DOCUMENT	ST
LEVEL	Confidential

Security Target of Argrace IoT Security Communication Module (BLE + Wi-Fi) V2.0A-009

V1.5-22/4/2022

REVISION HISTORY

Version	Date	Modification	Author
1.0	June 15, 2021	First edition released	Eason Chan Zhuoqian Liang
1.1	June 29, 2021	Preliminarily defined the scope of TOE, Security problem, Security objectives and Security Functional Requirements	Eason Chan Zhuoqian Liang
1.2	July 13, 2021	Update the hardware description, software description, and security functions description of the TOE	Eason Chan Zhuoqian Liang
1.3	July 28, 2021	Update Security Functions, TOE Scope, Security Objectives, Security Functional Requirement, Summary	Eason Chan Zhuoqian Liang
1.4	January 28, 2022	Update SFR for TOE Modify according to EOR	Zhuoqian Liang
1.5	April 22, 2022	Modify according to feedback from TACSL	Zhuoqian Liang

CONTENTS

This page is intentionally left blank

1 ST Introduction

1.1 ST Reference

Table 1-1 ST reference

Item	Description
Document Title:	Security Target of Argrace IoT Secure Communication Module（BLE + Wi-Fi）
Version:	1.5
Release date:	April 22, 2022
Author:	Zhuoqian Liang, Eason Chan

1.2 TOE Reference

Table 1-2 TOE reference

Item	Description
Name:	Argrace IoT Secure Communication Module（BLE + Wi-Fi）
Version:	2.0A-009
Release Date	December 10, 2021

1.3 TOE Overview

1.3.1 Usage and Major Security Functions of the TOE

The TOE is used for providing security assurance for IoT host devices and IoT users, including functions such as identity authentication, information encryption and decryption, confidential information management, and access control.

Major security functions are listed in the following and all these functions need to be evaluated:

Table 1-3 Major security functions of the TOE

Security Function	Description
Cryptographic support (TSF_CST)	Cryptographic function: ➢ Cryptographic key derivation: derive 16-byte AES key with MD5 algorithm. ➢ Encryption & Decryption: encrypt and decrypt data with AES/CBC/PKCS5Padding and AES/ECB/ZeroPadding cryptographic algorithms.
User data protection	Restrictions of network connection:

(TSF_UDP)	➢ Cloud address restriction. ➢ APP connection restriction by application connection control policy.
Secure firmware update (TSF_SFU)	MD5 verification of firmware image.
Trusted path (TSF_TPH)	Trusted communication path between TOE and APP and cloud ➢ TOE establishes trusted data transfer path between itself and APP. ➢ TOE initiates TLS communication between itself and cloud.
Memory protection (TSF_MPN)	Flash data encryption.

1.3.2 TOE Type

The TOE type in this ST is a security communication module which is used in IoT devices.

1.3.3 Required non-TOE Hardware/Software/Firmware

Required non-TOE hardware: CPU

Required non-TOE firmware: IC Dedicated Software (ICDS)

Required non-TOE application: IoT Cloud, Mobile App

The normal operation of TOE needs to include the above three components: non-TOE hardware, non-TOE firmware and non-TOE system. The CPU, ICDS and TOE together constitute the IoT host device. The device can support the use of functions by connecting with the App and the cloud.

1.4 TOE Description

The Target of Evaluation (TOE) in this ST is an IoT Security Communications Module (SCM), which consists of TOE dedicated software and TOE hardware. Generally, the IoT SCM is integrated into an IoT host device. This SCM is to enable the IoT host device connection to network, establish secure communication network channel between the IoT device and other terminals (i.e. Cloud, Mobile APP.), encrypt the user data for the IoT Application of IoT device, and store the encryption data. The software of above features is called IoT Security Communication Embedded Software (IoT SCES).

