Public

Common Criteria Information Technology Security Evaluation

Security Target of

Samsung SP of S3B512C 32-bit RISC Microcontroller for Biometric Smart Card

Version 0.0

07th March 2023

SAMSUNG ELECTRONICS

SAMSUNG

Important Notice

Samsung Electronics Co. Ltd. (“Samsung”) reserves the right to make changes to the information in this publication at any time without prior notice. All information provided is for reference purpose only. Samsung assumes no responsibility for possible errors or omissions, or for any consequences resulting from the use of the information contained herein.

This publication on its own does not convey any license, either express or implied, relating to any Samsung and/or third-party products, under the intellectual property rights of Samsung and/or any third parties.

Samsung makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does Samsung assume any liability arising out of the application or use of any product or circuit and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

Customers are responsible for their own products and applications. "Typical" parameters can and do vary in different applications. All operating parameters, including "Typicals" must be validated for each customer application by the customer's technical experts.

Samsung products are not designed, intended, or authorized for use in applications intended to support or sustain life, or for any other application in which the failure of the Samsung product could reasonably be expected to create a situation where personal injury or death may occur. Customers acknowledge and agree that they are solely responsible to meet all other legal and regulatory requirements regarding their applications using Samsung products notwithstanding any information provided in this publication. Customer shall indemnify and hold Samsung and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim (including but not limited to personal injury or death) that may be associated with such unintended, unauthorized and/or illegal use.

Samsung Electronics Co., Ltd.
San #24 Nongseo-Dong, Giheung-Gu
Yongin-City, Gyeonggi-Do, Korea 446-711

Contact Us: *junghyun.kim@samsung.com*

Home Page: *http://www.samsungsemi.com*

Chip Handling Guide

Precaution against Electrostatic Discharge

When using semiconductor devices, ensure that the environment is protected against static electricity:

1. Wear antistatic clothes and use earth band.
2. All objects that are in direct contact with devices must be made up of materials that do not produce static electricity.
3. Ensure that the equipment and work table are earthed.
4. Use ionizer to remove electron charge.

Contamination

Do not use semiconductor products in an environment exposed to dust or dirt adhesion.

Temperature/Humidity

Semiconductor devices are sensitive to:

- Environment
- Temperature
- Humidity

High temperature or humidity deteriorates the characteristics of semiconductor devices. Therefore, do not store or use semiconductor devices in such conditions.

Mechanical Shock

Do not to apply excessive mechanical shock or force on semiconductor devices.

Chemical

Do not expose semiconductor devices to chemicals because exposure to chemicals leads to reactions that deteriorate the characteristics of the devices.

Light Protection

In non- Epoxy Molding Compound (EMC) package, do not expose semiconductor IC to bright light. Exposure to bright light causes malfunctioning of the devices. However, a few special products that utilize light or with security functions are exempted from this guide.

Radioactive, Cosmic and X-ray

Radioactive substances, cosmic ray, or X-ray may influence semiconductor devices. These substances or rays may cause a soft error during a device operation. Therefore, ensure to shield the semiconductor devices under environment that may be exposed to radioactive substances, cosmic ray, or X-ray.

EMS (Electromagnetic Susceptibility)

Strong electromagnetic wave or magnetic field may affect the characteristic of semiconductor devices during the operation under insufficient PCB circuit design for Electromagnetic Susceptibility (EMS).

Revision History

Revision No.	Date	Description
0.0	07th March 2023	- Creation for initial version

Table of Contents

List of Figures

List of Tables

List of Conventions

Register RW Access Type Conventions

Type	Definition	Description
R	Read Only	The application has permission to read the Register field. Writes to read-only fields have no effect.
W	Write Only	The application has permission to write in the Register field.
RW	Read & Write	The application has permission to read and writes in the Register field. The application sets this field by writing 1'b1 and clears it by writing 1'b0.

Register Value Conventions

Expression	Description
x	Undefined bit
X	Undefined multiple bits
?	Undefined, but depends on the device or pin status
Device dependent	The value depends on the device
Pin value	The value depends on the pin status

Reset Value Conventions

Expression	Description
0	Clears the register field
1	Sets the register field
x	Don't care condition

Warning: Some bits of control registers are driven by hardware or write operation only. As a result the indicated reset value and the read value after reset might be different.

List of Terms

Terms	Descriptions
Application Data	All data managed by the Security IC Embedded Software in the application context. Application data comprise all data in the final Security IC.
Composite Product Integrator	Role installing or finalising the IC Embedded Software and the applications on platform transforming the TOE into the unpersonalised Composite Product after TOE delivery. The TOE Manufacturer may implement IC Embedded Software delivered by the Security IC Embedded Software Developer before TOE delivery (e.g. if the IC Embedded Software is implemented in ROM or is stored in the non-volatile memory as service provided by the IC Manufacturer or IC Packaging Manufacturer)
Composite Product Manufacturer	The Composite Product Manufacturer has the following roles (i) the Security IC Embedded Software Developer (Phase 1), (ii) the Composite Product Integrator (Phase 5) and (iii) the Personaliser (Phase 6). If the TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice) he has the role of the IC Packaging Manufacturer (Phase 4) in addition.
End-consumer	User of the Composite Product in Phase 7.
IC Dedicated Software	IC proprietary software embedded in a Security IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
Initialisation Data	Initialisation Data defined by the TOE Manufacturer to identify the TOE and to keep track of the Security IC's production and further life-cycle phases are considered as belonging to the TSF data. These data are for instance used for traceability and for TOE identification (identification data).
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
Pre-personalisation Data	Any data supplied by the Card Manufacturer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases.
Security IC	Composition of the TOE, the Security IC Embedded Software, User Data and the package (the Security IC carrier).
Security IC Embedded Software	Software embedded in a Security IC and normally not being developed by the IC Designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3 or in later phases of the Security IC product life-cycle. Some part of that software may actually implement a Security IC application others may provide standard services. Nevertheless, this distinction doesn't matter here so that the Security IC Embedded Software can be considered as being application dependent whereas the IC Dedicated Software is definitely not.

Terms	Descriptions
Security IC Product	Composite product which includes the Security Integrated Circuit (i.e. the TOE) and the Embedded Software and is evaluated as composite target of evaluation in the sense of the Supporting Document
TOE Delivery	The period when the TOE is delivered which is either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or (ii) after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.
TOE Manufacturer	The TOE Manufacturer must ensure that all requirements for the TOE and its development and production environment are fulfilled. The TOE Manufacturer has the following roles: (i) IC Developer (Phase 2) and (ii) IC Manufacturer (Phase 3). If the TOE is delivered after Phase 4 in form of packaged products, he has the role of the (iii) IC Packaging Manufacturer (Phase 4) in addition.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE. This includes information about the TOE's configuration, if any is coded in non-volatile non-programmable memories (ROM), in specific circuitry, in non-volatile programmable memories (for instance E2PROM) or a combination thereof.
User data	All data managed by the Smartcard Embedded Software in the application context. User data comprise all data in the final Smartcard IC except the TSF data.

List of Acronyms

Acronyms	Descriptions
CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Feature
TSFI	TSF Interface
TSP	TOE Security Policy
SE	Secure Element
SP	Secure Processor
FP	Finger Print
HWACC	Hardware Accelerator
SP firmware	Secure Processor firmware
SFP	Security Function Policy
ECC	Error Correcting Code

1 ST INTRODUCTION

1 This introductory chapter contains the following sections:

1.1 Security Target and TOE Reference

1.2 TOE Overview and TOE Description

1.3 Interfaces of the TOE

1.4 TOE Intended Usage

1.1 Security Target and TOE Reference

2 The Security Target version is 0.0 and dated 07th March 2023
The Security Target is built on *Common Criteria version 3.1*

- Title: Security Target of Samsung SP of S3B512C Secure 32-Bit RISC Microcontroller for Biometric Smart Cards
- Target of Evaluation (TOE): SP of S3B512C
- TOE Revision[1]: 3
- Provided by: Samsung Electronics Co., Ltd.
- Common Criteria version:

[1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB–2017–04–001

[2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part2: Security Functional Components, Version 3.1, Revision 5, April 2017, CCMB–2017–04–002

[3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, CCMB–2017–04–003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB–2017–04–004

1.2 TOE Overview and TOE Description

1.2.1 Introduction

3 The TOE is the SP of the Biometric Smart Card with security functionalities are finger image capture, feature extraction, and secure transmission of fingerprint features to the Secure Element of the Biometric Smart Card by AES encryption. All the matching and decision of fingerprint authentication mechanism is in SE of S3B512C which is not TOE.

