection protects the CPU operations from manipulation. So the objective OT.TSF_Operation_Protection covers T.Manipulation_on_Execution.

Security Objective: OT.TSF_Operation_Protection

- **T.Manipulation_on_RND**

OT.Random_Number_Generation_Protection protects the Random Number Generation functionality from manipulation. So the objective OT.Random_Number_Generation_Protection covers T.Manipulation_on_RND.

Security Objective: T.Manipulation_on_RND

- **T.Information_Leakage_Surface**

OT.Internal_TOE_Transfer_Confidentiality_Protection, protects the confidentiality of the transferred data, so interpretation of the emissions is not possible. OT.Internal_TOE_Transfer_Confidentiality_Protection covers this threat.

Security Objective: OT.Internal_TOE_Transfer_Confidentiality_Protection

- **T.Information_Leakage_Side_Channel**

OT.Side_Channel_Protection covers the threat T.Information_Leakage_Side_Channel.

Security Objective: OT.Side_Channel_Protection

- **T.Environmental_Stress_Application**

OT.Environmental_Stress_Protection covers the T.Environmental_Stress_Application.

Security Objective: OT.Environmental_Stress_Protection

- **T.Abuse_of_the_Test_Functions**

OT.Test_Functions_Disable_Mechanism and OE.Test_Functions_Disable cover the threat.

Security Objective: OT.Test_Functions_Disable_Mechanism, OE.Test_Functions_Disable

- **T.Abuse_of_the_Flash_Loader**

OT.Flash_Loader_Authorization prevents the usage of Flash Loader by unauthorized entities, so even if during delivery or within the card issuer facility attacker accesses to the TOE, he or she will not be able to use the flash loader to load an unauthentic embedded operating system. OT.Flash_Loader_Disable_Mechanism enables the manufacturer or the card issuer to disable the flash loader functionality irreversebly. OE.Flash_Loader_Disable declares that the manufacturer or the card issuer (depending on the life-cycle model) to disable the flash loader before delivery from their facility. So the objectives OT.Flash_Loader_Authorization, OT.Flash_Loader_Disable_Mechanism, and OE.Flash_Loader_Disable together covers this threat.

Security Objective: OT.Flash_Loader_Authorization, OT.Flash_Loader_Disable_Mechanism, OE.Flash_Loader_Disable

- **A.Personalisation_Agent**

OE.Personalisation_Agent covers the assumption.

Security Objective: OE.Personalisation_Agent

- **A.Passive_Authentication**

OE.Passive_Authentication covers the assumption.

Security Objective: OE.Passive_Authentication

- **A.BAC_Keys_Security**

OE.BAC_Keys_Security covers the assumption.

Security Objective: OE.BAC_Keys_Security

- **A.Basic_Inspection_System**

OE.Basic_Inspection_System covers the assumption.

Security Objective: OE.Basic_Inspection_System

- **A.Security_Management**

OE.Security_Management covers the assumption.

Security Objective: OE.Security_Management

5. EXTENDED COMPONENTS

Following components are added:

- FCS_RND.1
- FIA_POI.1
- FPT_SCP.1

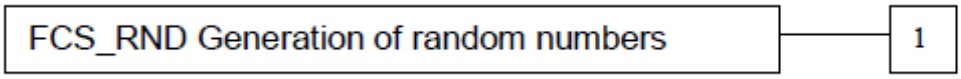
5.1 CLASS FCS CRYPTOGRAPHIC SUPPORT

FAMILY FCS_RND GENERATION OF RANDOM NUMBERS

Family behavior

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component leveling:



FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 **Quality metric for random numbers**

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric].

5.2 DEFINITION OF THE FAMILY FIA_POI

FIA_POI ABILITY TO PROVE ITS OWN IDENTITY

Family Behavior:

This family requires that the TOE has ability to prove its own identity to the external entities.

Component Leveling

FIA_POI Ability to Prove Its Own Identity	1

FIA_POI.1 Ability to Prove Its Own Identity

Management: FIA_POI.1

The following actions could be considered for the management functions in FMT:

a) management of authentication data by an administrator

Audit: FIA_POI.1

a) Minimal: The final decision on authentication;

FIA_POI.1 Ability to Prove Its Own Identity

Hierarchical to: No other components

Dependencies: No dependencies

FIA_POI.1.1 The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or role] to the [assignment: external entity].

5.3 CLASS FPT PROTECTION OF THE TSF

FAMILY FPT_SCP SIDE CHANNEL PROTECTION

The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2.

The family "Side Channel Protection (FPT_SCP)" is specified as follows.

Family behavior:

This family defines requirements to mitigate information leakage through time and power analysis.

Component leveling:

FPT_SCP: Side Channel Protection — 1

FPT_SCP.1 Side channel protection requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_SCP.1

There are no management activities foreseen.

Audit: FPT_SCP.1

There are no actions defined to be auditable.

FPT_SCP.1 Side Channel Protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SCP.1 The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

6. SECURITY REQUIREMENTS

6.1 SECURITY FUNCTIONAL REQUIREMENTS

6.1.1 LOGICAL DATA ACCESS CONTROL

Logical data access control is covered by two policies: ***Pre-Operational Data Access Control Policy*** and ***ePassport Data Access Control Policy***. . Pre-operational data access control policy is the policy that enables the activation, initialisation and personalisation of the TOE. Application data access control policy is active during operational phase and consists of rules of the application.

6.1.1.1 PRE-OPERATIONAL DATA ACCESS CONTROL POLICY

Pre-operational data access policy is related with the embedded operating system; this policy protects the application data during pre-operational phases.

FDP_ACC.1/Pre-Operational **Subset access control – Pre-Operational Access Control**

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control ***fulfilled*** by FDP_ACF.1/Pre-Operational

FDP_ACC.1.1 The TSF shall enforce the *Pre-Operational Data Access Control SFP*[6] on *attacker, initialization agent, personalisation agent, LDS and read, write, delete operations*[7].

FDP_ACF.1/Pre-Operational **Security attribute based access control – Pre-Operational Access Control**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control ***fulfilled*** by FDP_ACC.1/Pre-Operational

FMT_MSA.3 Static attribute initialization ***not fulfilled*** but justified

FDP_ACF.1.1 The TSF shall enforce the *Pre-Operational Data Access Control SFP*[8] to objects based on the following: *initialization agent, personalisation agent, LDS, subject identity and lifecycle phase*[9].