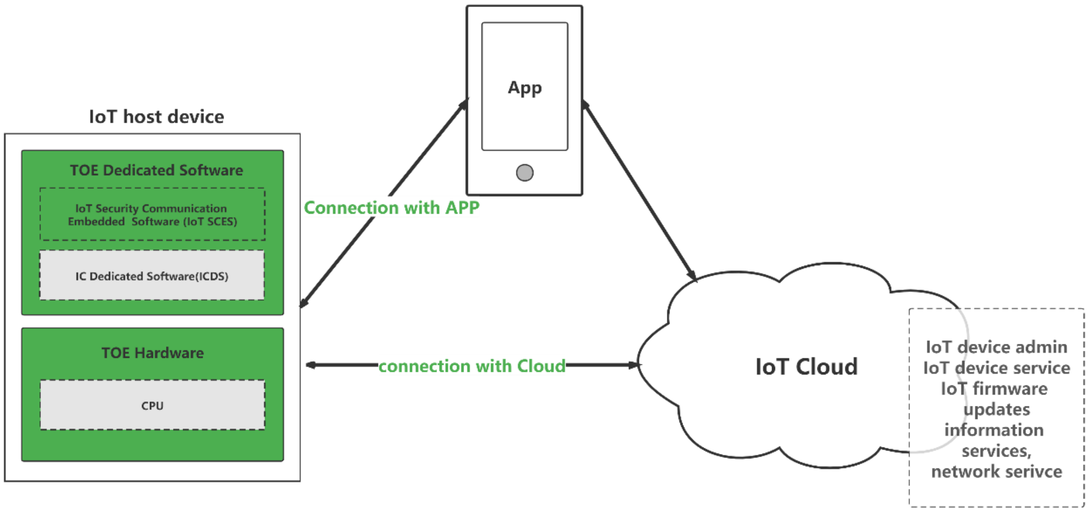

Figure 1-1 TOE (the green part) in the IoT device context

1.4.1 Physical Scope of the TOE

As shown in the following Table 1-4, the physical scope of the TOE consists of Hardware, Software and Documentation. For the hardware part, TOE includes the main components except CPU. The software part of TOE is called TOE dedicated software, which is mainly includes IoT Security Communication Embedded Software (IoT SCES) and except the IC dedicated software (ICDS). In addition, the Documentation called Argrace IoT Security Communication Module User Manual, is also in the scope of TOE, which provides user's guidance of TOE.

Table 1-4 Components of the TOE

Type	Name	Release Date	Form of delivery	Method of delivery
Hardware	Argrace IoT Secure Communications Module (Argrace IoT SCM)	June 3, 2021	Physical Module	Post
Software	IoT Security Communication Embedded Software (IoT SCES)	December 10, 2021	Embedded Software, *.bin	Post
Documentation	Argrace IoT Security Communication Module Users' Manual	March 28, 2022	Electrical Document, *.pdf	Email

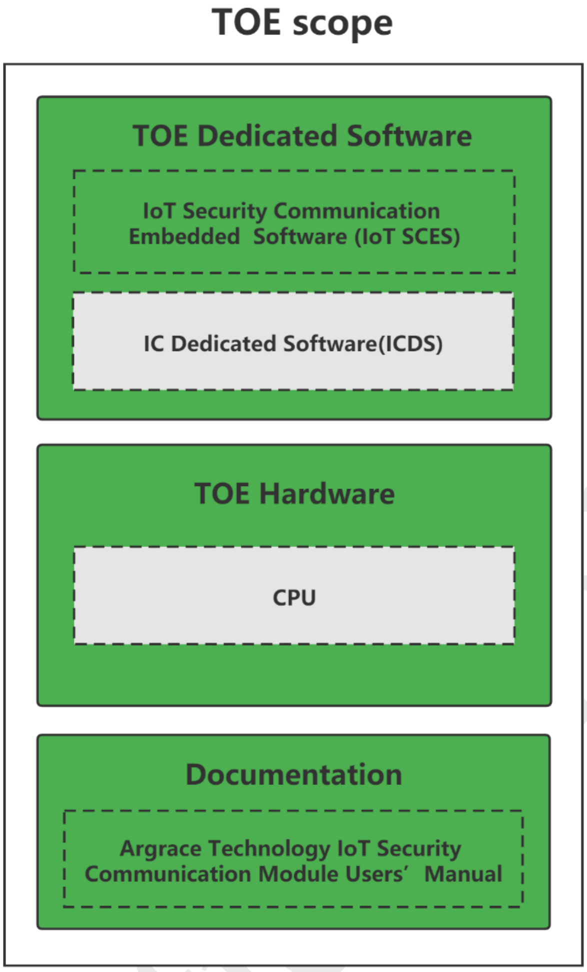
TOE scope
TOE Dedicated Software
IoT Security Communication Embedded Software (IoT SCES)
IC Dedicated Software(ICDS)
TOE Hardware
CPU
Documentation
Argrace Technology IoT Security Communication Module Users' Manual

Figure 1-2 TOE Physical Scope (The green part)

1.4.1.1 TOE Hardware Description

In this ST, TOE hardware is an IoT SCM, which is composed of I/O ports, physical memories (Flash and ROM), antenna connector and crystal oscillator. It provides the hardware functions required for operation of IoT dedicated software. In particular, the CPU that developed and provided by the third-party manufacturer is not in the scope of TOE hardware, which provides the security function of generating true random number.

1.4.1.2 TOE Dedicated Software

The TOE dedicated software in this ST operating on IoT SCM is called IoT Secure Communication Embedded Software (IoT SCES), which to implement the IoT device connection to network, establish secure communication network channel between the IoT device and other terminals (i.e., Cloud, mobile APP), encrypt and decrypt the data stored in Flash, and verify the firmware update image.

The IoT SCES is embedded in the IoT SCM, which is the operational environment of the IoT SCES. However, due to different requirements and certification, other than IoT SCES, the other embedded software (embedded software to fulfill IoT host device functions, non-security related) in IoT SCM should be excluded and is not part of the TOE scope.

The IoT Secure Communication Embedded Software comprises：

- IoT Secure Communication Embedded Software source code, which is stored in Flash.
- User data of the Composite TOE, especially personalization data and other data generated and used by the IoT Secure Communication Embedded Software, which is stored in Flash.

1.4.1.3 Documentation

The “Argrace IoT Security Communication Module Users’ Manual V1.0” is also part of the TOE which contains necessary description and guidance for users. In addition, the “Users’ Manual” also includes guidance and requirements focused on security aspects.