1.2.2 TOE Definition

4 The SP of S3B512C single-chip CMOS micro-controller is designed and packaged specifically for "Biometric Smart Card" applications.

5 The Cortex-M33 CPU architecture of the SP of S3B512C microcontroller follows the Harvard style, that is, it has separate program memory and data memory. Both instruction and data can be fetched simultaneously without causing a stall, using separate paths for memory access.

6 The main security features of the SP of S3B512C integrated circuit are:

- Secure fingerprint image capture and feature extraction provided by TOE SP firmware, integrity protected.

[1] TOE Revision includes the SP hardware version, SP firmware version and SP Data version specified in Table 1.

- Access control of Users to Flash memory positions where SP firmware is executed.
- TOE Unique Identification
- Countermeasures to avoid attackers reproduction of fingerprint data.
- An AES hardware block supporting AES encryption and decryption with keys in ECB mode. The AES block supports encryption of fingerprint features to be sent to SE of S3B512C.

7 The main hardware blocks of the SP of S3B512C Integrated Circuit are described in Figure 1 below:

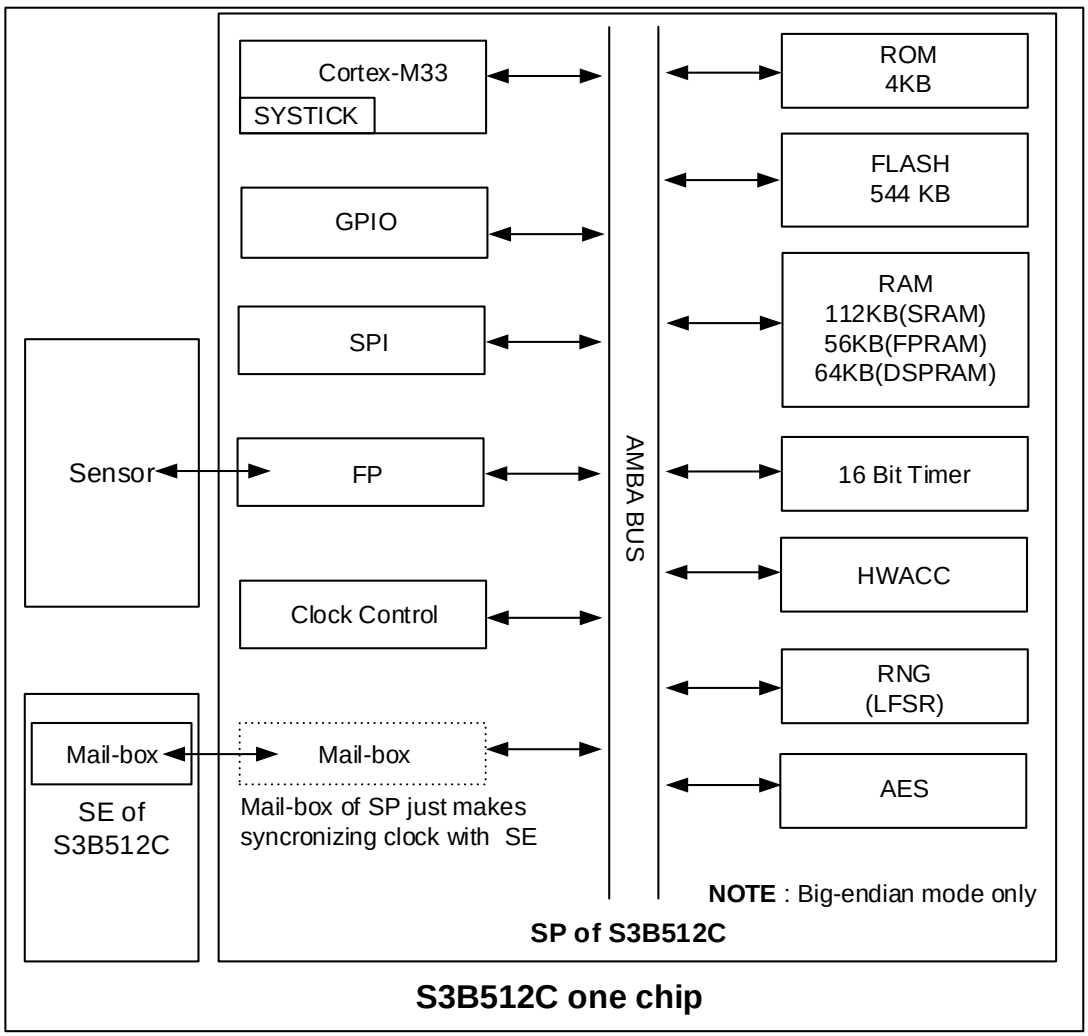


Figure 1 SP of S3B512C Block Diagram

NOTE: The Sensor chip is out of the TOE
NOTE: The SE of S3B512C chip is out of the TOE
NOTE: SE has all responsibilities of Mail-box communication between SE and SP

The TOE has the following Hardware and Software characteristics:

TOE Hardware Characteristics

- 32-bit ARM Cortex-M33 for Central Processing Unit (CPU)
- 544Kbytes of FLASH / 112Kbytes(SRAM)/56Kbytes(FPRAM)/64Kbytes (DSPRAM) for all devices in the device family
- Detectors & Sensors
- Filters
- Address & data buses
- Internal Clock
- Timers
- Power on Reset
- Random Number Generator LFSR
- AES hardware supporting encryption and decryption in ECB mode
- Mailbox to communicate with SE of S3B512C
- HWACC performs actual DSP operation (2D Convolution, MAC, ADD operation)
- FP controls sensor

TOE Software Characteristics

- SP Firmware
  - Capture/ Extraction

8 **The TOE configuration is summarized in table 1 below:**

Item type	Item	Version	Form of delivery
Hardware	SP Hardware	1.0	Wafer or Module
Software	SP Firmware	4.0[2]	Softcopy
Software	SP Data	3.0[3]	Softcopy
Document	S3B512C_SP_Firmware_AN	0.7	Softcopy
Document	S3B512C_SP_Loader_TN	0.3	Softcopy
Document	S3B512C_SP_UM	0.4	Softcopy
Document	S3B512C_SP_DV	0.5	Softcopy

Table 1 TOE Configuration

[2] Checksum of SP Firmware is part of Firmware identification. For given FW version, checksum is '06CE'.

[3] Checksum of SP Firmware data is part of Firmware identification. For given FW Data version, checksum is '2C49'.

9 **The delivery method is summarized in table 2 below:**

Item	Method of delivery
Hardware	Secure carrier
Documents	Documents are encrypted by PGP encryption and then delivered by email.

Table 2 Method of delivery

1.2.3 TOE Features

10 **CPU**

- 32-bit Cortex-M33 core

11 **Memory**

- 544K–bytes Data/Program Memory (FLASH)
- 112K–byte Data Memory (SRAM)
- 56K-byte FPRAM
- 64 K-bytes DSPRAM

12 **FLASH Write Operations**

13 **ECC**

14 **Security sensors and detectors**

15 **Interrupts**

- Source for IRQ: IO1 buffer available
- Source for IRQ: 16-bit Timer, IO1 falling edge, Flash erase/write time end interrupts, security and AES operation end interrupts
- Software Interrupts

16 **Serial I/O Interface**

- GPIO
- SPI

17 **Mailbox to communicate with SE of S3B512C**

18 **HWACC performs actual DSP operation (2D Convolution, MAC, ADD operation)**

19 **FP controls sensor**

20 **Reset and Power Down Mode**

21 **Timers**

- 16–Bit Timer with 8 Bit prescaler.

