Public

Security Evaluation Standard for IoT Platform (SESIP)

ST Lite of Pavo

S3JU100

Class: ASE

Version 1.0

2025-12-03

ST (Security Target) Lite

SAMSUNG ELECTRONICS

Public

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.

WARNING No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electric or mechanical, by photocopying, recording, or otherwise, without the prior written consent of Samsung. This publication is intended for use by designated recipients only. This publication contains confidential information (including trade secrets) of Samsung protected by Competition Law, Trade Secrets Protection Act and other related laws, and therefore may not be, in part or in whole, directly or indirectly publicized, distributed, photocopied or used (including in a posting on the Internet where unspecified access is possible) by any unauthorized third party. Samsung reserves its right to take any and all measures both in equity and law available to it and claim full damages against any party that misappropriates Samsung’s trade secrets and/or confidential information.

警 告 本文件仅向经韩国三星电子株式会社授权的人员提供，其内容含有商业秘密保护相关法规规定并受其保护的三星电子株式会社商业秘密，任何直接或间接非法向第三人披露、传播、复制或允许第三人使用该文件全部或部分内容的行为（包括在互联网等公开媒介刊登该商业秘密而可能导致不特定第三人获取相关信息的行为）皆为法律严格禁止。此等违法行为一经发现，三星电子株式会社有权根据相关法规对其采取法律措施，包括但不限于提出损害赔偿请求。

Samsung Electronics Co., Ltd.
DSR, 1-1 SamsungJeonja-Ro, Hwaseong-Si, Gyeonggi-Do, Republic of Korea

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

SAMSUNG ELECTRONICS

VERSION HISTORY

Version	Date	Comment
1.0	2025-12-03	First release

TABLE OF CONTENTS

LIST OF FIGURES

1 REFERENCES

1.1 Normative references

[1] Car Connectivity Consortium CCC-TS-101: “Digital Key Release 3”, Version 1.2.3.

[2] GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.2, July 2023

[3] SESIP Profile for Ultra-Wideband (UWB) module: CCC-CP-025, Version 1.0

[4] S3JU100_DATASHEET_REV_1.5, Samsung Electronics, 30 Aug 2024

[5] S3JU100_Security_Technical_Note_v0.9, Samsung Electronics, 22 July 2025

1.2 Informative references

[6] GlobalPlatform Technology, Secure Channel Protocol '03' Card Specification v2.3 – Amendment D, Version 1.1.2, March 2019, Document Reference: GPC_SPE_014

[7] GlobalPlatform Technology, Secure Channel Protocol '11', Card Specification v2.3 – Amendment F, Version 1.2, July 2018, Document Reference: GPC_SPE_093

[8] FiRa UWB Command Interface (UCI) Technical Specification, Version 2.0

2 ABBREVIATIONS

2.1 Abbreviations

For the purposes of the present document, the following abbreviations apply:

Acronyms	Descriptions
AoA	Angle of Arrival
BL0	Bootloader 0
BL1	Bootloader 0
BLE	Bluetooth Low Energy
BPRF	Base Pulse Repetition Frequency
CCC	Car Connectivity Consortium
CMAC	Cipher-based Message Authentication Code
CPA	Code Protection Area
CVE	Common Vulnerabilities and Exposures
DKA	Digital Key Applet
DKF	Digital Key Framework
dUDSK	Derived UWB Data Secret Key
dURSK	Derived URSK
FFT	Fast-Fourier Transform
HPRF	Higher Pulse Repetition Frequency
mUPSK[1|2]	Master UWB Privacy Secret Key
mURSK	Master URSK
NFC	Near Field Communication
NVM	Non Volatile Memory
PSIRT	Product Security Incident Response Team
ROM	Read Only Memory
RoT	Root of Trust
SAU	Secure Attribution Unit
SE	Secure Element
SESIP	Security Evaluation Standard for IoT Platforms
SFR	Security Functional Requirements
SoC	System-on-a-Chip
SR-FW	Secure Ranging Firmware
ST	Security Target
STS	Scrambled Timestamp Sequence
TOE	Target Of Evaluation
ToF	Time of Flight
URSK	UWB Ranging Secret Key

UWB	Ultra-Wideband

3 INTRODUCTION

The S3JU100 is designed for secure ranging application based on the UWB standard [1] which can be integrated in devices used for digital car key, indoor navigation etc.