1.4.2 Logical Scope of the TOE

The logical scope of TOE is the security functions as follows:

1 Cryptographic support (TSF_CST):

The TOE can derive 128-bit AES keys from true random number generated by CPU using MD5 algorithm. The TOE supports 128-bit AES CBC mode encryption and decryption function.

2 User data protection (TSF_UDP):

The TOE can only connect to cloud with approved IP address. The TOE can only connect to mobile APP with mutually known initial key.

3 Secure firmware update (TSF_SFU):

The TOE verifies the MD5 value of firmware image. The approved MD5 values are delivered to TOE via trusted path from cloud.

4 Trusted path (TSF_TPH):

The TOE will establish secure communication channel with mobile APP via self-defined mechanism. All the data transferred is protected by 128-bit AES algorithm. The TOE will initiate TLS channel with cloud.

5 Memory protection (TSF_MPN):

The TOE will encrypt all the data stored in Flash by 128-bit AES algorithm.

1.4.3 Life Cycle Description

The life-cycle of the IoT SCM TOE includes the following phases:

1. Development of hardware and firmware of IoT SCM
2. Production of hardware and firmware IoT SCM
3. Delivery of completed IoT SCM to IoT device manufacturer.
4. Integration of IoT SCM into IoT host device
5. Delivery of IoT device to IoT device user
6. Normal operation by IoT device user and IoT admin

Phases 1 to 3 will be responsible by the IoT SCM developer. It shall be ensured that these phases are performed by trusted personnel in secure environments. Since the realization of the phases depend on the concrete SCM, it is important that the IoT SCM developer considers and enforces appropriate security measures during phases 1 to 3.

In phase 3, the certified IoT SCM has to be completed and no more modification of the configuration is allowed, except the firmware update of security application.

Phases 4 and 5 will be responsible by the IoT device manufacturer. The IoT device manufacturer shall regard the assumptions as stated in Section 3.4 hereinafter (as far as these assumptions are applicable, according to the concrete form factor of the IoT SCM and the way of integration into the IoT host device).

2 Conformance Claim

This chapter is divided into the following sections:

- CC Conformance Claim;
- Package Claim;
- PP Claim;
- Conformance Claim Rationale.

2.1 CC Conformance Claim

This Security Target and TOE claim to be conformant to the Common Criteria version 3.1, Revision 5.

Furthermore, they claim to be CC Part 2 conformant/extended and CC Part 3 conformant/extended.

This Security Target and TOE have been built with the Common Criteria for Information Technology Security Evaluation Version 3.1 which comprises:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017 (extended conformance with ***list of extended components*** defined in chapter 5).
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017 (extended conformance with ***list of extended components*** defined in chapter 5).
- Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Revision 5, April 2017.

2.2 Package Claim

The assurance level for this Security Target is EAL 2 augmented with:

- ALC_FLR.1

2.3 PP Claim

This Security Target does not claim conformance to Protection Profile.

2.4 Conformance Claim Rationale

No conformance claims rationale is necessary as this ST does not claim conformance to Protection Profile.

3 Security Problem Definition

This chapter contains the following sections:

- Assets
- Threats
- Organizational Security Policies
- Assumptions

3.1 Assets:

List of TOE assets here.

Asset	Description	Protection needs
IoT device data	Any data sent from the IoT device to the IoT cloud / IoT device admin. IoT device data may be produced by the IoT application, and/or IoT SCM. IoT device data includes device status data, response data of control, consumption information, billing information, etc. (can’t provide the full list data type because it depends on the concrete use case of the IoT device).	Integrity/ authenticity, confidentiality
External data	Any data received by the IoT device, originating from external network terminals, which the IoT device has established a network connection to. External data may be originated from the external network terminals (i.e., IoT cloud, mobile App, IoT devices etc.), or may be just forwarded by the external network device (e.g., IoT admin data, which are received by the IoT device through an IoT gateway). External data does not refer to any specific kind of data, but the data via an established security network connection with trusted terminals, and has been fully tested during phase1-4 life-cycle of the IoT SCM.	Integrity/ authenticity, confidentiality

IoT Platform Registration Key	Each IoT device has unique registration key in IoT Platform, which contains “Product Key”, “Device Name”, and “Device Secret”/ “Device credentials”. When SCM establishes communication channel with IoT cloud for the IoT device, the cloud will verify the IoT device’s registration key.	Integrity/ authenticity confidentiality resistance against timing analysis
SCM FW	IoT Secure Communication Embedded Software running on the TOE hardware	Integrity/ authenticity, confidentiality
SCM FW update version	Attribute of the SCM FW update image specifying its version. The version will be updated into SCM when the new SCM FW image completes update.	Integrity/ authenticity

3.2 Threats

T.SCM: Modification

The attacker may attempt to intercept the information received and sent between IoT devices that the IoT SCM TOE is integrated in during the communication between IoT SCM TOE and external terminals. Furthermore, the attacker may attempt to modify, integrate, and replay the data in various ways without being discovered by IoT SCM TOE and external terminals.