22 **Clock Sources**

- External clock
- Internal clock

23 **Crypto**

- AES hardware supporting encryption and decryption in ECB mode

24 **Random Number Generator**

- A random number generator which is LFSR.

25 **Package**

- Wafer and Module

26 **IC Dedicated Software**

- Capture/ Extraction

1.2.4 TOE Life cycle

27 The following table describes the different locations of TOE life-cycle development and production:

Site/Building	Purpose	Phase
Hwasung Plant/ DSR Building	Development	Phase 2
Giheung Plant/ Line S1	Production(Wafer Fab)	Phase 3
Onyang Plant	Production(Warehouse/Delivery)	Phase 4
PKL Plant	Production (Mask House)	Phase 3
TESNA Plant	Wafer Testing, Pre-personalization	Phase 3
HANAMICRON Plant	Grinding/Sawing/Module/Packaging test	Phase 4

28 The TOE is the Secure Processor (SP) of the S3B512C. It is integrated in the same physical hardware than the Secure Element (SE) of the S3B512C. Therefore, the TOE life-cycle is equivalent to that of a Secure Element with the exception that "IC Embedded Software Development (Phase 1)" applies for SE of S3B512C only. The current TOE refers only to the part of the hardware of SP and its dedicated software.

29 The life-cycle of SP of S3B512C comprises Phase 2, Phase 3 and Phase 4:

- IC Development (Phase 2):
  - IC design (SP),
  - IC Dedicated Software development (SP)
- the IC Manufacturing (Phase 3):
  - integration and photomask fabrication (both SE and SP together),
  - IC production (both SE and SP together),
  - IC testing (both SE and SP together),
  - Initialization, and
  - Pre–personalization if necessary (both SE and SP together)
- the IC Packaging (Phase 4) can be include in the evaluation of the IC as an option:
  - Security IC packaging (and testing) (both SE and SP together),
  - Pre–personalisation if necessary. (if not done in phase 3) (both SE and SP together)

30 Other Phases of the below diagram are applicable for SE of S3B512.

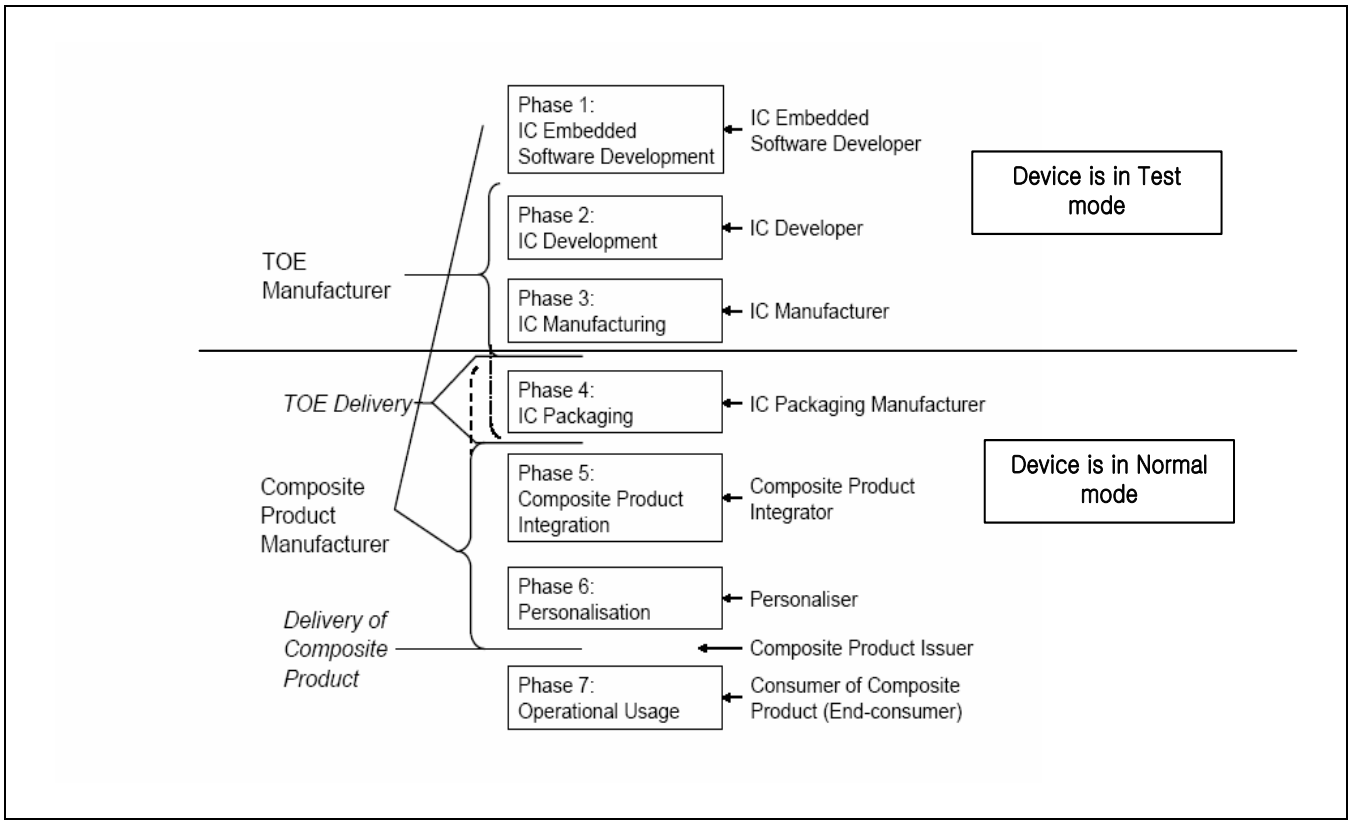


Figure 2 Definition of "TOE Delivery" and responsible Parties

31 The TOE can be offered to Composite developer in two configurations: (1) with Samsung SP firmware installed in SP Flash area during EDS (before TOE Delivery Phase), or (2) without any SP firmware installed.

32 In case (2) the development of SP firmware is considered part of "Phase 1: IC Embedded Software Development" and the Composite developer should develop SP firmware and include it in scope of Composite evaluation.

33 This Security Target only considers case (1) with Samsung SP firmware installed during IC manufacturing as the TOE in scope. Both case (1) and case (2) are clearly differentiated through TOE Identification process.

1.3 Interfaces of the TOE

34 TOE has the following interfaces:

- The physical interface of the TOE with the external environment is the entire surface of the IC.
- The electrical interfaces of the TOE with the external environment and the chip's pads including the VDD, RESETB, XCLK, GND.
- ADC (Analog Digital Convertor-AFE(Analog front end, RX/TX) is the interface with the FP sensor.
- The data interface between the SE and the SP is made of the Mailbox.
- The software interface of the TOE with the hardware consists of the SP Firmware commands.

1.4 TOE Intended Usage

35 The TOE is dedicated to application as:

- Within the context of banking and finance applications for credit or debit cards electronic purse (stored value cards) and electronic commerce, where the biometric fingerprint identification is a cardholder's authentication method, the TOE is intended to acquire the fingerprint image of the cardholder, process it and pass the fingerprint extracted features to the Secure Element.

36 Note SE is not TOE.

2 CONFORMANCE CLAIMS

37 This chapter 2 contains the following sections:

2.1 CC Conformance Claim

38 This Security target claims to be conformant to the Common Criteria version 3.1 R5.

39 Furthermore it claims to be CC Part 2 extended and CC Part 3 conformant. The extended Security Functional Requirements are defined in chapter 5.

40 This *Security Target* has been built with the Common Criteria for Information Technology Security Evaluation; Version 3.1 which comprises

[1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB–2017–04–001

[2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part2: Security Functional Components, Version 3.1, Revision 5, April 2017, CCMB–2017–04–002

[3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, CCMB–2017–04–003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB–2017–04–004

has been taken into account.