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

- *if the life-cycle phase is at initialisation phase and the subject is initialisation agent access to the LDS is granted*
- *if the life-cycle phase is at personalisation phase and the subject is personalisation agent access to the LDS is granted*[10].

[6] [assignment: access control SFP]
[7] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[8] [assignment: access control SFP]
[9] [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]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[11].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[12].

6.1.1.2 EPASSPORT DATA ACCESS CONTROL POLICY

When the TOE is in the operational phase the ePassport data access control policy (BAC policy) will be active. Writing to the LDS will not be allowed, read access will be granted only to the BIS.

FDP_ACC.1/BAC Subset access control – Basic Access Control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control ***fulfilled*** by FDP_ACF.1/Application

FDP_ACC.1.1 The TSF shall enforce the *Basic Access Control SFP*[13] on *BIS*, *LDS*, and *read, write, delete operations*[14].

FDP_ACF.1/BAC Security attribute based access control – Basic Access Control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control ***fulfilled*** by FDP_ACC.1/Application

FMT_MSA.3 Static attribute initialization ***not fulfilled*** but justified

FDP_ACF.1.1 The TSF shall enforce the *Basic Access Control SFP*[15] to objects based on the following: *BIS, LDS, subject identity and lifecycle phase*[16].

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

- [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects][17].

---

[10] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[11] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[12] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[13] [assignment: access control SFP]
[14] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[15] [assignment: access control SFP]
[16] [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]
[17] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[18].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[19].

6.1.2 PHYSICAL DATA ACCESS CONTROL POLICY

Probing threat can be modelled as the attacker tries to access to the physical memories and/or tries to monitor data traffic between the internal parts of the TOE. The security objectives "Data Access Control", and "Internal TOE Transfer Confidentiality Protection" states that the TOE should provide protection against this kind of threat. These objectives can be achieved by the enforcement of the ***Physical Data Access Policy*** which briefly states: "The TSF shall not allow only the attacker to physically access all data stored on memories and transmitted between internal parts of the TOE".

Physical Data Access Policy is enforced by the three SFRs: FDP_ACC.1/Physical, FDP_ACF.1/Physical and FDP_ITT.1. Both FDP_ACF.1 and FDP_ITT.1 are performing the denial of access to the attacker by encrypting the data and allowing access to the embedded operating system by decrypting it. So they depend on the cryptographic operations (key generation, encryption and decryption, key destruction). FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 is also added to the Protection against Probing SFRs.

FDP_ACC.1/Physical Subset access control – Physical Access Control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control ***fulfilled*** by FDP_ACF.1/Physical

FDP_ACC.1.1 The TSF shall enforce the *Physical Data Access Control SFP* [20] on *attacker, application data and physical access*[21].

FDP_ACF.1/Physical Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control ***fulfilled*** by FDP_ACC.1/Physical

FMT_MSA.3 Static attribute initialisation ***not fulfilled*** but justified

FDP_ACF.1.1 The TSF shall enforce the *Physical Data Access Control SFP*[22] to objects based on the following: *Attacker and Application Data, type of user*][23].

[18] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[19] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[20] [assignment: access control SFP]
[21] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[22] [assignment: access control SFP]

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

- *Physical access is not allowed to the attacker*[24]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[25].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *if the subject is attacker the physical access is explicitly denied*.[26]

FDP_ITT.1 Basic internal transfer protection

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/Physical

FDP_ITT.1.1 The TSF shall enforce the *Physical Data Access Policy*[27] to prevent the *disclosure, and modification*[28] of user data when it is transmitted between physically-separated parts of the TOE.

FDP_ITT.1 also prevents any confidential data leak through emanations through the physical surface of the IC.

6.1.2.1 CRYPTOGRAPHIC SUPPORT TO DATA ACCESS CONTROL AND TRANSFER PROTECTION

FCS_CKM.1/SP Cryptographic key generation – Storage Protection

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation] fulfilled by FCS_COP.1/SP

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm][29] and specified

[23] [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]
[24] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[25] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[26] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].
[27] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[28] [selection: disclosure, modification, loss of use]
[29] [assignment: cryptographic key generation algorithm]

cryptographic key sizes [assignment: cryptographic key sizes][30] that meet the following: [assignment: list of standards][31].

FCS_CKM.1/TP Cryptographic key generation – Transfer Protection

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation] fulfilled by FCS_COP.1/TP

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm][32] and specified cryptographic key sizes [assignment: cryptographic key sizes][33] that meet the following: [assignment: list of standards][34].

FCS_CKM.4/IC Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method][35] that meets the following: [assignment: list of standards][36].

FCS_COP.1/SP Cryptographic operation – Storage Protection

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/SP

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4

[30] [assignment: cryptographic key sizes]
[31] [assignment: list of standards]
[32] [assignment: cryptographic key generation algorithm]
[33] [assignment: cryptographic key sizes]
[34] [assignment: list of standards]
[35] [assignment: cryptographic key destruction method]
[36] [assignment: list of standards]

FCS_COP.1.1 The TSF shall perform *encryption and decryption* [37] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm][38] and cryptographic key sizes [assignment: cryptographic key sizes] [39] that meet the following: [assignment: list of standards][40].

FCS_COP.1/TP Cryptographic operation – Transfer Protection

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/TP

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4

FCS_COP.1.1 The TSF shall perform *encryption and decryptio*[41] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm][42] and cryptographic key sizes [assignment: cryptographic key sizes][43] that meet the following: [assignment: list of standards][44].

FPT_SCP.1/IC Side Channel Protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SCP.1 The TSF shall ensure *attackers*[45] are unable to use the following interface *physical contacts*[46] to gain access to *Data Storage Protection keys, Data Transfer Protection keys*[47] and *Stored Data and Transferred Data*[48].