As a result, the IoT device obtains or receives wrong information.

T.SCM: Disclosure

The attacker may attempt to intercept the information received and sent between the IoT devices and external terminals through direct or indirect means, and gain knowledge about transmitted IoT device data or external device data.

As a result, the attacker has access to data sent or received by the IoT device the TOE is integrated in and retrieves confidential assets from that data**.**

T.SCM: Impersonation

The attacker may attempt to send information to the IoT device that the IoT SCM TOE is integrated in, impersonating one of the external terminals, or to send information to one of the external terminals, impersonating the IoT SCM TOE, without the respective receiving party being able to detect that

The attacker can complete the attack without access to the device, and is not discovered by the IoT SCM TOE.

As a result, the IoT device that the IoT SCM TOE is integrated in, or the IoT device users may receive malicious order or information.

T.SCM: IllegalConnection

A faulty or maliciously modified IoT application may try to establish a network connection to external network devices/addresses, which are not related to the operation of the IoT device, possibly ending up in confidential data being sent to the wrong entity in the network. Furthermore, a faulty or maliciously modified IoT application may try to establish a network connection to external network devices/addresses without establishing a secure communication channel, possibly ending up in confidential data being disclosed during transit or data being modified, substituted or replayed without the receiving party being able to detect that.

T.SCM: PhysicalProb

The attacker may attempt to physically disassemble and connect to the TOE to access, obtain user data and cryptographic key data.

As a result, the attacker has access to data and crack the ciphertext sent and received by the IoT device the TOE is integrated in.

3.3 Organizational Security Policies

P.SCM: FirmwareUpdate

The TOE should provide functionality to securely update its firmware, protected concerning authenticity and confidentiality. Only authentic SCM firmware update images as provided by the developer of the TOE shall be accepted by the TOE. Non-authentic SCM firmware update images or those being issued by the TOE developer but modified thereafter shall be rejected by the TOE. The TOE shall not accept a SCM firmware update image, if its firmware version is older than the version of the latest successfully installed firmware.

P.SCM: RNG

The TOE should use and rely on the trusted true random number source to get true random numbers. Such random number source can be a separate random generator or a CPU providing true random number generation function.

3.4 Assumptions

A.SCM: IoTManufacturer

It is assumed that the IoT device manufacturer understands which expected IoT host devices can be physically bound and integrated with the IoT SCM TOE, and this operation is not easy to implement. In addition, IoT device manufacturers can detect whether the device has been physically modified.

A.SCM: IoTApplication

It is assumed that the security requirements of the IOT application are consistent with the security functions provided by the IoT SCM TOE, and the IoT application uses the security functions provided by the IoT SCM TOE to protect the information received or sent, and to ensure that the data is sent to the expected device or from the expected device receiving data

A.SCM: Communication

It is assumed that IoT device manufacturers only use IoT SCM TOE as the only way for IoT host devices to communicate with external network devices, that is, IoT devices do not use other methods to communicate with external devices.

4 Security Objectives

This chapter describes the security objectives for the TOE and the Security Objectives for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development and production environment and security objectives for the operational environment.

The following are the Parts of this chapter.

- Security Objectives for the TOE;
- Security Objectives for the Operational Environment;
- Security Objectives Rationale.

4.1 Security Objectives for the TOE

The following Table lists the Security Objectives of this Security Target regarding the TOE.

Table 4-1: Security objectives for the TOE

O.SCM: AuthorityProt	Verify the authority of connected IoT external terminals.
O.SCM: ConfidentialProt	Data encryption and decryption when the TOE communicates with external terminals.
O.SCM: FirmwareUpdate	Firmware update image verification
O.SCM: MemoryProt	Data encryption for the data stored in the TOE memory
O.SCM: IllegalConnectionRest	Secured communication for data transfer and restricts illegal connections by specified connection address

O.SCM: AuthorityProt

Before the IoT SCM TOE communicates with IoT external terminals (i.e., Cloud, Mobile App), the authority of the external terminals should be verified.

O.SCM: ConfidentialProt

The TOE provides functionality of data confidentiality protection by encryption of data sent to an external network device, and by decryption of ciphertext data received from an external network device. The encryption mechanism(s) used shall provide security level of at least 128-bit AES algorithm.

O.SCM: FirmwareUpdate

The IoT SCM TOE provides functionality to securely update its firmware, protected concerning authenticity and confidentiality. Only authentic SCM firmware update images as provided by the developer of the TOE can be accepted by the TOE. Non-authentic SCM firmware update images or those being issued by the TOE developer but modified thereafter should be rejected by the TOE. The TOE should not accept a SCM firmware update image, if its firmware version is older than the version of the latest successfully installed firmware.

O.SCM: MemoryProt

The user data stored in TOE memory are encrypted through 128-bit AES key derived from true random number by AES algorithm.

O.SCM: IllegalConnectionRest

TOE establishes secured communication for data transfer between itself and external terminals. TOE restricts illegal connections attempt from other external terminals.

