COMMON CRITERIA PROTECTION PROFILE

EMBEDDED OPERATING SYSTEM

Draft Version 1.0

TURKISH STANDARDS INSTITUTION

TABLE OF CONTENTS

FIGURES LIST

TABLES LIST

1. INTRODUCTION

1.1 PP Reference

1.1.1 TITLE

Embedded Operating System Protection Profile

1.1.2 VERSION

Draft

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 product consisting of Embedded Operating System and Secure IC. The packaging, external components such as battery and antenna, physical card are out of scope of the PP. The activities such as packaging, composite product manufacturing are also taken out of evaluation context.

1.2.2 TOE USAGE AND MAJOR SECURITY PROPERTIES

The TOE is used as a platform for following types of security sensitive applications:

- Identification and Authentication
- Electronic Fare and Purse
- Electronic Signature
- Secure Data Storage

The TOE protects the application data from attackers and optionally offers cryptographic services to the smart card application.

The TOE has following security properties:

- Data Access Control
- Security Management
- Self-Protection

- Cryptographic Support

1.2.3 REQUIRED NON-TOE HARDWARE/SOFTWARE/FIRMWARE

None

1.3 TOE DEFINITION

1.3.1 THE TOE CONTENTS

The TOE consists of:

- Hardware of Security IC
- Security IC Dedicated Software
- IC Unique Identification Data + Configuration Data (optional)
- Embedded OS
- Security Guidance Documentation

The Hardware: The hardware consists of CPU, volatile and non-volatile memories, I/O components and security components.

Security IC Dedicated Software: Any software other than the embedded OS is the Security IC Dedicated Software. Security IC Dedicated Software consists of IC Dedicated Test Software, IC Dedicated Support Software and if embedded OS is stored on Flash Memory additionally Flash Loader Software.

IC Unique Identification Data: Unique identification is the requirement of the card issuer.

Configuration Data (optional)**:** IC manufacturers offer their consumers wide range of products with different sizes of memories and with different functionalities. They usually use the same physical product with different configurations to provide the range of products. Different configurations are implemented with mechanisms to disable the functionalities and with some configuration data that limits or blocks the memory size and/or functionalities. A vendor may not offer different configurations of same physical product, in this case configuration data does not exit, so it is optional.

Security Guidance Documentation: Contains the information about the secure usage of the TOE. The Security Guidance Documentation is also evaluated and if and if only a TOE is used accordingly to this security guidance it is considered as certified. Any failure in compliance to the security guidance will break the security certificate and the TOE can be assumed as in the evaluated configuration state.

1.3.2 THE TOE PHYSICAL VIEW

The Physical Hardware consists of:

- CPU
- Volatile and Non-Volatile Memories
- Security Components
- Communication Interfaces