2.2 PP Claim

41 This ST does not claim conformance to any PP.

2.3 Package Claim

42 The assurance level for this Security Target is EAL2.

3 SECURITY PROBLEM DEFINITION

43 This chapter 3 contains the following sections:

3.1 Description of Assets

3.2 Threats

3.3 Organizational Security Policies

3.4 Assumptions

3.1 Description of Assets

44 The assets (related to standard functionality) to be protected are:

- the User Data and TSF Data, the following asset is explicitly mentioned:
  - **Biometric User Data**: This includes the live (actual) biometric data (actual user fingerprint) to be verified against the biometric reference. The biometric reference is stored in SE of S3B512C and comparison is in SE.

    Biometric reference and SE are not TOE.
- the SP Dedicated Software (SP Firmware) stored and in operation,
- the security services provided by the TOE for the SE of S3B512C (AES encryption/decryption).

45 The assets are related to the following high–level security concerns:

SC1 integrity of User data and TSF data,

SC2 confidentiality of User data and TSF data,

SC3 correct operation of the security services provided by the TOE to the SE of S3B512C.

46 Main asset of TOE is biometric live record and TOE firmware processing it. This is the fingerprint image of User which it captures, feature extraction and encrypts before sending to SE.

47 The process of User enrolment is assumed to be already performed assisted with additional security. The biometric reference is the result of the enrolment process. It is stored in SE.

48 SE hosts the matching library for authentication. TOE is only responsible of capturing User fingerprint, feature extraction and encryption and so the assets have been described in this section accordingly.

3.2 Threats

49 The following explanations help to understand the focus of the threats defined below from the identified security concerns:

- Manipulation of the biometric samples or the TOE Dedicated Software is main threat considering scenario in which the attacker manipulates the firmware or the extracted features of a fingerprint to break confidentiality or integrity of future biometric samples allowing to bypass the Biometric authentication system. This should be considered for the threat T.Unauthorized_Modification.
- Forgery of biometric samples information by monitoring and reproducing the digital data of a valid fingerprint image to gain access to Biometric Smart Card. This should be considered for the threat T.Reproduce.
- By abuse of the communication channel between SP and SE during User authentication, the attacker can try to disclose biometric data and gain access to the Biometric Smart Card. This should be considered for the threat T.Abuse_Communication.

50 The high-level security concerns are refined below by defining threats as required by the Common Criteria (refer to Figure 3).

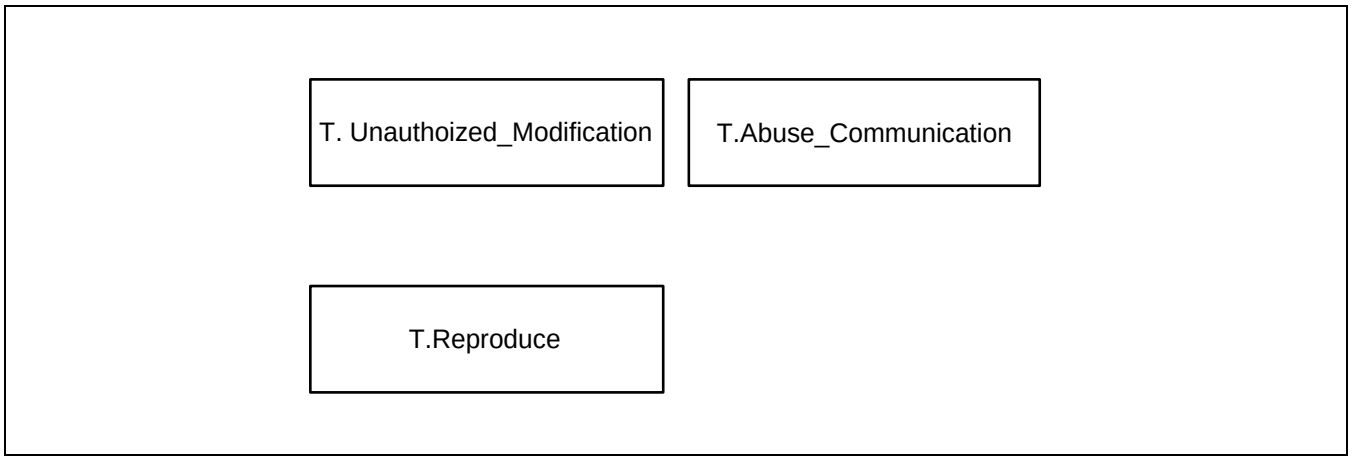


Figure 3 Threats

51 The TOE shall avert the threat "Unauthorized Modification of User/TSF data (T.Unauthorized_Modification)" as specified below.

T.Unauthorized_Modification	Unauthorized Modification of User/TSF data An attacker may try to modify assets like biometric image, biometric features, IC Dedicated Software or other security-relevant User authentication data from TOE memories or during usage. Such attacks could compromise the integrity of the User biometric attributes resulting in an unauthorized access to the Biometric Smart Card.

52 An attacker may also try to disclose and exploit sensitive information extracted from the TOE memories (like biometric image, biometric features or other security-relevant User authentication data) in an attempt of generating fake fingerprint data. This is considered in the next threat T.Reproduce.

53 The TOE shall avert the threat "Reproduction of Biometric data (T.Reproduce)" as specified below.

T.Reproduce	Reproduction of Biometric data An attacker may try to reproduce or generate the biometric characteristic of an authorized user directly by reading temporal data from TOE during processing of fingerprint features or images and try to reproduce such data to gain unauthorized access to the Biometric Smart Card.

54 In this way the attacker is trying to get access to the assets residing in the environment that should be protected with the support of the TOE remaining information from a successful authentication, or by the generation of the biometric characteristic from monitoring and reproducing temporal information obtained from the TOE during operation.

55 The TOE shall avert the threat "Abuse Communication between SP and SE (T.Abuse_Communication)" as specified below.

T.Abuse_Communication	Abuse Communication between SP and SE An attacker may interfere or monitor the trusted channel between SP and SE in order to modify biometric data to gain unauthorized access to the Biometric Smart Card.

3.3 Organizational Security Policies

56 The following Figure 4 shows the policies applied in this Security Target.

Figure 4 Policies

57 The IC Developer / Manufacturer must apply the policy "Protection during TOE Development and Production (P.Process–TOE)" as specified below.

P.Process–TOE	Protection during TOE Development and Production An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries a unique identification.

58 The TOE provides specific security functionality which can be used by the User to identify the TOE as genuine.

59 The IC Developer / Manufacturer must apply the policy "Cryptographic Service (P.Crypto-Service)" as specified below.

P.Crypto-Service	Cryptographic Services provided by the TOE The TOE shall provide the following cryptographic services to the IC Embedded Software: • Advanced Encryption Standard (AES)

3.4 Assumptions

60 The following Figure 5 shows the assumptions applied in this Security Target.

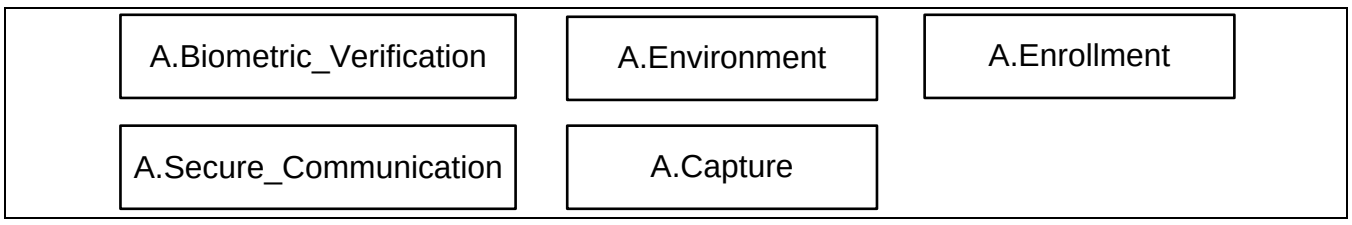


Figure 5 Assumptions

A.Environmnet	Environment

It is assumed that necessary TOE operating infrastructure is available at Secure Element for the cardholder's biometric authentication: e.g. authentication application as payment application, PIN backup for supporting biometric system failure, matching library and decision thresholds and criteria.