4.2 Security Objectives for the Operational Environment

The following Table lists the Security Objectives of this Security Target regarding the operational environment of the TOE:

Table 4-2: Security objectives for the operational environment

OE.SCM: IoTManufacturer	Manufacturer should confirm IoT host device can be physically integrated with the TOE correctly.
OE.SCM: IoTApplication	IOT applications should use the security functions provided by TOE and ensure the consistency of use.
OE.SCM: Communication	TOE should be the only way for IoT host device to communicate with external network devices.
OE.SCM: RNG	The TOE shall relay on the trusted CPU to get random numbers.

OE.SCM: IoTManufacturer

The IoT device manufacturer should understand which expected IoT host devices can be physically bound and integrated with the IoT SCM TOE, and this operation is not easy to implement. In addition, IoT device manufacturers shall detect whether the device has been physically modified.

OE.SCM: IoTApplication

The security requirements of the IOT application should be consistent with the security functions provided by the IoT SCM TOE, and the IoT application shall use the security functions provided by the IoT SCM TOE to protect the information received or sent, and to ensure that the data is sent to the expected device or from the expected device receiving data

OE.SCM: Communication

The IoT device manufacturers should only use IoT SCM TOE as the only way for IoT host devices to communicate with external network devices, that is, IoT devices do not use other methods to communicate with external devices.

OE.SCM: RNG

The TOE can use and rely on the IoT SCM CPU to generate true random numbers.

4.3 Security Objectives Rationale

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

Table 4-3: Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or Organizational Security Policy	Security Objective
T.SCM: Modification	O.SCM: AuthorityProt
T.SCM: Disclosure	O.SCM: ConfidentialProt
T.SCM: Impersonation	O.SCM: AuthorityProt
T.SCM: IllegalConnection	O.SCM: IllegalConnectionRest
T.SCM: PhysicalProb	O.SCM: MemoryProt
P.SCM: FirmwareUpdate	O.SCM: FirmwareUpdate
P.SCM: RNG	OE.SCM: RNG
A.SCM: IoTManufacturer	OE.SCM: IoTManufacturer
A.SCM: IoTApplication	OE.SCM: IoTApplication
A.SCM: Communication	OE.SCM: Communication

4.3.1 Justification of Security Objectives

Justification for each threat, OSP, and assumption.

T.SCM: Modification is directly countered by **O.SCM: AuthorityProt**, which states that the IoT SCM TOE shall complete the authority authentication with IoT external terminals and provide protection.

T.SCM: Disclosure is directly countered by **O.SCM: ConfidentialProt,** which states that the IoT SCM TOE shall provide confidentiality protection of information exchanged between IoT devices and external terminals.

T.SCM: Impersonation is directly countered by **O.SCM: AuthorityProt**, which states that the IoT SCM TOE should complete the authority authentication with IoT external terminals and provide protection.

T.SCM: IllegalConnection is directly countered by **O.SCM: IllegalConnectionRest**, which states that the TOE should establishes secured communication for data transfer and restricts illegal connections from external terminals.

T.SCM: PhysicalProb is directly countered by **O.SCM: MemoryProt,** which states that the TOE should encrypt the data stored in the memory.

P.SCM: FirmwareUpdate is directly enforced by **O.SCM: FirmwareUpdate**, which states that the TOE should verify the firmware update images.

P.SCM: RNG is directly enforced by **OE.SCM: RNG**, which states that the TOE should use trusted CPU to generate random numbers.

A.SCM: IoTManufacturer is directly upheld by **OE.SCM: IoTManufacturer** (objective re-states assumption).

A.SCM: IoTApplication is directly upheld by **OE.SCM: IoTManufacturer** (objective re-states assumption).

A.SCM: Communication is directly upheld by **OE.SCM: Communication** (objective re-states assumption).

5 Extended Components Definition

5.1 Definition of the component cryptographic key management (FCS_CKM.5)

This component describes functional requirements for key derivation as process by which one or more keys are calculated from either a pre-shared key or a shared secret and other information. The component is part of the family FCS_CKM of the class FCS. The component FCS_CKM.5 has been specified as follows:

Management: FCS_CKM.5

There are no management activities foreseen.

Audit: FCS_CKM.5

There are no actions defined to be auditable.

FCS_CKM.5	Cryptographic key derivation
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.5.1 The TSF shall derive cryptographic keys **[assignment: key type]** from **[assignment: input parameters]** in accordance with a specified cryptographic key derivation algorithm **[assignment: cryptographic key derivation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards].**

6 Security Functional Requirements

This chapter contains the following sections:

- Security Functional Requirement for the TOE
- Security Assurance Requirements for the TOE
- Security Requirements Rationale

This chapter describes the Security Functional Requirement of the ST, Operations such as the Selection, Assignment and Refinement of the ST will be highlighted as following:

1) Assignment: bold and between brackets

2) Selection: italics and between brackets

3) Refinement: underlying

4) Iteration: SFR/Identifier, bold

6.1 Security Functional Requirement for the TOE

This chapter describes the security requirements for the TOE.

In order to define the Security Functional Requirements Part 2 of the Common Criteria was used.

FCS_CKM.4: **Cryptographic key destruction**

Hierarchical to: No other components

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

FCS_CKM.4.1: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[delete cryptographic key instantly when complete session with the key]** that meets the following: **[FIPS 197, NIST SP 800-38A]**.