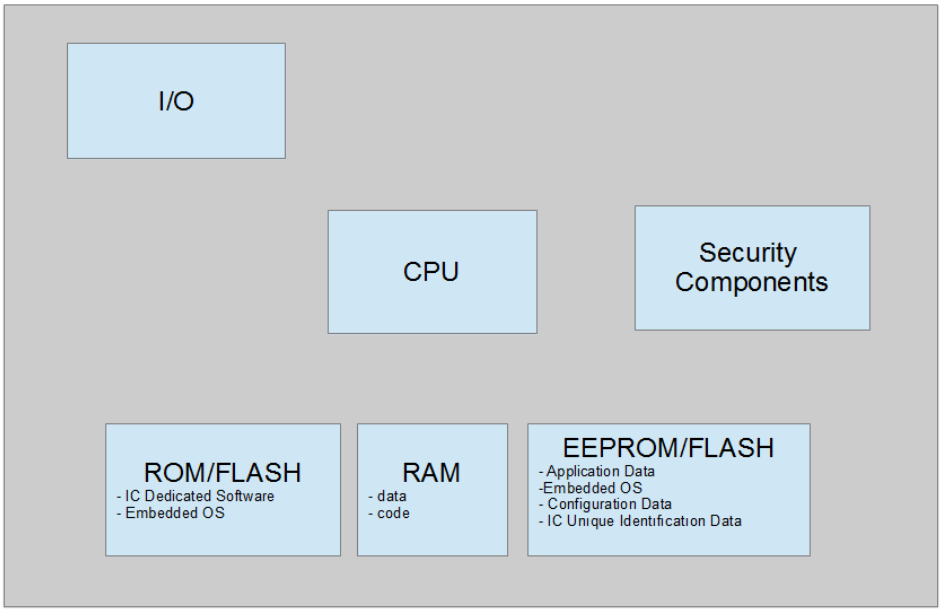


Figure 1: Secure IC Diagram

Data Stored on the Non-Volatile Memories

- IC Dedicated Software
- Embedded OS
- Application Data
- Configuration Data
- Activation, Initialisation and Personalisation Data
- IC Unique Identification Data

Separately Delivered Item(s):

- Guidance Documentation

1.3.3 THE TOE LOGICAL VIEW

The logical view of the TOE is in the below figure 2. The Embedded OS, IC Dedicated Test Software, IC Dedicated Support Software and Security IC Hardware together form the TOE and set the boundaries of it. In the TOE interacts with the card issuer, card holder and the attacker and it protects the smart card application from the attacker. Before delivery to the card issuer, the TOE manufacturer interacts with the IC Dedicated Test Software and IC Dedicated Support Software.

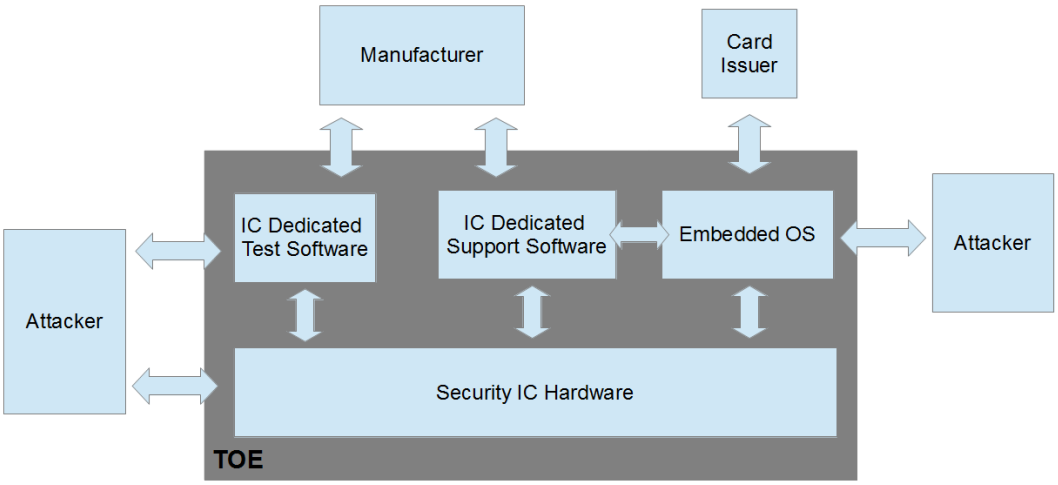


Figure 2: Logical View of the TOE

1.3.4 LIFE-CYCLE MODEL

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 [Ref].

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.

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.

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 INTRODUCTION

3.1.1 ASSETS AND SECURITY SERVICES

Application Data: Application data is the data belonging to the application and its management is performed via the *Application Data Access Control Policy* which is determined by the application and enforced by the ES.

Random Number Generation: The TOE provides to the users of it. Random numbers are essential for the security applications that ES serves for.

TSF Data:

The secondary assets are the *Unique Identification Data*, *Activation Authentication Reference Data*, *Personalisation and Initialisation Authentication Keys*, *TSF Code*.

Additional Items:

Any security service and TSF data belonging to that security service may be added by ST author.

3.1.2 SUBJECTS AND EXTERNAL ENTITIES

Manufacturer (Composite Product): The roles of the IC Manufacturer, the ES 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 card issuer as a whole product including the ES and the Secure IC.

Card Issuer: Card issuer performs the application development activity and all the other legitimate activities; including activation agent, initialisation agent, personalisation agent, card holder, the card administrator (optional role) and, the card holder; are assumed to be performed on behalf of card 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. Whenever the communication environment is not assumed secure, the TOE and the terminal shall protect the communication channel between them.