Specifically the following is assumed to be provided by SE: A database for the biometric reference of enrolled users, whereby confidentiality, integrity, authenticity and freshness are ensured.

The TOE is bound and operated by the Secure Element which is certified with the required security assurance level for the intended Biometric Smart Card application.

A.Capture	Capture device

The capture device, fingerprint sensor, has a user visible interface that operates inside its regular range and is suitable to be used with the TOE and for the intended applications of the Biometric Smart Card.

Furthermore, it is assumed that bypassing the capture device in a technical manner is not possible. Note this assumption does not prevent an attacker from presenting an imitated or recorded biometric characteristic to the capture device because such a misuse of the system would be possible. This ST does not cover this event.

A.Enrolment	Protection during enrolment

For the TOE, the enrolment is assumed to be already performed in a secure way and therefore, the biometric reference for each authorized user is assumed to be given. The generated reference is of sufficient quality and is linked to the correct user. The biometric references are assumed not known by an attacker.

A.Biometric_Verification	Protection during verification

All the verification, authentication, matching algorithm and decision making is conducted securely by the SE of S3B512C, including the proper management of errors FAR and FRR meeting recognized standards.

A.Secure_Communication	Secure communication

The SE ensures a secure communication of security relevant data from and to the TOE. The SE requesting a fingerprint image acquisition to the TOE is responsible, in particular, for generating the data required for the generation of the key for the trusted channel.

4 SECURITY OBJECTIVES

61 This chapter Security Objectives contains the following sections:

4.1 *Security Objectives for the TOE*

4.2 *Security Objectives for the* Operational Environment

4.3 *Security Objectives Rationale*

4.1 Security Objectives for the TOE

62 The TOE has the following high-level security goals related to the assets to avoid any abuse of the TOE security functionality:

SG1 maintain the integrity of the IC Dedicated Software for fingerprint image capture and feature extraction,

SG2 maintain the confidentiality and integrity of Biometric User Data when processed and when transmitted to SE,

SG3 maintain the correct operation of the secure channel with the SE,

SG4 avoid permanent storage of any biometric data and/or TSF data that could allow an attacker to take advantage of the biometric authentication system after the Biometric sample is transmitted to the SE, and

SG5 avoid dump of biometric features or biometric characteristics from TOE volatile memory during operation that could allow an attacker to gain unauthorized access to Biometric Smart Card.

63 These standard high-level security goals in the context of the security problem definition build the starting point for the definition of security objectives as required by the Common Criteria (refer to Figure 6).

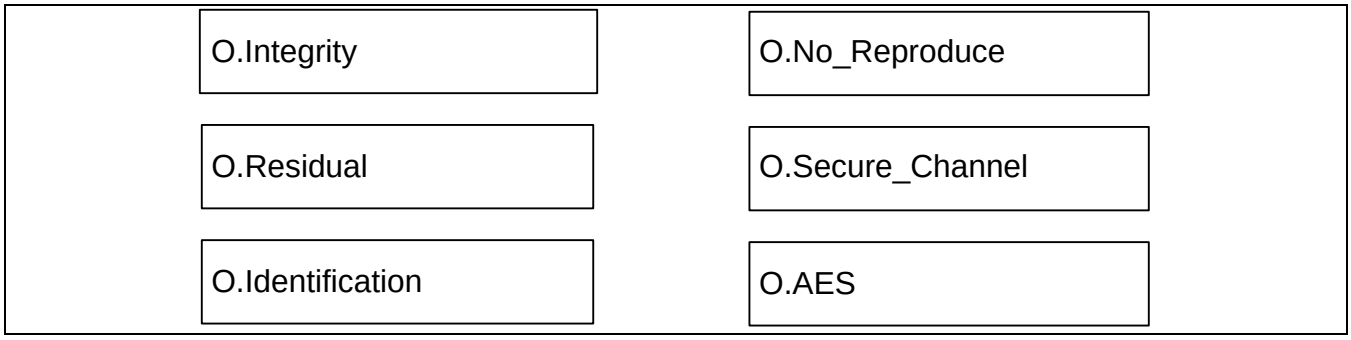


Figure 6 Standard Security Objectives

4.1.1 Standard Security Objectives

64 The TOE shall provide "Integrity of Biometric User Data and TSF Data (O.Integrity)" as specified below.

O.Integrity	Integrity of Biometric User Data and TSF Data The TOE must provide protection against modification of TOE firmware that could allow corruption or modification of biometric user data acquired, processed and/or transmitted by the TOE that could allow an unauthorized user to bypass the biometric authentication system.

65 The TOE shall provide "Protection against disclosure of Biometric User Data and TSF Data (O.Residual)" as specified below.

O.Residual	Protection against disclosure of Biometric User Data and TSF Data The TOE shall ensure that no residual or unprotected security relevant data remains in the TOE after biometric operations are completed or during processing

of biometric samples that could allow an attacker to bypass the biometric authentication system.

Here, security relevant data stands for Biometric User Data and TSF data which disclosure may allow attacker to bypass the biometric authentication system.

66 The TOE shall provide "Protection against forgery of biometric samples (O.No-Reproduce)" as specified below.

O.No-Reproduce Protection against forgery of biometric samples

The TOE must avoid attempts of attackers to monitor and reproduce fingerprint features or any other fingerprint data temporary stored in TOE during operation that could allow to gain unauthorized access by reproducing or generating forged biometric data.

67 The TOE shall provide "Secure communication with SE (O.Secure-Channel)" as specified below.

O.Secure-Channel Secure communication with SE

The TOE shall be able to communicates with SE through a secure channel in order to transmit Biometric User Data protecting the confidentiality and the integrity of the biometric data.

68 The TOE shall provide "TOE Identification (O.Identification)" as specified below.

O.Identification TOE Identification

The TOE must provide means to store Unique Identification Data in its non–volatile memory which shall be available for TOE User.

4.1.2 Security Objectives for Cryptographic Services

69 The TOE shall provide "Cryptographic service AES (O.AES)" as specified below.

O.AES Cryptographic service AES

The TOE provides secure hardware based cryptographic services for the AES for encryption and decryption.

4.2 Security Objectives for the Operational Environment

70 The following presents the security objectives defined for the operational environment.

71 The Operational Environment of the TOE shall provide "Enrolment of authorized users' biometric reference (OE.Enrolment)" as specified below.

OE.Enrolment Enrolment of authorized users' biometric reference

The biometric reference for each authorized user is given. The generated references shall be of sufficient quality and linked to the correct user. All

biometric references shall be stored in a secure way in the SE ensuring the confidentiality, authenticity, actuality and integrity of these data.

72 The Operational Environment of the TOE shall provide "Secure communication with the TOE (OE.Secure-Communication)" as specified below.

OE.Secure-Communication	Secure communication with the TOE
	The SE shall support TOE communication by generating the cryptographic key data required by the TOE to operate the secure channel. The SE shall correctly protect the secure channel related key material preventing Biometric User Data to be disclosed, modified, inserted, deleted and/or replayed.

73 The Operational Environment of the TOE shall provide "Authorization through fingerprint verification (O.Biometric-Verification)" as specified below.

OE.Biometric-Verification	Authorization through fingerprint verification
	The matching library and all required algorithms and decision thresholds meeting recognized standards to authorize users of the Biometric Smart Card through the biometric system are located and operated securely in SE.
	The TOE, it provides biometric samples with enough quality for the SE to conduct the verification and authorize only legitimate users.

74 The Operational Environment of the TOE shall provide the "Biometric infrastructure (O.Environmnet)" as specified below.

OE.Environment	Biometric infrastructure
	The Operational Environment and the Secure Element which achieves certified High assurance level provide the necessary infrastructure and data for the TOE to operate with the biometric samples (e.g. error rates, fingerprint reference database, authentication criteria, decision thresholds, matching algorithms).

75 The Operational Environment of the TOE shall provide "Suitable capture device (OE.Capture)" as specified below.

OE.Capture	Suitable capture device
	The capture device, as user visible interface, operates inside its regular range and is suitable for being used with the TOE. This includes that all environmental factors are appropriate with respect to the used capture device for fingerprint image acquisition. Because the capture device has to be accessible for each user, a moderate physical robustness is ensured.