FCS_CKM.5 **Cryptographic key derivation**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.5.1 The TSF shall derive cryptographic keys [**AES key**] from [**Bluetooth device name, Specific string, true random numbers**] in accordance with a specified cryptographic key derivation algorithm [**MD5**] and specified cryptographic key sizes [**128 bits**] that meet the following: [**FIPS 197, NIST SP 800-38A**].

Application Notes: **Bluetooth device name** is the name of the device where the TOE is integrated. **Specific string** is a pre-defined string embedded in the source code of the TOE.

FCS_COP.1: Cryptographic operation

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]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1: The TSF shall perform **[encryption, decryption]** in accordance with a specified cryptographic algorithm **[AES/CBC mode/ PKCS5Padding, AES/ECB mode/ZeroPadding]** and cryptographic key sizes **[128 bits]** that meet the following: **[FIPS 197, NIST SP 800-38A]**.

FDP_ACC.1/Cloud: Subset of access control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1: The TSF shall enforce the **[network connection control policy]** on

[Objects: cloud

Subjects: IoT SCM

Operations: establishing network connection]

FDP_ACF.1/Cloud: Security attribute based access control

Hierarchical to:	No other components
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1:	The TSF shall enforce the **[network connection control policy]** to objects based on the following: **[objects: cloud; subjects: IoT SCM; attributes: requested IP address of cloud, TLS certificate**, **connection control rule (tuple of allowed IP address)]**
FDP_ACF.1.2:	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[network connection control policy: Establishing network connection to a cloud is allowed, if there is a connection control rule configured in the TOE, whose allowed network address matches the requested network address, and TLS handshake between TOE and cloud is successful].**
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: **[Establishing network connection to a cloud is denied if the requested network address does not match allowed network address].**

FDP_ACC.1/APP:	**Subset of access control**
Hierarchical to:	No other components
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1:	The TSF shall enforce the **[APP connection control policy]** on **Objects: APPs** **Subjects: IoT SCM** **Operations: establishing APP connections**

FDP_ACF.1/App:	**Security attribute based access control**

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute 25nitialization

FDP_ACF.1.1: The TSF shall enforce the **[APP connection control policy]** to objects based on the following: **[objects: APP; subjects: IoT SCM; attributes: Bluetooth device name, Specific string, connection control rule (Bluetooth device name + Specific string)].**

FDP_ACF.1.2: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[APP connection control policy: Establishing connection to a mobile APP is allowed if encrypted information sent by TOE can be decrypted by the mobile APP with initial key. The initial key is derived by MD5 of Bluetooth device name and Specific string. Bluetooth device name of TOE is public, and the Specific string is embedded in mobile APP source code and the TOE firmware source code during development and manufacturing phase].**

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].**

FDP_ACC.1/SCMFW: Subset of access control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1: The TSF shall enforce the **[IoT firmware update policy]** on

Objects: SCM firmware update image

Subjects: IoT SCM

Operations: SCM firmware update

FDP_ACF.1/SCMFW: Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1: The TSF shall enforce the **[IoT firmware update policy]** to objects based on the following: **[objects: SCM firmware update image; subjects: IoT SCM; attributes: MD5 of SCM firmware update image, SCM firmware update version, latest SCM firmware version].**

FDP_ACF.1.2: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[IoT firmware update policy: SCM firmware update is allowed, if the MD5 of SCM firmware update image is successfully verified against the corresponding SCM firmware update image and SCM firmware update version presented in the SCM firmware update request].**

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: **[SCM firmware update is denied, if the SCM firmware version presented in the SCM firmware update request is older than the latest SCM firmware version].**

FTP_ITC.1 **Inter-TSF trusted channel**

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **[the TSF]** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[Firmware update, Router connection information transfer].**

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist **[Memory physical reading]** to the **[Flash]** by responding automatically such that the SFRs are always enforced.

6.2 TOE Security Assurance Requirement

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 (EAL 2)

and augmented by the following components:

ALC_FLR.1

Table 5-1: Security Assurance Requirements

Assurance Class	Assurance Family	Assurance Level
Development	ADV_ARC.1 Security architecture description	2
	ADV_FSP.2 Security-enforcing functional specification	2
	ADV_TDS.1 Basic design	2
Guidance Documents	AGD_OPE.1 Operational user guidance	2
	AGD_PRE.1 Preparative procedures	2
Life Cycle Support	ALC_CMC.2 Use of a CM system	2
	ALC_CMS.2 Parts of the TOE CM coverage	2

	ALC_DEL.1 Delivery procedures	2
	ALC_FLR.1 Basic flaw remediation	augmented
Security Target Evaluation	ASE_CCL.1 Conformance claims	2
	ASE_ECD.1 Extended components definition	2
	ASE_INT.1 ST introduction	2
	ASE_OBJ.2 Security objectives	2
	ASE_REQ.2 Derived security requirements	2
	ASE_SPD.1 Security problem definition	2
	ASE_TSS.1 TOE summary specification	2
Tests	ATE_COV.1 Evidence of coverage	2
	ATE_FUN.1 Functional testing	2
	ATE_IND.2 Independent testing - sample	2
Vulnerability Assessment	AVA_VAN.2 Vulnerability analysis (refined)	2

6.3 Security Requirement Rationale

6.3.1 Rationale for the security functional requirements

Table 5-2 below gives an overview on how the security functional requirements are combined to meet the security objectives. The detailed justification follows after the table.