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

Card Administrator (optional): The optional subject whom performs the administrative task(s) if any exists.

Attacker: The attacker is the entity who tries to undermine the security policies of the card issuer. Attacker is assumed to possess *high attack potential*.

3.2 THREATS

LOGICAL THREATS

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

T.Logical_Data_Access: An attacker may illegitimately read out or change the application data.

T.Logical_Malfunction: An attacker may cause the TSF to malfunction by sending unexpected input.

PROBING AND MANIPULATION THREATS:

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

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

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

T.Manipulation_on_Data_Transfer: An attacker may physically attack to the internals of the TOE to make changes to the application 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.

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 application data.

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

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.

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.

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)***

3.3 ORGANISATIONAL SECURITY POLICIES

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 ES.

P.Random_Number_Generation: The TOE should provide random numbers to the ES.

ORGANISATIONAL SECURITY POLICY FOR THE FLASH LOADER CONFIGURATION

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

3.4 ASSUMPTIONS

A.Communication_Environment: It is assumed that the environment where the legitimate actors and the TOE communicate is secure.

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 is securely protected outside of the TOE.

A.Responsible_Application: The application, that the TOE provides services and protection, specifies the data access policy properly and implements correctly to the TOE.

4. SECURITY OBJECTIVES

4.1 SECURITY OBJECTIVES FOR THE TOE

4.1.1 LOGICAL PROTECTION

OT.Logical_Data_Access: The TOE must protect the data stored and processed on the TOE from unauthorized access through logical access.

OT.Security_Management: The TOE must have activation, initialisation and personalisation management functions and protect these functions from abuse.

OT.Residual_Information_Protection: The TOE shall ensure that any previous information content of a resource is made unavailable upon deselecting that resource.

OT.Recovery_Environmental_Stress: The TOE shall preserve its internal integrity after an Environmental Stress Attack.

4.1.2 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_Contacts.

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 RANDOM NUMBER GENERATION

OT.Random_Number_Generation: The TOE should have mechanisms to provide random numbers to the embedded operating system.

4.1.8 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.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 should act responsively. Any authentication reference data should be securely protected outside of the TOE.

OE.Responsible_Application: The application, that the TOE provides services and protection, should specify the data access policy properly and implement correctly to the TOE.

OE.Secure_Communication: The environment that communication between the TOE and the legitimate actors takes place should be secure.

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

The following table provides an overview for security objectives coverage.

No	SPD	SO
1.	T.Unauthorized_Management	OT.Security_Management, OE.Security_Management
2.	T.Logical_Data_Access	OT.Logical_Data_Access, OE.Responsible_Application
3.	T.Logical_Malfunction	OT.Residual_Information_Protection
4.	T.Probing_on_Data_Storage	OT. Phy_Data_Access_Control
5.	T.Probing_on_Data_Transfer	OT.Internal_TOE_Transfer_Confidentiality_Protection
6.	T.Manipulation_on_Data_Storage	OT. Phy_Data_Access_Control, OT.Data_Integrity
7.	T.Manipulation_on_Data_Transfer	OT.Internal_TOE_Transfer_Confidentiality_Protection, OT.Internal_TOE_Transfer_Integrity_Protection
8.	T.Manipulation_on_Execution	OT.TSF_Operation_Protection OT.Residual_Information_Protection
9.	T.Manipulation_on_RND	OT.Random_Number_Generation_Protection
10.	T.Information_Leakage_Surface	OT.Internal_TOE_Transfer_Confidentiality_Protection
11.	T.Information_Leakage_Contacts	OT.Side_Channel_Protection
12.	T.Environmental_Stress_Application	OT.Environmental_Stress_Protection OT.Recovery_Environmental_Stress
13.	T.Abuse_of_the_Test_Functions	OT.Test_Functions_Disable_Mechanism, OE.Test_Functions_Disable
14.	P.Security_Management	OT.Security_Management
15.	P.IC_Unique_Identification_Data	OT.Unique_ID_Storage, OE.Unique_Identification
16.	P.Random_Number_Generation	OT.Random_Number_Generation
17.	A.Security_Management	OE.Security_Management
18.	A.Responsible_Application	OE.Responsible_Application
19.	A.Communication_Environment	OE.Secure_Communication

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 PROBLEM JUSTIFICATION

In this section justification of security problem by security objectives is given.