4.3 Security Objectives Rationale

76 Table 4 below gives an overview, how the assumptions, threats, and organizational security policies are addressed by the objectives. The text following after the table justifies this in detail.

Assumption, Threat or Organizational Security Policy	Security Objective	Notes
T.Unauthorized_Modification	O.Integrity, OE.Biometric_Verification	
T.Reproduce	O.Residual, O.No_Reproduce, OE.Biometric_Verification	
T.Abuse_Communication	O.Secure_Channel, O.AES, OE.Secure_Communication	
P.Process-TOE	O.Identification	
P.Crypto-Service	O.AES	
A.Enrolment	OE.Enrolment	
A.Biometric_Verification	OE.Biometric_Verification	
A.Secure_Communication	OE.Secure_Communication	
A.Environment	OE.Environment	
A.Capture	OE.Capture	

Table 4 Relationship between Security Objectives, Assumptions, Threats and Policies

4.3.1 Countering the threats

77 The threat "Unauthorized Modification of User/TSF data (T.Unauthorized_Modification) is countered by the objective O.Integrity which ensures integrity of TOE firmware that could allow tampering of the biometric samples, acquired and processed, and by OE.Biometric_Verification which ensures that the fingerprint verification algorithms and processes are provided by SE with High assurance level.

78 The threat "Reproduction of Biometric data (T.Reproduce)"is fully countered by the security objectives O.No_Reproduce (as directly follows from the security objective definition) and O.Residual, which counters the possibility to exploit residual data from the TOE to bypass the biometric authentication system once the biometric operations are completed. OE.Biometric_Verification ensures that the fingerprint verification algorithms and processes are provided by SE with High assurance level.

79 The threat "Abuse Communication between SP and SE (T.Abuse_Communication)" is fully countered by the combination of security objectives O.Secure_Channel, O.AES and OE.Secure_Communication which provide the TOE with the cryptographic mechanisms and key-related material to avoid an attacker to abuse the trusted channel between SP and SE as described by the threat.

4.3.2 Coverage of the TOE security objectives

80 The security objective "Integrity of Biometric User Data and TSF Data (O.Integrity)" can be traced back to the threat T.Unauthorized_Modification which considers the scenario that an attacker modifies the TOE firmware and abuse the User biometric data to gain unauthorized access in the biometric system.

81 The security objective "Protection against disclosure of Biometric User Data and TSF Data (O.Residual) can be traced back to the threat T.Reproduce because it considers the scenario of an attacker exploiting TOE

remaining biometric information to generate forged biometric data in an attempt to gain a successful authentication after the authentication process is finished.

82 The security objective "Protection against forgery of biometric samples (O.No_Reproduce)" can be traced back to the threat T.Reproduce as directly follows: the objective is stated in a way that directly corresponds with the description of the threat.

83 The security objective "Secure communication with SE (O.Secure_Channel)" can be traced back to the threat T.Abuse_Communication as it is stated in a way that directly corresponds with the description of the threat.

84 The security objective "Cryptographic Service AES (O.AES)" can be traced back to OSP P.Crypto-Service and to threat T.Abuse_Communication because the cryptographic service is demanded by the Secure Element to receive the biometric samples from the TOE with AES encryption. Therefore, AES protects the data through the communication channel with SE as mandated by T.Abuse_Communication.

85 The security objective "TOE Identification (O.Identification)" can be traced back to OSP P.Process-TOE and it is stated in a way that directly corresponds with the description of the organizational security policy.

4.3.3 Coverage of the assumptions

86 The assumption "Capture device (A.Capture)" is covered by security objective OE.Capture as directly follows.

87 The assumption "Protection during enrolment (A.Enrolment)" is covered by security objective OE.Enrolment as directly follows.

88 The assumption "Environment (A.Environment)" is covered by security objectives OE.Environment as directly follows.

89 The assumption "Protection during verification (A.Biometric_Verification)" is covered by security objective OE.Biometric_Verification as directly follows.

90 The assumption "Secure communication (A.Secure_Communication)" is covered by objective OE.Secure_Communication as directly follows.

91 For all assumptions, the corresponding objectives for the Operational Environment are stated in a way which directly corresponds to the descriptions of the assumptions. It is clear from the description of each objective that the corresponding assumption is covered, if the objective is valid. Nevertheless some objectives exceed the statements of the assumptions they cover.

4.3.4 Coverage of the organizational security policies

92 The justification related to the organizational security policy "Protection during TOE Development and Production (P.Process-TOE)" is as follows: O.Identification requires that the TOE supports the possibility of a unique identification. The unique identification can be stored in the TOE. Since the unique identification is generated by the production environment it must support the integrity of the unique identification. Therefore, the organizational security policy P.Process-TOE is covered by O.Identification as far as organizational measures are concerned.

93 The justification related to the organizational security policy "Cryptographic Service (P.Crypto-Service)" is as follows: Since O.AES requires the TOE to implement the same specific security functionality as required by P.Crypto-Service, the organizational security policy is covered by the objective.

5 EXTENDED COMPONENTS DEFINITION

94 This chapter 5 Extended Components Definition contains the following sections:

5.1 Definition of the Family FAU_SAS

5.1 Definition of the Family FAU_SAS

95 To define the security functional requirements of the TOE an additional family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

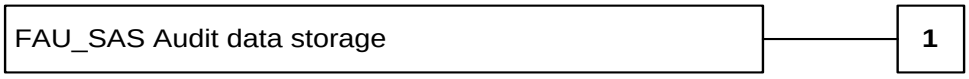
96 The family "Audit data storage (FAU_SAS)" is specified as follows.

FAU_SAS Audit data storage

Family behaviour

This family defines functional requirements for the storage of audit data.

Component levelling



FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
Management:	FAU_SAS.1 There are no management activities foreseen.
Audit:	FAU_SAS.1 There are no actions defined to be auditable.
FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide [assignment: *list of subjects*] with the capability to store [assignment: *list of audit information*] in the [assignment: *type of persistent memory*].

6 IT security requirements

97 This chapter 6 IT Security Requirements contains the following sections:

6.1 Security Functional Requirements for the TOE

6.2 Security Assurance Requirements for the TOE

6.3 Security Requirements Rationale

6.1 Security Functional Requirements for the TOE

98 In order to define the Security Functional Requirements the Part 2 of the Common Criteria was used. However, some Security Functional Requirements need some clarification. Clarifications are identified as Application Notes below the associated SFR.

99 Please note that, the following conventions are used to state each Security Functional Requirement:

- Refinement operations are explicitly identified at the end of the SFR definition.
- Assignment operations are identified *italic*.
- Selection operations are identified by underline.

100 The following table summarizes all TOE functional requirements:

Class FAU: Security Audit	
FAU_SAS.1	Audit data storage
Class FDP: User Data Protection	
FDP_RIP.2	Full residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_ITT.1	Basic internal transfer protection
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
FDP_ITC.1	Import of user data without security attributes
Class FPT: Protection of the TSF	
FPT_ITT.1	Basic internal TSF data transfer protection
Class FTP: Trusted Path / Channels	
FTP_TRP.1	Trusted path
Class FCS: Cryptographic Support	
FCS_COP.1	Cryptographic operation
FCS_CKM.4	Cryptographic key destruction
Class FMT: Security Management	
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization

Table 5 Security Functional Requirements

6.1.1 Security Audit

101 The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria Part 2 extended).

FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
FAU_SAS.1.1	The TSF shall provide *the test process before TOE Delivery* with the capability to store *the Identification Data* in the *Flash memory*.
Dependencies:	No dependencies.
Application Note1:	The integrity and uniqueness of the unique identification of the TOE must be supported by the development, production and test environment.

6.1.2 User Data Protection

102 The TOE shall meet the requirement "Full residual information protection (FDP_RIP.2)" as specified below.

FDP_RIP.2	**Full residual information protection**
Hierarchical to:	FDP_RIP.1 Subset residual information protection
FDP_RIP.2.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from all objects.
Dependencies:	No dependencies.