6.1.3 SECURE COMMUNICATION

FDP_UCT.1 Basic Data Exchange Confidentiality

[37] [assignment: list of cryptographic operations]
[38] [assignment: cryptographic algorithm]
[39] [assignment: cryptographic key sizes]
[40] [assignment: list of standards]
[41] [assignment: list of cryptographic operations]
[42] [assignment: cryptographic algorithm]
[43] [assignment: cryptographic key sizes]
[44] [assignment: list of standards]
[45] [assignment: type of users]
[46] [assignment: type of connection]
[47] [assignment: list of types of TSF data]
[48] [assignment: list of types of user data]

Hierarchical to: No other components

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] ***not fulfilled*** but justified

[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] ***fulfilled*** by FDP_ACC.1/BAC

FDP_UCT.1.1 The TSF shall enforce the *Basic Access Control SFP*[49] to *transmit and receive* [50]user data in a manner protected from unauthorised disclosure.

FDP_UIT.1 Data Exchange Integrity

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] ***fulfilled*** by FDP_ACC.1/BAC

[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] ***not fulfilled*** but justified

FDP_UIT.1.1 The TSF shall enforce the *Basic Access Control SFP*[51] to *transmit and receive* [52]user data in a manner protected from [selection: modification, deletion, insertion, replay][53] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion and replay*[54] has occurred.

6.1.4 CLASS FIA IDENTIFICATION AND AUTHENTICATION

6.1.4.1 OT.ANONYMITY

FIA_UID.1/Operational Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow *none*[55] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[49] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[50] [selection: transmit, receive]
[51] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[52] [selection: transmit, receive]
[53] [selection: modification, deletion, insertion, replay]
[54] [selection: modification, deletion, insertion, replay]
[55] [assignment: list of TSF-mediated actions]

FIA_UAU.1/Operational Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification fulfilled by FIA_UID.1/Operational

FIA_UAU.1.1 The TSF shall allow *none*[56] on behalf of the user to be performed before the user is authenticated.

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

Application Note: The TOE shall not give out any information that can be linked to the identity of the Passport Holder. The TOE will generate a random identifier to initiate the contactless communication.

6.1.4.2 OT.ACTIVE_AUTHENTICATION

FIA_POI.1 Ability to Prove Its Own Identity

Hierarchical to: No other components

Dependencies: No dependencies

FIA_POI.1.1 The TSF shall provide an *Active Authentication mechanism*[57] to prove the identity of the *ePassport*[58] to the *BIS*[59]

6.1.4.3 ACCESS BEFORE IDENTIFICATION AND AUTHENTICATION

FIA_UID.1/Pre-Operational Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow *IC Identification data write and read; and Test Functions disable*[60] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[56] [assignment: list of TSF mediated actions]
[57][assignment: *authentication mechanism*]
[58][assignment: *authorized user or role*]
[59][assignment: external entity]
[60] [assignment: list of TSF-mediated actions]

FIA_UAU.1/Pre-Operational Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification fulfilled by FIA_UID.1

FIA_UAU.1.1 The TSF shall allow *IC Identification data write and read; Test Functions disable*[61] on behalf of the user to be performed before the user is authenticated.

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

6.1.4.4 AUTHENTICATION MECHANISMS

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to *BIS Authentication Mechanism*[62]

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

- *Flash Loader Authentication Mechanism**
- *Activation Agent Authentication Mechanism*
- *Initialisation Agent Authentication Mechanism*
- *Personalisation Agent Authentication Mechanism*
- *BIS Authentication Mechanism*[63]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the

- *Flash Loader Authentication Mechanism authenticates the Card Issuer or the Manufacturer**
- *Activation Agent authenticates mechanism the Activation Agent*
- *Initialisation Agent Authentication mechanism authenticates the Initialisation Agent*
- *Personalisation Agent Authentication mechanism authenticates the Personalisation Agent*
- *BIS Authentication mechanism authenticates the BIS*[64]

[61] [assignment: list of TSF mediated actions]
[62] [assignment: identified authentication mechanism(s)]
[63] [assignment: list of multiple authentication mechanisms]

***Application Note:** Flash loader authentication mechanism exists only for the flash loader configuration.

6.1.4.5 AUTHENTICATION FAILURE HANDLING

FIA_AFL.1/BAC Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication fulfilled by FIA_UAU.1

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]][65] unsuccessful authentication attempts occur related to *BIS Authentication*[66].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed][67], the TSF shall [assignment: list of actions][68].

FIA_AFL.1/Activation Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication fulfilled by FIA_UAU.1

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]][69] unsuccessful authentication attempts occur related to *Activation Agent Authentication*[70].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed][71], the TSF shall [assignment: list of actions][72].

FIA_AFL.1/Initialisation Authentication failure handling

Hierarchical to: No other components.

---

[64] assignment: rules describing how the multiple authentication mechanisms provide authentication]
[65] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[66] [assignment: list of authentication events]
[67] [selection: met, surpassed]
[68] [assignment: list of actions]
[69] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[70] [assignment: list of authentication events]
[71] [selection: met, surpassed]
[72] [assignment: list of actions]

Dependencies: FIA_UAU.1 Timing of authentication ***fulfilled*** by FIA_UAU.1

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]][73] unsuccessful authentication attempts occur related to *Initialisation Agent Authentication*[74].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed][75], the TSF shall [assignment: list of actions][76].

FIA_AFL.1/Personalisation Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication ***fulfilled*** by FIA_UAU.1

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]][77] unsuccessful authentication attempts occur related to *Personalisation Agent Authentication*[78].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed][79], the TSF shall [assignment: list of actions][80].

FIA_AFL.1/Flash Authentication failure handling* (See below Application Note)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication fulfilled by FIA_UAU.1

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]][81] unsuccessful authentication attempts occur related to *Flash Loader Authentication*[82].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed][83], the TSF shall [assignment: list of actions][84].

***Application Note:** Present only for flash loader configuration

[73] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[74] [assignment: list of authentication events]
[75] [selection: met, surpassed]
[76] [assignment: list of actions]
[77] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[78] [assignment: list of authentication events]
[79] [selection: met, surpassed]
[80] [assignment: list of actions]
[81] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[82] [assignment: list of authentication events]
[83] [selection: met, surpassed]
[84] [assignment: list of actions]

6.1.5 CLASS FMT SECURITY MANAGEMENT

6.1.5.1 MANAGEMENT OF TSF DATA

FMT_MTD.1/AA_PrK_Write Management of TSF data – Writing of Active Authentication Private Key

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles ***fulfilled*** by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions ***fulfilled*** by FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to *write*[85] the *Active Authentication Private Key*[86] to the *Initialisation and Personalisation Agents*[87].