- **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.

- **T.Logical_Data_Access**

OT.Logical_Data_Access protects the user data from unauthorised access accordingly to the rules defined by the application. OE.Responsible_Application determines the rules as it is to be to protect data from unauthorised access.

- **T.Logical_Malfunction**

OT.Residual_Information_Protection clears any residual information and prevents the attackers to access any confidential data by causing malfunctions.

- **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.

- **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.

- **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 covers this threat.

- **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.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.Internal_TOE_Transfer_Confidentiality_Protection and OT.Internal_TOE_Transfer_Integrity_Protection covers this threat.

- **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.

- **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.

- **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.

- **T.Information_Leakage_Contacts**

OT.Side_Channel_Protection cover the threat T.Information_Leakage_Contacts.

- **T.Environmental_Stress_Application**

OT.Environmental_Stress_Protection address the T.Environmental_Stress_Application. OT.Recovery_Environmental_Stress puts additional countermeasure in place by adding logical measures to preserve the TOE's internal integrity.

- **T.Abuse_of_the_Test_Functions**

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.

- **P.Security_Management**

OT.Security_Management puts the Activation, Initialisation and Personalisation management functions and respective security management roles in place.

- **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 covers the P.IC_Unique_Identification_Data

- **P.Random_Number_Generation**

OT.Random_Number_Generation covers the policy P.Random_Number_Generation.

- **P.Embedded_OS_Load**

OT.Flash_Loader_Functionality covers the policy P.Embedded_OS_Load.

- **A.Communication_Environment**

OE.Secure_Communication cover the assumption.

- **A.Security_Management**

OE.Security_Management cover the responsible behaviour of the security management roles.

- **A.Responsible_Application**

OE.Responsible_Application cover the application's correctly specification and implementation of data access policies.

5. EXTENDED COMPONENTS

Following components are added:

- FCS_RND.1
- FPT_SCP.1

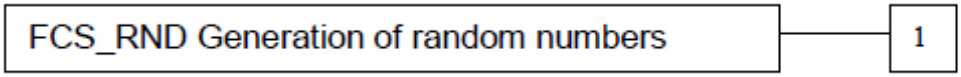
5.1 CLASS FCS CRYPTOGRAPHIC SUPPORT

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 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

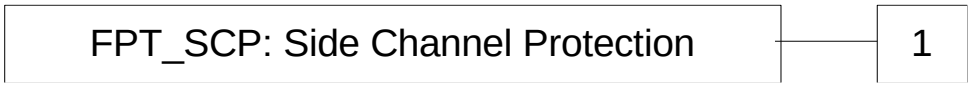
requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2.

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.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 PHYSICAL AND LOGICAL DATA ACCESS CONTROL AND TRANSFER PROTECTION

Two types of access categories exist, and they are ***Physical Access*** and ***Logical Access***. Physical access is performed by the Physical Access Control Policy and the logical access is performed by two policies: ***Pre-Operational Data Access Control Policy*** and ***Application 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, these policies enable the Security Management Policy and protect 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*[1] on *attacker, activation agent, initialization agent, personalisation agent, application and read, write, delete operations*[2].

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 [assignment: access control SFP][3] to objects based on the following: [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][4].

[1] [assignment: access control SFP]
[2] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[3] [assignment: access control SFP]
[4] [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.1.2 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][5].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects][6].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects][7].

6.1.1.2 APPLICATION DATA ACCESS CONTROL POLICY

FDP_ACC.1/Application Subset access control – Application Data 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 *Application Data Access Control*[8] on *[assignment: list of subjects]*, *Application Data*, and *read, write, delete operations*[9].

FDP_ACF.1/Application Security attribute based access control – Application Data 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 ***fulfilled*** by FMT_MSA.3

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP][10] to objects based on the following: [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][11].

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

[5] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[6] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[7] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[8] [assignment: access control SFP]
[9] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[10] [assignment: access control SFP]
[11] [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]

controlled subjects and controlled objects using controlled operations on controlled objects][12].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects][13].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects][14].