103 The TOE shall meet the requirement "Basic internal transfer protection (FDP_ITT.1)" as specified below.

FDP_ITT.1	**Basic internal transfer protection**
Hierarchical to:	No other components.
FDP_ITT.1.1	The TSF shall enforce the *Data Processing Policy* to prevent the disclosure of user data when it is transmitted between physically-separated parts of the TOE.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
Application Note2:	The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically-separated parts of the TOE.

104 The following SFP *Data Processing Policy* is defined: Biometric User Data shall be acquired and processed by TOE only upon request of Secure Element and shall be transmitted to SE encrypted and with integrity control without remain stored into TOE memories after the biometric data is sent to SE.

105 The TOE shall meet the requirement "Import of user data without security attributes (FDP_ITC.1)" as specified below.

FDP_ITC.1	**Import of user data without security attributes**
Hierarchical to:	No other components.
FDP_ITC.1.1	The TSF shall enforce the *Key Share Control Policy* when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *none*.
Dependencies:	[[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialization

106 The following SFP *Key Share Control Policy* is defined for the requirement FDP_ITC.1: Import of key related material for secure channel communication must always come only from Secure Element through Mailbox interface.

107 The TOE shall meet the requirement "Stored data integrity monitoring and action (FDP_SDI.2)" as specified below.

FDP_SDI.2	**Stored data integrity monitoring and action**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring.
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for *ECC* on all objects, based on the following attributes: *Flash memory content*.
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF *corrects error data.*
Dependencies:	No dependencies.

108 The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below.

FDP_ACC.1	**Subset access control**
Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the *Memory Access Control Policy* on *all subjects (software with privilege mode), all objects (data including code stored in Flash memory) and all the operations defined in the Memory Access Control Policy*. *Subjects are software codes in Privilege mode.* *Objects are data stored in Flash memory.*
Dependencies:	FDP_ACF.1 Security attribute based access control

109 The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below.

FDP_ACF.1	**Security attribute based access control**
Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the *Memory Access Control Policy* to objects based on the following: *Flash memory area where firmware is stored*.
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *only Secure Element can communicate SP through Mailbox to request SP firmware processing*.
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

110 The following SFP *Memory Access Control Policy* is defined for the requirements FDP_ACC.1 and FDP_ACF.1: TOE Firmware can be only operated by Secure Element through data commands through Mailbox interface; TOE firmware responses to commands are only stored in Mailbox interface as answer back to Secure Element.

111 The TOE shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below.

FDP_UCT.1	**Basic data exchange confidentiality**
Hierarchical to:	No other components.
FDP_UCT.1.1	The TSF shall enforce the *Data Processing Policy* to transmit user data in a manner protected from unauthorized disclosure.
Dependencies:	[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]

112 The TOE shall meet the requirement "Data exchange integrity (FDP_UIT.1)" as specified below.

FDP_UIT.1	**Data exchange integrity**
Hierarchical to:	No other components.
FDP_UIT.1.1	The TSF shall enforce the *Data Processing Policy* to transmit user data in a manner protected from modification errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification has occurred.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

6.1.3 Protection of the TSF

113 The TOE shall meet the requirement "Basic internal TSF data transfer protection (FPT_ITT.1)" as specified below.

FPT_ITT.1	**Basic internal TSF data transfer protection**
Hierarchical to:	No other components.
FPT_ITT.1.1	The TSF shall protect TSF data from disclosure when it is transmitted between separated parts of the TOE.
Dependencies:	No dependencies.
Application Note3:	The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE.

6.1.4 Trusted Path / Channels

114 The TOE shall meet the requirement "Trusted path (FTP_TRP.1)" as specified below.

FTP_TRP.1	**Trusted path**
Hierarchical to:	No other components.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end-points and protection of the communicated data from modification, disclosure.
FTP_TRP.1.2	The TSF shall permit local users to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for *sending User Biometric Data encrypted and integrity protected to SE*.
Dependencies:	No dependencies.
Application Note4:	The term "local user" above refer only to Secure Element of S3B512C.

6.1.5 Cryptographic Support

115 The AES operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1	**Cryptographic operation**
Hierarchical to:	No other components.

FCS_COP.1.1	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Advanced Encryption Standard (AES)* and cryptographic key sizes *128bit, 192bit or 256bit key size* that meet the following: *[FIPS197], chapter 5*.
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] FCS_CKM.4 Cryptographic key destruction

116 The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

FCS_CKM.4	**Cryptographic key destruction**
Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *wipe session keys AES* that meets the following: *None*.
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]

6.1.6 Security Management

117 The TOE shall meet the requirement "Management of security attributes (FMT_MSA.1)" as specified below.

FMT_MSA.1	**Management of security attributes**
Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the *Memory Access Control Policy* to restrict the ability to modify the security attributes *Flash access privileges* to *none*.
Dependencies:	[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

118 The TOE shall meet the requirement "Static attribute initialisation (FMT_MSA.3)" as specified below.

FMT_MSA.3	**Static attribute initialisation**
Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the *Memory Access Control Policy* to provide *well defined* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2	The TSF shall allow the *none* to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

6.2 TOE Assurance Requirements

The Security Target will be evaluated according to

Security Target evaluation (Class ASE)

The TOE Assurance Requirements for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 2 (EAL2)

The assurance requirements are:

Class ADV: Development	
Architectural design	(ADV_ARC.1)
Functional Specification	(ADV_FSP.2)
TOE Design	(ADV_TDS.1)
Class AGD: Guidance documents activities	
Operational User Guidance	(AGD_OPE.1)
Preparative procedures	(AGD_PRE.1)
Class ALC: Life-cycle support	
CM Capabilities	(ALC_CMC.2)
CM Scope	(ALC_CMS.2)
Delivery	(ALC_DEL.1)
Class ASE: Security Target evaluation	
Conformance claims	(ASE_CCL.1)
Extended components definition	(ASE_ECD.1)
ST introduction	(ASE_INT.1)
Security objectives	(ASE_OBJ.2)
Derived security requirements	(ASE_REQ.2)
Security problem definition	(ASE_SPD.1)
TOE summary specification	(ASE_TSS.1)
Class ATE: Tests	
Coverage	(ATE_COV.1)
Functional Tests	(ATE_FUN.1)
Independent Testing	(ATE_IND.2)
Class AVA: Vulnerability assessment	
Vulnerability Analysis	(AVA_VAN.2)

6.3 Security Requirements Rationale

6.3.1 Rationale for the Security Functional Requirements

119 Table 6 below gives an overview, how the security functional requirements are combined to meet the security objectives. The detailed justification follows after the table.

Objective	TOE Security Functional Requirements
O.Integrity	– FDP_SDI.2 "Stored data integrity monitoring and action" – FDP_ACC.1 "Subset access control" – FDP_ACF.1 "Security attribute based access control" – FMT_MSA.1 "Management of security attributes" – FMT_MSA.3 "Static attribute initialization"
O.Residual	– FDP_RIP.2 "Full residual information protection"
O.No-Reproduce	– FDP_ITT.1 "Basic internal transfer protection" – FPT_ITT.1 "Basic internal TSF data transfer protection"
O.Secure-Channel	– FTP_TRP.1 "Trusted path" – FDP_UCT.1 "Basic data exchange confidentiality" – FDP_UIT.1 "Data exchange integrity"
O.Identification	– FAU_SAS.1 "Audit storage"
O.AES	– FCS_COP.1 "Cryptographic operation" – FCS_CKM.4 "Cryptographic key destruction" – FDP_ITC.1 "Import of user data without security attributes"

Table 6 Coverage of Security Objectives by Security Functional Requirements

120 The justification related to the security objective "Integrity of Biometric User Data and TSF Data (O.Integrity)" is as follows: the SFR FDP_SDI.2 requires the TSF to detect the integrity errors of the stored user data and react in case of detected errors; the SFRs FDP_ACC.1 and FDP_ACF.1 with the related Security Function Policy (SFP) "Memory Access Control Policy" restricts the access to memory areas where the IC Dedicated Software is stored only to the Secure Element bound to the TOE; the SFR FMT_MSA.3 requires that the TOE provides default values for the security attributes, since the TOE is a hardware platform these default values are generated by the reset procedure; together with the SFR FMT_MSA.1 that requires that the ability to change those security attributes is restricted to no one.