FMT_MTD.1/AA_PrK_Read Management of TSF data – Reading of Active Authentication Private Key

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles ***fulfilled*** by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions ***fulfilled*** by FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to *read*[88] the *Active Authentication Private Key*[89] to the *none*[90].

FMT_MTD.1/DBAK_Write Management of TSF data – Reading of Document Basic Access Keys

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles ***fulfilled*** by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions ***fulfilled*** by FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to *write*[91] the *Document Basic Access Keys*[92] to the *Initialisation and Personalisation Agents*[93].

FMT_MTD.1/DBAK_Read Management of TSF data – Reading of Document Basic Access Keys

Hierarchical to: No other components.

[85] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[86] [assignment: list of TSF data]
[87] [assignment: the authorised identified roles]
[88] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[89] [assignment: list of TSF data]
[90] [assignment: the authorised identified roles]
[91] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[92] [assignment: list of TSF data]
[93] [assignment: the authorised identified roles]

Dependencies: FMT_SMR.1 Security roles ***fulfilled*** by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions ***fulfilled*** by FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to *read*[94] the *Document Basic Access Keys*[95] to the *none*[96].

FMT_MTD.1/Ini_Per_Data_Write Management of TSF data – Writing of Initialisation and Personalisation Data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles ***fulfilled*** by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions ***fulfilled*** by FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to *write*[97] the *Initialisation and Personalisation Agent Authentication Reference Data*[98] to the *Activation Agent*[99].

FMT_MTD.1/Ini_Per_Data_Read Management of TSF data – Reading of Initialisation and Personalisation Data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles ***fulfilled*** by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions ***fulfilled*** by FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to *read*[100] the *Initialisation and Personalisation Agent Authentication Reference Data*[101] to the *none*[102].

6.1.5.2 ABUSE OF THE TEST FUNCTIONS

FMT_MOF.1/Test Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles ***fulfilled*** by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions ***fulfilled*** by FMT_SMF.1

[94] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[95] [assignment: list of TSF data]
[96] [assignment: the authorised identified roles]
[97] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[98] [assignment: list of TSF data]
[99] [assignment: the authorised identified roles]
[100] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[101] [assignment: list of TSF data]
[102] [assignment: the authorised identified roles]

FMT_MOF.1.1 The TSF shall restrict the ability to *disable*[103] the functions *the manufacturing test functions*[104] to *the Manufacturer*[105].

Refinement: Once test functions are disabled, the TSF should irreversibly and permanently disable the test functions, so that their abuse during the usage of the TOE by embedded OS is not possible.

6.1.5.3 IC UNIQUE IDENTIFICATION DATA

FMT_MTD.1/ID Management of TSF data - Identification

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles ***fulfilled*** by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions ***fulfilled*** by FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to *write once*[106] the *IC Identification Data*[107] to the *Manufacturer*[108].

6.1.5.4 MANAGEMENT FUNCTIONS AND ROLES

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Disabling the manufacturing test functions*
- *Write once the IC Identification data*
- *Embedded OS Loading*
- *Embedded OS Loading Locking*
- *Activation*
- *Initialisation*
- *Personalisation*[109].

Application Note:

Embedded OS Loading, Embedded OS Loading Locking is valid for Flash Loader Configuration For the ROM based configuration they do not exist.

---

[103] [selection: determine the behaviour of, disable, enable, modify the behaviour of]
[104] [assignment: list of functions]
[105] [assignment: the authorised identified roles]
[106] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[107] [assignment: list of TSF data]
[108] [assignment: the authorised identified roles]
[109] [assignment: list of management functions to be provided by the TSF]

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification not fulfilled but justified

FMT_SMR.1.1 The TSF shall maintain the roles

- *Manufacturer*
- *Activation Agent*
- *Initialisation Agent*
- *Personalisation Agent*[110].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.5.5 ADDITIONAL SFRS FOR THE FLASH LOADER CONFIGURATION

FMT_MTD.1/ES Management of TSF data – Embedded OS

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles ***fulfilled*** by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions ***fulfilled by*** FMT_SMF.1

FMT_MTD.1.1 The TSF shall restrict the ability to *write*[111] the *Embedded OS*[112] to the *Manufacturer and the Card Issuer*[113].

FMT_MOF.1/FL Management of security functions behavior – Flash Loader

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles ***fulfilled*** by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions ***fulfilled*** by FMT_SMF.1

FMT_MOF.1.1 The TSF shall restrict the ability to *disable*[114] the functions *Embedded OS Loading*[115] to *Manufacturer and the Card Issuer*[116].

6.1.6 CLASS FPT PROTECTION OF THE SECURITY FUNCTIONS

[110] [assignment: the authorised identified roles]
[111] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[112] [assignment: list of TSF data]
[113] [assignment: the authorised identified roles]
[114] [selection: determine the behaviour of, disable, enable, modify the behaviour of]
[115] [assignment: list of functions]
[116] [assignment: the authorised identified roles]

6.1.6.1 SIDE CHANNEL ATTACKS PROTECTION

FPT_SCP.1/Application Side Channel Protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SCP.1 The TSF shall ensure *attackers*[117] are unable to use the following interface *physical contacts*[118] to gain access to *Active Authentication Private Key*[119] and *none*[120].

6.1.6.2 TSF TESTING

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]][121] to demonstrate the correct operation of *CPU Operation and Random Number Generator*[122].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *TSF data*[123].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of *TSF*[124].

6.1.6.3 ADDITIONAL PROTECTION AGAINST PHYSICAL ATTACKS

Memory and bus encryption and also error detection is not sufficient against physical attacks since still attacker may attack to these encryption and error detection mechanisms so additional physical protection is necessary.

First of all FPT_PHP.3 is necessary for the protection of the TSF.