6.1.1.3 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.2, FDP_ACF.1 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* [15] on *attacker, application data and physical access*[16].

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

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*[17] to objects based on the following: *Attacker and Application Data, type of user*][18].

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*

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects][19]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[20].

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*.[21]

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*[22] to prevent the *disclosure, and modification*[23] 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.

[17] [assignment: access control SFP]
[18] [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]
[19] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[20] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[21] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].
[22] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[23] [selection: disclosure, modification, loss of use]

6.1.1.3.1 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][24] and specified cryptographic key sizes [assignment: cryptographic key sizes][25] that meet the following: [assignment: list of standards][26].

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][27] and specified cryptographic key sizes [assignment: cryptographic key sizes][28] that meet the following: [assignment: list of standards][29].

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

[24] [assignment: cryptographic key generation algorithm]
[25] [assignment: cryptographic key sizes]
[26] [assignment: list of standards]
[27] [assignment: cryptographic key generation algorithm]
[28] [assignment: cryptographic key sizes]
[29] [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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method][30] that meets the following: [assignment: list of standards][31].

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

FCS_COP.1.1 The TSF shall perform *encryption and decryption* [32] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm][33] and cryptographic key sizes [assignment: cryptographic key sizes] [34] that meet the following: [assignment: list of standards][35].

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*[36] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm][37] and cryptographic key sizes [assignment: cryptographic key sizes][38] that meet the following: [assignment: list of standards][39].

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

FPT_SCP.1 Side Channel Protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SCP.1 The TSF shall ensure *attackers*[40] are unable to use the following interface *physical contacts*[41] to gain access to *Data Storage Protection keys, Data Transfer Protection keys*[42] and *Stored Data and Transferred Data*[43].

6.1.2 SECURITY MANAGEMENT

FMT_MSA.1 Management of security attributes

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/Application

FMT_SMR.1 Security roles ***fulfilled*** FMT_SMR.1

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

FMT_MSA.1.1 The TSF shall enforce the *Application Data Access Control SFP*[44] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]][45] the security attributes [assignment: list of security attributes][46] to [assignment: the authorised identified roles][47].

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes ***fulfilled*** by FMT_MSA.1

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

[40] [assignment: type of users]
[41] [assignment: type of connection]
[42] [assignment: list of types of TSF data]
[43] [assignment: list of types of user data]
[44] [assignment: access control SFP(s), information flow control SFP(s)]
[45] [selection: change_default, query, modify, delete, [assignment: other operations]]
[46] [assignment: list of security attributes]
[47] [assignment: the authorised identified roles]

FMT_MSA.3.1 The TSF shall enforce the *Application Data Access Control SFP*[48] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]][49] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: the authorised identified roles][50] to specify alternative initial values to override the default values when an object or information is created.

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*[51] the *Initialisation and Personalisation Agent Authentication Reference Data*[52] to the *Activation Agent*[53].

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure and modification*[54] when it is transmitted between separate parts of the TOE.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

[48] [assignment: access control SFP, information flow control SFP]
[49] [selection, choose one of: restrictive, permissive, [assignment: other property]]
[50] [assignment: the authorised identified roles]
[51] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[52] [assignment: list of TSF data]
[53] [assignment: the authorised identified roles]
[54] [selection: disclosure, modification]

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*
- [assignment: list of management functions to be provided by the TSF][55].

Application Note:

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

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*
- [assignment: the authorised identified roles][56].

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

6.1.3 USER IDENTIFICATION AND AUTHENTICATION

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

[55] [assignment: list of management functions to be provided by the TSF]
[56] [assignment: the authorised identified roles]

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]][57] unsuccessful authentication attempts occur related to *Flash Loader Authentication*[58].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed][59], the TSF shall [assignment: list of actions][60].

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

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]][61] unsuccessful authentication attempts occur related to *Activation Agent Authentication*[62].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed][63], the TSF shall [assignment: list of actions][64].

FIA_AFL.1/Initialisation 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 *Initialisation Agent 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].