121 The justification related to the security objective "Protection against disclosure of Biometric User Data and TSF Data (O.Residual)" is as follows: the SFR FDP_RIP.2 requires the TSF to made unavailable for an attacker any residual information of the User authentication data that could allow to bypass the Biometric Authentication System.

122 The justification related to the security objective "Protection against forgery of biometric samples (O.No-Reproduce)" is as follows: the SFRs FDP_ITT.1 and FPT_ITT.1 require the TSF to protect the confidentiality of User data and TSF data while processed by the TSF, they explicitly require the prevention of disclosure of secret data (TSF data as well as User Data) when transmitted between separate parts of the TOE or while being processed. TOE memories are defined as "separate parts of the TOE" in these SFRs.

123 The justification related to the security objective "Secure communication with SE (O.Secure-Channel)" is as follows: the SFR FTP_TRP.1 requires the TSF to provide a communication path between SP and SE where the confidentiality and integrity of the biometric data transmitted to the SE are protected. Additionally, the SFRs FDP_UCT.1 and FDP_UIT.1 require the TSF to enforce the SFP "*Data Processing Policy*" to send the Biometric

User Data to SE protecting their confidentiality and integrity.

124 The justification related to the security objective "TOE Identification (O.Identification)" is as follows: the operations for FAU_SAS.1 are chosen in a way that they require the TOE to provide the functionality needed for O.Identification, the Identification Data (or parts of them) are used for TOE identification, the technical capability of the TOE to store Identification Data is provided according to FAU_SAS.1.

125 It was chosen to define FAU_SAS.1 explicitly (not using a given security functional requirement from Part 2 of the Common Criteria) for the following reason: the security functional requirement FAU_GEN.1 in Part 2 of the CC requires the TOE to generate the audit data and gives details on the content of the audit records (for instance data and time). The possibility to use the functions in order to store security relevant data which are generated outside of the TOE, is not covered by the family FAU_GEN or by other families in Part 2. Moreover, the TOE cannot add time information to the records, because it has no real time clock. Therefore, the new family FAU_SAS was defined for this situation.

126 The FCS_COP.1 meets the security objective "Cryptographic service AES (O.AES)" together with the SFRs FDP_ITC.1 and FCS_CKM.4 which require to import the required key material for AES encryption/decryption and the explicit destruction of such key material once utilized for the security objective.

6.3.1.1 Dependencies of Security Functional Requirements

127 Table 7 below lists the security functional requirements defined in this Security Target, their dependencies and whether they are satisfied by other security requirements defined in this Security Target. The text following the table discusses the remaining cases.

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FAU_SAS.1	None	No dependency
FDP_RIP.2	None	No dependency
FDP_SDI.2	None	No dependency
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes Yes
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes
FDP_UCT.1	FTP_ITC.1 or FTP_TRP.1 FDP_ACC.1 or FDP_IFC.1	Yes Yes
FDP_UIT.1	FDP_ACC.1 or FDP_IFC.1 FTP_ITC.1 or FTP_TRP.1	Yes Yes
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1 FMT_MSA.3	Yes Yes
FPT_ITT.1	None	No dependency
FTP_TRP.1	None	No dependency
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Yes Yes
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes See discussion below See discussion below
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes See discussion below

Table 7 Dependencies of the Security Functional Requirements

128 The dependency FMT_SMR.1 introduced by the two components FMT_MSA.1 and FMT_MSA.3 is considered to be satisfied because the access control specified for the intended TOE is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of a security functional requirement FMT_SMR.1.

129 The dependency FMT_SMF.1 introduced by the component FMT_MSA.1 is considered satisfied because the security attributes of the TOE memories are static and cannot be modified by any role nor the TSF. Therefore, the TSF management functions which should be identified in the component FMT_SMF.1 do not exist in the TOE.

6.3.2 Rationale for the Security Assurance Requirements

130 The assurance level EAL2 has been chosen for this type of TOE due to the special nature of the Biometric Smart Card technology in which all security functions related to User authentication are performed by the Secure Element while the Secure Processor is only in charge of acquiring, processing and passing the biometric sample to the SE encrypted.

131 In addition, the TOE does not store permanently any asset related to the User biometric identification. All biometric references are guarded by the SE.

132 EAL2 is chosen because it provides a basic assurance that the TOE operates as specified in the ST.

6.3.2.1 Dependencies of assurance components

133 The dependencies of the assurance requirements taken from EAL2 are fulfilled automatically.

7 TOE SUMMARY SPECIFICATION

134 This chapter 7 TOE Summary Specification contains the following sections:

7.1 List of Security Functional Requirements

7.1 List of Security Functional Requirements

SFR1: FAU_SAS.1: Audit data storage

135 This requirement is fulfilled by the traceability/identification data written once and for all during the manufacturing process.

SFR2: FDP_RIP.2: Full residual information protection

136 This requirement is achieved by firmware. All User data on SP is deleted after send to SE.

SFR3: FDP_SDI.2: Stored data integrity monitoring and action

137 This requirement is achieved by ECC in Flash.

SFR4: FDP_ACC.1: Subset access control

138 This requirement is achieved by Flash memory security attributes.

SFR5: FDP_ACF.1: Security attribute based access control

139 This is covered by the Privilege and User modes of the TOE.

SFR6: FDP_ITT.1: Basic internal transfer protection

140 When SE send command of SP firmware, SE power on SP and after finish command, SP power is cut off.

SFR7: FDP_UCT.1: Basic data exchange confidentiality

141 This requirement is achieved by AES encryption of User data between SE and SP.

SFR8: FDP_UIT.1: Data exchange integrity

142 This requirement is achieved by checksum of User data between SE and SP.

SFR9: FDP_ITC.1: Import of user data without security attributes

143 The TOE achieves this SFR by importing the key related data to generate the AES session key to transfer the biometric sample to the SE for a particular authentication session.

SFR10: FPT_ITT.1: Basic internal TSF Data transfer protection

144 This requirement is achieved by synthesizable processor core and de-synchronization mechanisms.

SFR11: FTP_TRP.1: Trusted path

145 A trusted path is established between SE and SP on the Mailbox interface with AES encrypted data and checksum exchange.

SFR12: FCS_COP.1: Cryptographic operation

146 This requirement is covered by AES operation.

SFR13: FCS_CKM.4: Cryptographic key destruction

147 This requirement is achieved by firmware. All key related data on SP is deleted after Biometric User data is sent to SE.

SFR14: FMT_MSA.1: Management of security attributes

148 All security attributes of TOE Flash memory have DEFAULT values and cannot be modified once defined.

SFR15: FMT_MSA.3: Static attribute initialization

149 All security attributes of TOE Flash memory have DEFAULT values after Power on Reset.

8 Annex

8.1 References

[1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

[5] Joint Interpretation Library: Application of Attack Potential to Smartcards, January 2013, Version 2.9

[6] Supporting Document, Mandatory Technical Document: The Application of CC to Integrated Circuits, March 2009, Version 3.0, Revision 1, CCDB-2009-03-002

[7] Supporting Document Guidance: Smartcard Evaluation, February 2010, Version 2.0, CCDB-2010-03-001

[8] Supporting Document Guidance Security Architecture requirements (ADV_ARC) for smart cards and similar devices, April 2012, Version 2.0, CCDB-2012-04-003

[9] Supporting Document: Composite product evaluation for Smart Cards and similar devices, April 2012, Version 2.1, CCDB-2012-04-001

[10] Supporting Document Mandatory Technical Document: Application of Attack Potential to Smartcards April 2012, Version 2.8, CCDB-2012-04-002

[11] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation

[12] [FIPS 197] Advanced Encryption Standard (AES), 2001-11-26