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

---

[117] [assignment: type of users]
[118] [assignment: type of connection]
[119] [assignment: list of types of TSF data]
[120] [assignment: list of types of user data]
[121] [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions[assignment: conditions under which self test should occur]]
[122] [selection: [assignment: parts of TSF], the TSF]
[123] [selection: [assignment: parts of TSF data], TSF data]
[124] [selection: [assignment: parts of TSF], TSF]

FPT_PHP.3.1 The TSF shall resist *physical probing and manipulation*[125] to the [assignment: list of TSF devices/elements][126] by responding automatically such that the SFRs are always enforced.

6.1.6.4 PROTECTION FROM ENVIRONMENTAL STRESS

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *exposure to operating conditions which may not be tolerated* [127].

6.1.7 CLASS FCS: CRYPTOGRAPHIC SUPPORT

6.1.7.1 FAMILY CRYPTOGRAPHIC KEY MANAGEMENT (FCS_CKM)

FCS_CKM.1/BAC Cryptographic key generation – Basic Access Control

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] ***fulfilled*** by FCS_COP.1/TDES and FCS_COP.1/MAC

FCS_CKM.4 Cryptographic key destruction ***fulfilled*** by FCS_CKM.4/ES

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document *Basic Access Keys Derivation Algorithm*[128] and specified cryptographic key sizes *112*[129] that meet the following: [assignment: list of standards][130].

FCS_CKM.4/ES Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] ***fulfilled*** by FCS_CKM.1

[125] [assignment: physical tampering scenarios]
[126] [assignment: list of TSF devices/elements]
[127] [assignment: list of types of failures in the TSF]
[128] [assignment: cryptographic key generation algorithm]
[129] [assignment: cryptographic key sizes]
[130] [assignment: list of standards]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method][131] that meets the following: [assignment: list of standards][132].

6.1.7.2 FAMILY CRYPTOGRAPHIC OPERATIONS (FCS_COP)

FCS_COP.1/SHA Cryptographic operation – Secure Hash Algorithm

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] ***not fulfilled*** but justified

FCS_CKM.4 Cryptographic key destruction ***not fulfilled*** but justified

FCS_COP.1.1 The TSF shall perform *hash value calculation*[133] in accordance with a specified cryptographic algorithm *SHA-1* [134] and cryptographic key sizes *none*[135] that meet the following: [assignment: list of standards][136].

FCS_COP.1/TDES Cryptographic operation – Message Encryption and Decryption

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] ***fulfilled*** by FCS_CKM.1/BAC

FCS_CKM.4 Cryptographic key destruction ***fulfilled*** by FCS_CKM.4/ES

FCS_COP.1.1 The TSF shall perform *encryption and decryption* [137] in accordance with a specified cryptographic algorithm *Triple-DES in CBC Mode*[138] and cryptographic key sizes *112 bit*[139] that meet the following: [assignment: list of standards][140].

FCS_COP.1/MAC Cryptographic operation – Message Encryption and Decryption

Hierarchical to: No other components.

[131] [assignment: cryptographic key destruction method]
[132] [assignment: list of standards]
[133] [assignment: list of cryptographic operations]
[134] [assignment: cryptographic algorithm]
[135] [assignment: cryptographic key sizes]
[136] [assignment: list of standards]
[137] [assignment: list of cryptographic operations]
[138] [assignment: cryptographic algorithm]
[139] [assignment: cryptographic key sizes]
[140] [assignment: list of standards]

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] ***fulfilled*** by FCS_CKM.1/BAC

FCS_CKM.4 Cryptographic key destruction ***fulfilled*** by FCS_CKM.4/ES

FCS_COP.1.1 The TSF shall perform *message authentication*[141] in accordance with a specified cryptographic algorithm *Retail MAC*[142] and cryptographic key sizes *112 bit*[143] that meet the following: [assignment: list of standards][144].

FCS_COP.1/AA Cryptographic operation – Active Authentication

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] ***not fulfilled*** but justified

FCS_CKM.4 Cryptographic key destruction ***fulfilled*** by FCS_CKM.4/ES

FCS_COP.1.1 The TSF shall perform *electronic signing*[145] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm][146] and cryptographic key sizes [assignment: cryptographic key sizes][147] that meet the following: [assignment: list of standards][148].

6.1.7.3 FAMILY RANDOM NUMBER GENERATION (FCS_RND.1)

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric][149].

[141] [assignment: list of cryptographic operations]
[142] [assignment: cryptographic algorithm]
[143] [assignment: cryptographic key sizes]
[144] [assignment: list of standards]
[145] [assignment: list of cryptographic operations]
[146] [assignment: cryptographic algorithm]
[147] [assignment: cryptographic key sizes]
[148] [assignment: list of standards]
[149] [assignment: a defined quality metric]

6.2 ASSURANCE REQUIREMENTS

Security Assurance Requirements for the TOE for the evaluation of the TOE are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by taking the following components:

- ALC_DVS.2 Sufficiency of security measures

6.3 SECURITY REQUIREMENTS RATIONALE

6.3.1 SFRS RATIONALE TABLE

	OT.Anonymity	OT.BIS_Authentication	OT.Secure_Communication	OT.LDS_Access_Control	OT.Active_Authentication	OT.AA_PrK_Protection	OT.Security_Management	OT.Phy_Data_Access_Control	OT.Data_Integrity	OT.Internal_TOE_Transfer_Confidentiality_Protection	OT.Internal_TOE_Transfer_Integrity_Protection	OT.TSF_Operation_Protection	OT.Random_Number_Generation_Protection	OT.Environmental_Stress_Protection	OT.Side_Channel_Protection	OT.Test_Functions_Disable_Mechanism	OT.Unique_ID_Storage
FDP_ACC.1/Pre-Operational				✓													
FDP_ACF.1/Pre-Operational				✓													
FDP_ACC.1/BAC				✓													
FDP_ACF.1/BAC				✓													
FDP_ACC.1/Physical								✓									
FDP_ACF.1/Physical								✓									
FDP_ITT.1										✓	✓						
FCS_CKM.1/SP								✓									
FCS_CKM.1/TP										✓	✓						
FCS_CKM.4/IC								✓									
FCS_COP.1/SP								✓									
FCS_COP.1/TP										✓	✓						
FPT_SCP.1/IC								✓		✓	✓				✓		
FDP_UCT.1			✓														
FDP_UIT.1			✓														
FIA_UID.1/Operational	✓			✓													
FIA_UAU.1/Operational	✓			✓													
FIA_POI.1					✓												
FIA_UID.1/Pre-Operational				✓			✓										
FIA_UAU.1/Pre-Operational				✓			✓										
FIA_UAU.4		✓															
FIA_UAU.5		✓		✓			✓										
FIA_AFL.1/BAC		✓															
FIA_AFL.1/Activation							✓										
FIA_AFL.1/Initialisation							✓										
FIA_AFL.1/Personalisation							✓										
FMT_MTD.1/AA_PrK_Write					✓												
FMT_MTD.1/AA_PrK_Read						✓											
FMT_MTD.1/DBAK_Write		✓															
FMT_MTD.1/DBAK_Read		✓															
FMT_MTD.1/Ini_Per_Data_Write							✓										
FMT_MTD.1/Ini_Per_Data_Read							✓										
FMT_MOF.1/Test																✓	
FMT_MTD.1/ID																	✓
FMT_SMF.1							✓										
FMT_SMR.1							✓										