---

[57] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[58] [assignment: list of authentication events]
[59] [selection: met, surpassed]
[60] [assignment: list of actions]
[61] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[62] [assignment: list of authentication events]
[63] [selection: met, surpassed]
[64] [assignment: list of actions]
[65] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[66] [assignment: list of authentication events]

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]][69] unsuccessful authentication attempts occur related to *Personalisation 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_UID.1 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* [73] 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.

FIA_UAU.1 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*[74] 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.

---

[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]
[73] [assignment: list of TSF-mediated actions]
[74] [assignment: list of TSF mediated actions]

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*
- *Personalisation Agent Authentication*
- *and other authentication mechanisms*[75]

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*
- *And other rules*[76]

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

6.1.4 RESIDUAL INFORMATION PROTECTION

FDP_RIP.2 Full residual information protection

Hierarchical to: FDP_RIP.1 Subset residual information protection

Dependencies: No dependencies.

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from][77] all objects.

[75] [assignment: list of multiple authentication mechanisms]
[76] assignment: rules describing how the multiple authentication mechanisms provide authentication]
[77] [selection: allocation of the resource to, deallocation of the resource from]

6.1.5 RECOVERY FROM ENVIRONMENTAL STRESS

FDP_ROL.1 Basic rollback

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/Pre-Operational

FDP_ROL.1.1 The TSF shall enforce *Pre-Operational Data Access Control SFP*[78] to permit the rollback of the [assignment: list of operations][79] on the [assignment: information and/or list of objects][80].

FDP_ROL.1.2 The TSF shall permit operations to be rolled back within the [assignment: boundary limit to which rollback may be performed][81].

FPT_RCV.4 Function recovery

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_RCV.4.1 The TSF shall ensure that [assignment: list of functions and failure scenarios][82] have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

6.1.6 PROTECTION AGAINST MANIPULATION

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: integrity errors][83] on all objects, based on the following attributes: *for all application data*[84].

[78] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[79] [assignment: list of operations]
[80] [assignment: information and/or list of objects]
[81] [assignment: boundary limit to which rollback may be performed]
[82] [assignment: list of functions and failure scenarios]
[83] [assignment: integrity errors]

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [assignment: action to be taken][85].

FDP_ITT.3 Integrity monitoring

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 Basic internal transfer protection ***fulfilled*** by FDP_ITT.1

FDP_ITT.3.1 The TSF shall enforce the *Physical Data Access Policy*[86] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [assignment: integrity errors][87].

FDP_ITT.3.2 Upon detection of a data integrity error, the TSF shall [assignment: specify the action to be taken upon integrity error][88].

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]][89] to demonstrate the correct operation of *CPU Operation and Random Number Generator*[90].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *TSF data*[91].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of *TSF*[92].

6.1.7 ADDITIONAL PROTECTION AGAINST PHYSICAL ATTACKS

[84] [assignment: user data attributes].
[85] [assignment: action to be taken]
[86] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[87] [assignment: integrity errors]
[88] [assignment: specify the action to be taken upon integrity error]
[89] [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]]
[90] [selection: [assignment: parts of TSF], the TSF]
[91] [selection: [assignment: parts of TSF data], TSF data]
[92] [selection: [assignment: parts of TSF], TSF]

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.

FPT_PHP.3.1 The TSF shall resist *physical probing and manipulation*[93] to the [assignment: list of TSF devices/elements][94] by responding automatically such that the SFRs are always enforced.

6.1.8 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* [95].

6.1.9 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

FMT_MOF.1.1 The TSF shall restrict the ability to *disable*[96] the functions *the manufacturing test functions*[97] to *the Manufacturer*[98].

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.

[93] [assignment: physical tampering scenarios]
[94] [assignment: list of TSF devices/elements]
[95] [assignment: list of types of failures in the TSF]
[96] [selection: determine the behaviour of, disable, enable, modify the behaviour of]
[97] [assignment: list of functions]
[98] [assignment: the authorised identified roles]

6.1.10 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*[99] the *IC Identification Data*[100] to the *Manufacturer*[101].

6.1.11 RANDOM NUMBER GENERATION

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][102].

6.1.12 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*[103] the *Embedded OS*[104] to the *Manufacturer and the Card Issuer*[105].