Table 5-2 Security Functional Requirements versus Security Objectives

Objective	TOE Security Functional Requirement	Justification
O.SCM: AuthorityProt	FCS_CKM.5	Defines the elements required for the initial key generation, algorithm and key sizes. And the initial key is used to verify the authority of connected mobile APP.
O.SCM:ConfidentialProt	FCS_CKM.4	Defines the cryptographic key destruction method.
	FCS_COP.1	Provides encryption and decryption function and defines the cryptographic algorithm and

		key sizes.
O.SCM: FirmwareUpdate	FDP_ACC.1/SCMFW	Defines the requirement for a firmware update policy and defines the corresponding objects, which can be updated, and the update operations.
	FDP_ACF.1/SCMFW	Defines the requirement for security attribute based access control for the update operations, the corresponding security attributes and the rules allowing only authentic images updated, and preventing downgrading.
	FTP_ITC.1	Establishes trusted channel for TOE to get requested MD5 value of firmware update image.
O.SCM: MemoryProt	FCS_COP.1	Provides encryption and decryption function and defines the cryptographic algorithm and key sizes.
	FPT_PFP.3	Provides the function that resists memory physical reading.
O.SCM: IllegalConnectionRest	FTP_ITC.1	Establishes trusted channel between TOE and external terminals.
	FDP_ACC.1/Cloud	Defines the requirement for network connection control policy and defines the corresponding objects (cloud) operations (connection establishment).
	FDP_ACF.1/Cloud	Defines the requirement for security attribute based access control for the connection establishment, the corresponding security attributes and the rules allowing only those connections, which have been configure in terms of connection control rules (security attribute). Requested connections, whose connection rules do not match the allowed, are denied.
	FDP_ACC.1/APP	Defines the requirement for APP connection control policy and defines the corresponding objects (mobile APP) operations (connection establishment).
	FDP_ACF.1/APP	Defines the requirement for security attribute based access control for the connection

		establishment, the corresponding security attributes and the rules allowing only those connections, which control the same initial key for TOE and mobile APP.

6.3.2 Dependencies of security functional requirements

Table 5-3 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.

Table 5-3: Dependencies of the Security Functional Requirements

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_CKM.4	FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2	No, but qualified by FCS_CKM.5
FCS_CKM.5	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Yes, qualified by FCS_COP.1 Yes
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	No, but qualified by FCS_CKM.5 Yes
FDP_ACC.1/Cloud	FDP_ACF.1	Yes
FDP_ACF.1/Cloud	FDP_ACC.1 FMT_MSA.3	Yes No, not applicable as qualified by FDP_ACF.1
FDP_ACC.1/APP	FDP_ACF.1	Yes
FDP_ACF.1/APP	FDP_ACC.1 FMT_MSA.3	Yes No, not applicable as qualified by FDP_ACF.1
FDP_ACC.1/SCMFW	FDP_ACF.1	Yes
FDP_ACF.1/SCMFW	FDP_ACC.1 FMT_MSA.3	Yes No, not applicable as qualified by FDP_ACF.1
FTP_ITC.1	/	
FPT_PHP.3	/	

As the above Table shows, all other dependencies of functional requirements are fulfilled by security requirements defined in this Security Target.

Note:

The dependency to FCS_CKM.1 is replaced by FCS_CKM.5. In this TOE, it does not directly use the function of Cryptographic key generation but use key derived from random number.

The dependency to FMT_MSA.3 is not applicable. There are no default values for the attributes of this access control policy as the controlled objects, i.e. the SCM firmware update image, cloud, and mobile APP are not created under this access control policy.

6.3.3 Rationale for the Assurance Requirements

The assurance level EAL 2 and the augmentation with the requirements ALC_FLR.1 was chosen in order to meet assurance expectations explained in the following paragraphs.

The primary use case for the IoT SCM is to be integrated in IoT host devices like smart home appliances running in a household with no physical access by potential attackers. Furthermore, there is an SFR that requires countermeasures against timing analyses. As finally the TOE has to be resistant against network-based penetration attacks, the evaluation assurance level EAL2 including vulnerability assessment component AVA_VAN.2 (refined) was chosen (providing assurance concerning resistance of the TOE against attackers possessing basic attack potential and requiring vulnerability analysis concerning all network services provided). The AVA_VAN.2 vulnerability analysis has to regard all applicable publicly known vulnerabilities. For the TOE’s main security needs, i.e. securely implemented network protocols and – if used – a securely implemented underlying general-purpose operating system, those are readily available in form of comprehensive public databases containing commonly known vulnerabilities. By the refinement of AVA_VAN.2, the vulnerability analysis explicitly has to cover known vulnerabilities for all network services provided by the TOE (and not only those related to its evaluated security functions), to make sure that the IoT SCM cannot be compromised by any kind of known network attack. For security flaws detected in the TOE once evaluated and certified, the TOE developer is expected to have basic flaw remediation procedures in place, therefore ALC_FLR.1 is augmented. (As long as a flaw could be remediated in firmware and no changes to the hardware of the TOE would be necessary, the TOE developer would simply issue a corresponding firmware update for the TOE as part of their flaw remediation procedure.)