FPT_SCP.1/Application														✓		
FPT_TST.1									✓			✓	✓			
FPT_PHP.3								✓	✓	✓	✓					
FPT_FLS.1														✓		
FCS_CKM.1/BAC			✓													
FCS_CKM.4/ES			✓													
FCS_COP.1/SHA		✓														
FCS_COP.1/TDES		✓	✓													
FCS_COP.1/MAC		✓	✓													
FCS_COP.1/AA					✓											
FCS_RND.1		✓														

Table 3: SFRs Rationale Table

ADDITIONAL RATIONALE FOR THE FLASH LOADER CONFIGURATION

OT.Flash_Loader_Functionality	FPT_MTD.1/ES, FMT_SMF.1, FMT_SMR.1
OT.Flash_Loader_Authorization	FIA_AFL.1/Flash, FIA_UAU.1, FIA_UAU.5, FIA_UID.1
OT.Flash_Loader_Disable_Mechanism	FPT_MOF.1/FL, FMT_SMF.1, FMT_SMR.1

Table 4: Additional SFRs Rationale for the Flash Loader Configuration

6.3.2 SFRS JUSTIFICATION

— **OT.Anonymity**

FIA_UID.1/Operational and FIA_UAU.1/Operational do not let any information, that can be linked to the identity of the passport holder, be disclosed before BIS authentication takes place. So they cover OT.Anonymity.

SFRs: FIA_UID.1/Operational, FIA_UAU.1/Operational

— **OT.BIS_Authentication**

The authentication mechanism and the authentication rule of Basic Inspection System is given in FIA_UAU.5. FIA_UAU.4 requires the BIS authentication mechanism to be single use. The cryptographic support for the BIS authentication is given by FCS_COP.1/TDES, FCS_COP.1/SHA, FCS_RND.1. FIA_AFL.1/BAC protects the authentication mechanism from attacks. FMT_MTD.1/DBAK_Write is needed to securely write the authentication reference data for BIS authentication and FMT_MTD.1/DBAK_Read to protect the authentication reference data.

SFRs: FIA_AFL.1/BAC, FIA_UAU.5, FIA_UAU.4, FCS_COP.1/TDES, FCS_COP.1/MAC, FCS_COP.1/SHA, FCS_RND.1, FMT_MTD.1/DBAK_Write, FMT_MTD.1/DBAK_Read.

— **OT.Secure_Communication**

The secure communication is performed by the FDP_UIT.1 and FDP_UCT.1 requirements. The cryptographic key generation necessary for the secure communication is stated in FCS_CKM.1/BAC, the crytographic operations for message confidentiality and authentication are performed by FCS_COP.1/TDES and FCS_COP.1/MAC. Finally after the secure communication channel is terminated, cryptographic key destruction is performed by FCS_CKM.4/ES.

SFRs: FDP_UIT.1, FDP_UCT.1, FCS_CKM.1/BAC, FCS_COP.1/TDES, FCS_COP.1/MAC, FCS_CKM.4/ES

- **OT.Logical_Data_Acces**

FDP_ACC.1/Pre-Operational, FDP_ACF.1/Pre-Operational, FDP_ACC.1/BAC and FDP_ACF.1/BAC control the user data access. FIA_UID.1/Pre-Operational, FIA_UAU.1/Pre-Operational, FIA_UID.1/Operational, FIA_UAU.1/Operational prevent the attackers to access to the user data without identification and authentication. FIA_UAU.5 enable the mechanisms to authenticate the users.

SFRs: FDP_ACC.1/Pre-Operational, FDP_ACF.1/Pre-Operational, FDP_ACC.1/BAC, FDP_ACF.1/BAC, FIA_UID.1/Pre-Operational, FIA_UAU.1/Pre-Operational, FIA_UID.1/Operational, FIA_UAU.1/Operational ,FIA_UAU.5

- **OT.Active_Authentication**

FIA_POI.1 requries the TOE to have ability to prove itself as stated in objective OT.Active_Authentication. FCS_COP.1/AA addresses the cryptographic support needed by FIA_POI.1 and FMT_MTD.1/AA_Write addresses the writing of Active Authentication Private Key to the TOE.

SFRs: FIA_POI.1, FCS_COP.1/AA, FMT_MTD.1/AA_Write

- **OT.AA_PrK_Protection**

FMT_MTD.1/AA_Read prevents from attackers to read the Active Authentication Private Key.

SFR: FMT_MTD.1/AA_Read

- **OT.Security_Management**

FMT_SMR.1 and FMT_SMF.1 require the necessary management functions and roles be present in the TOE. FIA_UID.1/Pre-Operational and FIA_UAU.1/Pre-Operational prevent the attackers to access to the roles without identification and authentication. FIA_UAU.5 enable the mechanisms to authenticate the management roles. FIA_AFL.1/Activation, FIA_AFL.1/Initialisation and FIA_AFL.1/Personalisation prevent the attackers to attack to the authentication mechanisms. FMT_MTD.1/Ini_Per_Data_Write and FMT_MTD.1/Ini_Per_Data_Read enable the secure entry of the authentication reference data to the TOE and protects from reading out and manipulations performed by the attackers.