[99] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[100] [assignment: list of TSF data]
[101] [assignment: the authorised identified roles]
[102] [assignment: a defined quality metric]
[103] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[104] [assignment: list of TSF data]
[105] [assignment: the authorised identified roles]

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*[106] the functions *Embedded OS Loading*[107] to *Manufacturer and the Card Issuer*[108].

6.2 ASSURANCE REQUIREMENTS

Security Assurance Requirements for the TOE for the evaluation of the TOE are those taken from the Evaluation Assurance Level 5 (EAL5) and augmented by taking the following components:

- ALC_DVS.2 Sufficiency of security measures
- AVA_VAN.5. Advanced methodical vulnerability analysis

[106] [selection: determine the behaviour of, disable, enable, modify the behaviour of]
[107] [assignment: list of functions]
[108] [assignment: the authorised identified roles]

6.3 SECURITY REQUIREMENTS RATIONALE

6.3.1 SFRS RATIONALE TABLE

	OT.Logical_Data_Access	OT.Security_Management	OT.Residual_Information_Protection	OT.Recovery_Environmental_Stress	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.Random_Number_Generation	OT.Unique_ID_Storage
FDP_ACC.1/Pre-Operational	X														
FDP_ACF.1/Pre-Operational	X														
FDP_ACC.1/Application	X														
FDP_ACF.1/Application	X														
FDP_ACC.1/Physical					X	X									
FDP_ACF.1/Physical					X	X									
FDP_ITT.1							X	X							
FCS_CKM.1/SP					X	X									
FCS_CKM.1/TP							X								
FCS_CKM.4					X	X	X								
FCS_COP.1/SP					X	X									
FCS_COP.1/TP							X								
FPT_SCP.1												X			
FMT_MSA.1															
FMT_MSA.3															
FMT_MTD.1/Ini_Per_Data_		X													
FPT_ITT.1					X		X	X							
FMT_SMF.1		X											X	X	
FMT_SMR.1		X											X	X	
FIA_AFL.1/Activation		X													

FIA_AFL.1/Initialisation		X												
FIA_AFL.1/Personalisation		X												
FIA_UID.1	X	X												
FIA_UAU.1	X	X												
FIA_UAU.5	X	X												
FDP_RIP.2			X											
FDP_ROL.1				X										
FPT_RCV.4				X										
FDP_SDI.2						X								
FDP_ITT.3								X						
FPT_TST.1						X			X	X				
FPT_PHP.3					X	X	X	X						
FPT_FLS.1											X			
FMT_MOF.1/Test													X	
FMT_MTD.1/ID														X
FCS_RND.1															X

Table 3: Security Functional Requirements Rationale

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: Security Functional Requirements Rationale

6.3.2 SFRS JUSTIFICATION

— **OT.Logical_Data_Acces**

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

— **OT.Security_Management**

FMT_SMR.1 and FMT_SMF.1 requires the necessary management functions and roles be present in the TOE. FIA_UID.1 and FIA_UAU.1 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 enables the secure entry of the authentication reference data to the TOE and protects from reading out and manipulations performed by the attackers.

- **OT.Residual_Information_Protection**

FDP_RIP.2 performs the residual information protection.

- **OT.Recovery_Environmental_Stress**

FDP_ROL.1 and FPT_RCV.4 will recover the user data and security functions from the failures resulting from environmental stress.

- **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 and FCS_COP.1/DP. FPT_PHP.3 provides additional protection against physical attacks.

- **OT.Data_Integrity**

FDP_SDI.2 and 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.

- **OT.Internal_TOE_Transfer_Confidentiality_Protection**

FDP_ITT.1 and FPT_ITT.1 provide 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.

- **OT.Internal_TOE_Transfer_Integrity_Protection**

FDP_ITT.3 monitors the integrity of the data transferred and performs the actions determined by the ST writer. FPT_PHP.3 provides additional 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.

- **OT.TSF_Operation_Protection**

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

- **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.

- **OT.Side_Channel_Protection**

FPT_SCP.1 protects the TOE from side channel attacks.

- **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.

- **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.

- **OT.Random_Number_Generation**

FCS_RND.1 provides the random number generation functionality that OT.Random_Number_Generation states.