7 TOE Summary Specification

TOE summary specification defines TOE security functions in line with known SFR, technologies referring to security mechanism or implementing TOE security functions, and security guarantee measures that meet known requirements of assurance.

7.1 Security Functional Requirements and Fulfillment

7.1.1 Cryptographic support (TSF_CST)

The TOE provides cryptographic support for data transfer and memory protection. For data transferred between TOE and mobile APP, the TOE utilizes CPU to generate a true random number, and then derives a 128-bit AES key from the random number via MD5 calculation to encrypts and decrypts data transferred. For the data stored in Flash, the TOE derives a 128-bit AES key via MD5 calculation of Bluetooth device name and Specific string, and then encrypts and decrypts data stored in Flash through this key.

In addition, the TOE will not store any derived keys. Every derived key will be deleted instantly after completion of cryptographic operations via this key.

<u>**SFRs:**</u>

- **FCS_CKM.5: Cryptographic key derivation**
- **FCS_CKM.4: Cryptographic key destruction**
- **FCS_COP.1: Cryptographic operation**

7.1.2 User data protection (TSF_UDP)

The TOE mainly ensures the security of user data by establishing connection control policy. For the connection between APP and TOE, the TOE enforces the rules based on key attributes, including Bluetooth device name and Specific string.

The rule is that a mobile APP is allowed to connect with TOE if encrypted information sent by TOE can be decrypted by the mobile APP with initial key. The initial key is derived by MD5 calculation of Bluetooth device name and Specific string. Bluetooth device name of TOE is public （It can be found when searching for devices through APP）, and the Specific string is embedded in mobile APP source code and the TOE firmware source code during development and manufacturing phase.

For the connection between Cloud and TOE, the TOE enforces the rules based on requested of IP address, TLS certificate, connection control rule (tuple of allowed network address).

The rule is that a cloud is allowed to connect with TOE if there is a connection control rule configured in the TOE, whose allowed network address matches the requested network address, and TLS handshake between TOE and cloud is successful.

SFRs:

- **FDP_ACC.1/Cloud: Subset of access control**
- **FDP_ACC.1/APP: Subset of access control**
- **FDP_ACF.1/Cloud: Security attribute based access control**
- **FDP_ACF.1/APP: Security attribute based access control**

7.1.3 Secure firmware update (TSF_SFU)

The TOE establishes the trusted channel with IoT cloud via TLS protocol. This ensures that the MD5 of requested firmware update image is delivered to the TOE securely.

The TOE will calculate the MD5 of received firmware update image and verify it with the requested MD5. If matches, update is allowed, otherwise, it will be denied. The TOE also compares version of the update firmware with the current firmware. If update firmware version is older than current one, it will be denied.

SFRs:

- **FTP_ITC.1: Inter-TSF trusted channel**
- **FDP_ACC.1/SCMFW: Subset of access control**
- **FDP_ACF.1/SCMFW: Security attribute based access control**

7.1.4 Trusted path (TSF_TPH)

The TOE is mainly connected to external terminals in two ways. One is to connect with cloud using HTTPS/TLS protocol for data transferring, especially secured firmware update. All connection requests with cloud must be authenticated using token that TOE requests from cloud according to TLS 1.2 protocol.

The other way is to connect with APP using self-defined secure path. After APP is successfully connected to TOE according to APP connection control policy, the TOE will send generated true random number encrypted by initial key to the APP. APP will decrypt the random number with its initial key and using this random number to derive 128-bit AES key. After that, all the data transferred between the TOE and APP will be encrypted by this 128-bit AES key during this session. When the session is completed, the key will be deleted instantly.

SFRs:

- **FTP_ITC.1: Inter-TSF trusted channel**

7.1.5 Memory protection (TSF_MPN)

The data stored in the Flash, such as user data and firmware is encrypted. All the data will be encrypted together before writing into the Flash. Therefore, all the data in the Flash is encrypted and secure.

SFRs:

- **FPT_PHP.3: Resistance to physical attack**

7.2 Mapping of SFR and TSF

The below Table shows the mapping between SFR and supporting TSF:

Table 7-1 Mapping between SFR and TSF

SFR	TSF				
	TSF_CST	TSF_UDP	TSF_SFU	TSF_TPH	TSF_MPN
FCS_CKM.4	√				
FCS_CKM.5	√				
FCS_COP.1	√				

FDP_ACC.1/Cloud		√			
FDP_ACF.1/Cloud		√			
FDP_ACC.1/APP		√			
FDP_ACF.1/APP		√			
FDP_ACC.1/SCMFW			√		
FDP_ACF.1/SCMFW			√		
FTP_ITC.1			√	√	
FPT_PHP.3					√