SFRs: FMT_SMR.1, FMT_SMF.1, FIA_UID.1/Pre-Operational, FIA_UAU.1/Pre-Operational, FIA_UAU.5, FIA_AFL.1/Activation, FIA_AFL.1/Initialisation, FIA_AFL.1/Personalisation, FMT_MTD.1/Ini_Per_Data_Write, FMT_MTD.1/Ini_Per_Data_Read

— **OT.Phy_Data_Access_Control**

FDP_ACC.1/Physical and FDP_ACF.1/Physical provides access to the embedded OS while prevents the attacker. This is performed by storing the data encrypted and decrypting it with the support of FCS_CKM.1/DP, FCS_CKM.4/IC and FCS_COP.1/DP. FPT_PHP.3 provides additional protection against physical attacks.

SFRs: FDP_ACC.1/Physical, FDP_ACF.1/Physical, FCS_CKM.1/DP, FCS_CKM.4/IC, FCS_COP.1/DP, FPT_PHP.3

— **OT.Data_Integrity**

FPT_TST.1 monitors the integrity of the data and performs the actions determined by the ST writer. FPT_PHP.3 provides additional protection against physical attacks. The SFRs covering OT.Phys_Data_Access_Control is also valid for this objective, making reasonable changes to the encrypted data is not possible.

SFRs: FPT_TST.1, FPT_PHP.3, FDP_ACC.1/Physical, FDP_ACF.1/Physical, FCS_CKM.1/DP, FCS_CKM.4/IC, FCS_COP.1/DP

— **OT.Internal_TOE_Transfer_Confidentiality_Protection**

FDP_ITT.1 provides protection while the data is in transmit between internal parts of the TOE. Protection is performed by encrypting the internal data traffic; encryption and decryption operations are performed by FCS_CKM.1/TP, FCS_CKM.4, FCS_COP.1/TP requirements. FPT_PHP.3 provides additional protection against physical attacks.

SFRs: FDP_ITT.1, FCS_CKM.1/TP, FCS_CKM.4, FCS_COP.1/TP, FPT_PHP.3

— **OT.Internal_TOE_Transfer_Integrity_Protection**

FPT_PHP.3 provide protection against physical attacks. The SFRs covering OT.Internal_TOE_Transfer_Confidentiality_Protection is also valid for this objective, making reasonable changes to the encrypted data is not possible.

SFRs: FPT_PHP.3, FDP_ITT.1, FCS_CKM.1/TP, FCS_CKM.4, FCS_COP.1/TP

— **OT.TSF_Operation_Protection**

FPT_TST.1 includes the test of correct operation of TSF, so covers the OT.TSF_Operation_Protection.

SFR: FPT_TST.1

- **OT.Random_Number_Generation_Protection**

FPT_TST.1 includes the test of correct operation of the Random Number Generation Functionality. So it covers the OT.Random_Number_Generation_Protection.

SFR: FPT_TST.1

- **OT.Side_Channel_Protection**

FPT_SCP.1/IC and FPT_SCP.1/ES protect the TOE from side channel attacks.

SFRs: FPT_SCP.1/IC, FPT_SCP.1/ES

- **OT.Environmental_Stress_Protection**

FPT_FLS.1 require that if the TOE encounters environmental stress that it may not handle, it will preserve the secure state.

SFR: FPT_FLS.1

- **OT.Unique_ID_Storage**

FMT_MTD.1/ID provides the functionality to the manufacturer to write the IC Identification data. So OT.Unique_ID_Storage is covered.

SFR: FMT_MTD.1/ID

- **OT.Test_Functions_Disable_Mechanism**

FMT_MOF.1/Test enables the functionality to irreversebly disable the test functionality. FMT_SMF.1 and FMT_SMR.1 defines this functionality and related roles.

SFRs: FMT_MOF.1/Test, FMT_SMF.1, FMT_SMR.1

ADDITIONAL RATIONALE FOR THE FLASH LOADER CONFIGURATION

- **OT.Flash_Loader_Functionality**

FPT_MTD.1/ES enables the embedded operating system loading function. FMT_SMF.1 and FMT_SMR.1 defines this functionality and related roles.

SFRs: FMT_MTD.1/ES, FMT_SMF.1, FMT_SMR.1

— **OT.Flash_Loader_Authorization**

FIA_UAU.5 requires a Flash Loader Authentication mechanism exist and FIA_UAU.1/Pre-Operational and FIA_UID.1/Pre-Operational require that Flash Loader operation can be performed before identification and authentication of the user. Finally FIA_AFL.1/Flash protects the Flash Loader authentication mechanisms from false authentication attempts.

SFRs: FIA_UAU.5, FIA_UAU.1/Pre-Operational, FIA_UID.1/Pre-Operational, FIA_AFL.1/Flash

— **OT.Flash_Loader_Disable_Mechanism**

FMT_MOF.1/FL enables the functionality to irreversebly disable the flash loader mechanism. FMT_SMF.1 and FMT_SMR.1 defines this functionality and related roles.

SFRs: FMT_MOF.1/FL, FMT_SMF.1, FMT_SMR.1

6.3.3 DEPENDENCIES FOR THE SECURITY FUNCTIONAL REQUIREMENTS

SFR	**Dependencies**	**Support of the Dependencies**
FDP_ACC.1/Pre-Operational	FDP_ACF.1	FDP_ACF.1/Pre-Operational
FDP_ACF.1/Pre-Operational	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Pre-Operational justified (see justification 1)
FDP_ACC.1/BAC	FDP_ACF.1	FDP_ACF.1/Pre-Operational
FDP_ACF.1/BAC	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Pre-Operational justified (see justification 1)
FDP_ACC.1/Physical	FDP_ACF.1	FDP_ACF.1/Pre-Operational
FDP_ACF.1/Physical	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Pre-Operational justified (see justification 1)
FDP_ITT.1	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	fulfilled by FDP_ACC.1/Physical
FCS_CKM.1/SP	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	fulfilled by FCS_COP.1 /SP fulfilled by FCS_CKM.4/IC