- **OT.Test_Functions_Disable_Mechanism**

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

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.

- **OT.Flash_Loader_Authorization**

FIA_UAU.5 requires a Flash Loader Authentication mechanism exist and FIA_UAU.1 and FIA_UID.1 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.

- **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.

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/Application	FDP_ACF.1	FDP_ACF.1/Application
FDP_ACF.1/Application	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Application fulfilled by FMT_MSA.3
FDP_ACC.1/Physical	FDP_ACF.1	fulfilled by FDP_ACF.1/Physical
FDP_ACF.1/Physical	FDP_ACC.1 FMT_MSA.3	fulfilled by FDP_ACC.1/Physical 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
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
FCS_CKM.4	[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	fulfilled by FCS_CKM.1/SP

	FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	fulfilled by FCS_CKM.4
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	None	----
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	fulfilled by FDP_ACC.1/Application fulfilled FMT_SMR.1 fulfilled FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	fulfilled by FMT_MSA.1 fulfilled by FMT_SMR.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
FPT_ITT.1	None	----
FMT_SMF.1	None	----
FMT_SMR.1	FIA_UID.1	fulfilled by FIA_UID.1
FIA_AFL.1/Activation	FIA_UAU.1 Timing of authentication	fulfilled by FIA_UAU.1
FIA_AFL.1/Initialisation	FIA_UAU.1 Timing of authentication	fulfilled by FIA_UAU.1
FIA_AFL.1/Personalisation	FIA_UAU.1 Timing of authentication	fulfilled by FIA_UAU.1
FIA_UID.1	None	----
FIA_UAU.1	FIA_UID.1	fulfilled by FIA_UID.1
FIA_UAU.5	None	----

FDP_RIP.2	None	----
FDP_ROL.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	***fulfilled*** by FDP_ACC.1/Pre-Operational
FPT_RCV.4	None	----
FDP_SDI.2	None	----
FDP_ITT.3	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FDP_ITT.1 Basic internal transfer protection	fulfilled by FDP_ACC.1/Physical fulfilled by FDP_ITT.1
FPT_TST.1	None	---
FPT_PHP.3	None	---
FPT_FLS.1	None	---
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/Identification	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	fulfilled by FMT_SMR.1 fulfilled by FMT_SMF.1
FCS_RND.1	None	---

Table 5: Dependencies for the SFRs

Justification 1: The FPT_ACF.1 applies to the all data. So security attribute management is not 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	fulfilled by FMT_SMR.1

	FMT_SMF.1 Specification of Management Functions	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 TOE within this PP aims to withstand attackers with attack potential of HIGH; so besides the functional requirements, the assurance requirements: architectural soundness and well defined and tested internals are important. EAL5 package requires semiformal design descriptions, a more structured (and hence analyzable) architecture, internal focused testing which EAL4 does not require. So assurance requirements for the TOE and EAL5 match. Since reverse engineering is also an important treat for the TOE and the required assurance from Development Environment is high; ALC_DVS.2 is added. Finally to meet withstand attackers with HIGH attack potential AVA_VAN.5 added.

EAL5 to EAL4 Differences

EAL4	**EAL5**
ADV_FSP.4	ADV_FSP.5
---	ADV_INT.2
ADV_TDS.3	ADV_TDS.4
ALC_CMS.4	ALC_CMS.5
ALC_TAT.1	ALC_TAT.2
ATE_DPT.1	ATE_DPT.3
AVA_VAN.3	AVA_VAN.4

Table 7: Differences between EAL4 and EAL5

The dependencies for augmented SARs:

SAR	**Dependencies**	**Support of the Dependencies**
ALC_DVS.2	None	---
AVA_VAN.5	ADV_ARC.1 Security architecture description ADV_FSP.4 Complete functional specification ADV_TDS.3 Basic modular design ADV_IMP.1 Implementation representation of the TSF AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures ATE_DPT.1 Testing: basic design	Included in EAL5

Table 8: The Dependencies for augmented SARs

6.3.5 SECURITY REQUIREMENTS – MUTUAL SUPPORT AND INTERNAL CONSISTENCY

Current PP aims to withstand against attacker of HIGH 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