FCS_CKM.1/TP	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	fulfilled by FCS_COP.1 /TP fulfilled by FCS_CKM.4/IC
FCS_CKM.4/IC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	fulfilled by FCS_CKM.1/SP and FCS_CKM.1/TP
FCS_COP.1/SP	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	fulfilled by FCS_CKM.1/SP fulfilled by FCS_CKM.4/IC
FCS_COP.1/TP	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	fulfilled by FCS_CKM.1/TP fulfilled by FCS_CKM.4
FPT_SCP.1/IC	None	----
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	justified (see justification 2) fulfilled by FDP_ACC.1/BAC
FDP_UIT.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	fulfilled by FDP_ACC.1/BAC]

	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path	justified (see justification 2)
FIA_UID.1/Operational	None	----
FIA_UAU.1/Operational	FIA_UID.1	fulfilled by FIA_UID.1/Operational
FIA_POI.1	None	----
FIA_UID.1/Pre-Operational	None	----
FIA_UAU.1/Pre-Operational	FIA_UID.1	fulfilled by FIA_UID.1/Pre-Operational
FIA_UAU.4	None	----
FIA_UAU.5	None	----
FIA_AFL.1/BAC	FIA_UAU.1 Timing of authentication	fulfilled by FIA_UAU.1/ Operational
FIA_AFL.1/Activation	FIA_UAU.1 Timing of authentication	fulfilled by FIA_UAU.1//Pre-Operational
FIA_AFL.1/Initialisation	FIA_UAU.1 Timing of authentication	fulfilled by FIA_UAU.1//Pre-Operational
FIA_AFL.1/Personalisation	FIA_UAU.1 Timing of authentication	fulfilled by FIA_UAU.1//Pre-Operational
FMT_MTD.1/AA_PrK_Write	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	fulfilled by FMT_SMR.1 fulfilled by FMT_SMF.1
FMT_MTD.1/AA_PrK_Read	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	fulfilled by FMT_SMR.1 fulfilled by FMT_SMF.1
FMT_MTD.1/DBAK_Write	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	fulfilled by FMT_SMR.1 fulfilled by FMT_SMF.1
FMT_MTD.1/DBAK_Read	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	fulfilled by FMT_SMR.1 fulfilled by FMT_SMF.1
FMT_MTD.1/Ini_Per_Data_Write	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	fulfilled by FMT_SMR.1 fulfilled by FMT_SMF.1
FMT_MTD.1/ Ini_Per_Data_Read	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	fulfilled by FMT_SMR.1 fulfilled by FMT_SMF.1

FMT_MOF.1/Test	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	fulfilled by FMT_SMR.1 fulfilled by FMT_SMF.1
FMT_MTD.1/ID	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	fulfilled by FMT_SMR.1 fulfilled by FMT_SMF.1
FMT_SMF.1	None	----
FMT_SMR.1	FIA_UID.1	fulfilled by FIA_UID.1
FPT_SCP.1/Application	None	----
FPT_TST.1	None	---
FPT_PHP.3	None	---
FPT_FLS.1	None	---
FCS_CKM.1/BAC	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	fulfilled by FCS_COP.1 /TDES and FCS_COP.1/MAC fulfilled by FCS_CKM.4/ES
FCS_CKM.4/ES	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	fulfilled by FCS_CKM.1/BAC
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	justified (see justification 3) justified (see justification 3)
FCS_COP.1/TDES	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or	fulfilled by FCS_CKM.1/BAC

	FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	fulfilled by FCS_CKM.4/ES
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	fulfilled by FCS_CKM.1/BAC fulfilled by FCS_CKM.4/ES
FCS_COP.1/AA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	justified (see justification 4) fulfilled by FCS_CKM.4/ES
FCS_RND.1	None	---

Table 5: Dependencies for the SFRs

Justification 1: The FPT_ACF.1/BAC, FPT_ACF.1/Pre-Operational and FPT_ACF.1/Physical apply to the all data. So security attribute management is not necessary.

Justification 2: The SFRs FDP_UCT.1 and FDP_UIT.1 require the TOE to communicate securely with BIS, since there is no other communication channel and there is no human interface neither FTP_ITC.1 nor FTP_TRP.1 is necessary here.

Justification 3: The hash algorithm defined in FCS_COP.1/SHA does not need any key to function. So neither key generation nor import is necessary.

Justification 4: The active authentication private key is permanently stored in the TOE and it is written to the TOE by FMT_MTD.1/AA_Write, neither import nor generation is necessary.

ADDITIONAL FOR FLASH LOADER

SFR	Dependencies	Support of the Dependencies
FIA_AFL.1/Flash	FIA_UAU.1 Timing of Authentication	fulfilled by FIA_UAU.1
FMT_MTD.1/ES	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	fulfilled by FMT_SMR.1 fulfilled by FMT_SMF.1
FMT_MOF.1/FL	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	fulfilled by FMT_SMR.1 fulfilled by FMT_SMF.1

Table 6: Dependencies for the Additional SFRs of the Flash Loader

6.3.4 RATIONALE AND DEPENDENCIES FOR THE SARS

The EAL4 is chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

ALC_DVS.2 is added to the assurance requirements to obtain higher assurance of the TOE's development and manufacturing.

The dependencies for augmented SARs:

SAR	Dependencies	Support of the Dependencies
ALC_DVS.2	None	---

Table 7: The Dependencies for augmented SARs

6.3.5 SECURITY REQUIREMENTS – MUTUAL SUPPORT AND INTERNAL CONSISTENCY

Current PP aims to withstand against attacker of Enhanced Basic attack potential. Both the SFRs and the SARs are selected to reach this goal. The rationale of both requirement types (functional requirements and assurance requirements are given and dependency analysis of them are made; no inconsistency exists. The SFRs and SARs internally support each other.

The support for the SFRs and SFRs of each other is such that SARs are sufficient to give enough assurance for the required functionality.

7. REFERENCES

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 1, September 2012

[4] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

[5] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organisation

[6] Common Criteria Protection Profile, Secure IC Platform, Draft Version 1.0

8. ACCROYNMS

AA: Active Authentication

BAC: Basic Access Control

BIS: Basic Inspection System

LDS: Logical Data Structure