This Security Target document describes the S3JU100 security features against Security Evaluation Standard for IoT Platforms (SESIP) [2].

3.1 ST Reference

S3JU100, SESIP Security Target Lite, Revision 1.0, Samsung Electronics, 3 December 2025.

3.2 SESIP Profile Reference and Conformance Claims

Table 1 SESIP Profile for Ultra-Wideband (UWB) module Conformance Claims

Reference	Value
SP Name	SESIP Profile for Ultra-Wideband (UWB) module [3]
SP Version	Version 1.0
Assurance Claim	SESIP Assurance Level 3 (SESIP3)

3.3 Platform Reference

S3JU100 has following reference.

Table 2 Platform Reference

Reference	Value	
Platform Name and Version	HW version	S3JU100 EVT1
	Bootloader 0	BL0 v2.0.11
	Bootloader 1	BL1 v2.1.2
	Secure ranging firmware (SR-FW)	SR-FW v00.05.0500
Platform Type	UWB controller for secure ranging with its security services as trusted firmware	

Table 3 Guidance Documents

Document	Reference
Datasheet	S3JU100_DATASHEET_REV_1.5, Samsung Electronics, 30 Aug 2024
Security technical note	S3JU100_Security_Technical_Note_v0.91_Samsung Electronics 12 August 2025
Bootloader user manual	S3JU100_Bootloader_User_Manual_v0.4, Samsung Electronics, 07 Jan 2025

FW UCI user manual	S3JU100_FW_UCI_User_Manual_v0.25, Samsung Electronics, 13 June 2025
HW description document	S3JU100 Security. S3JU100_HW_Description_Document_v0.2, Samsung Electronics, 6 Aug 2024
HW register map	S3JU100 Security. S3JU100_Register_Map_v0.1, Samsung Electronics, 8 Aug 2024

3.4 Platform Overview and Description

The S3JU100 is a fully integrated Ultra Wideband (UWB) single chip solution which supports CH5 and CH9 frequency bands, 802.15.4z-based Base Pulse Repetition Frequency (BPRF), High Pulse Repetition Frequency (HPRF), and low power mode.

S3JU100 has two Cortex-M33 processors running with 512 KB NOR flash memory and 256 KB static RAM. It also supports ARM TrustZone technology, which can isolate secure domain from non-secure application. S3JU100 also provides hardware engines for cryptographic calculations such as AES accelerator, CRC32 calculator, True random number generator, PKE for big number multiplication and FFT.

S3JU100 provides external interface functions such as two SPI channels, one UART channel, several GPIOs and JTAG interface for debugging. For wireless connectivity, S3JU100 supports IEEE 802.15.4z with 6.5GHz and 8 GHz frequency. It has one transmitter and three receivers, which support ToF and AoA application.

The S3JU100 is designed for secure ranging application such as digital car key. SSS ™ (Security Sub System) technology is implemented for providing security solutions such as AES, SHA2, TRNG and PKE.

The S3JU100 is offering secure boot, secure firmware update, secure ranging and secure life cycle management with hardware cryptography. From a firmware perspective, the S3JU100 is composed of three parts. The BL0 serves as the root of trust for secure booting, sets up and manages the TrustZone, and supports secure downloading of the BL1. The BL1 is implemented to be updatable to support the functions required by the user, acts as an intermediary in the secure booting chain, and supports the download function of secure ranging firmware (SR-FW). The SR-FW supports secure ranging, communication with the SE, communication with the vehicle, and communication with the host.

3.5 Platform component functional overview and description

3.5.1 UWB module security features and scope

The UWB module is intended to be used by a mobile integrator as a basis for ranging computation solution along with an application processor and a Secure Element.

The UWB module scope and an integration in a final product is represented in Figure 1 below:

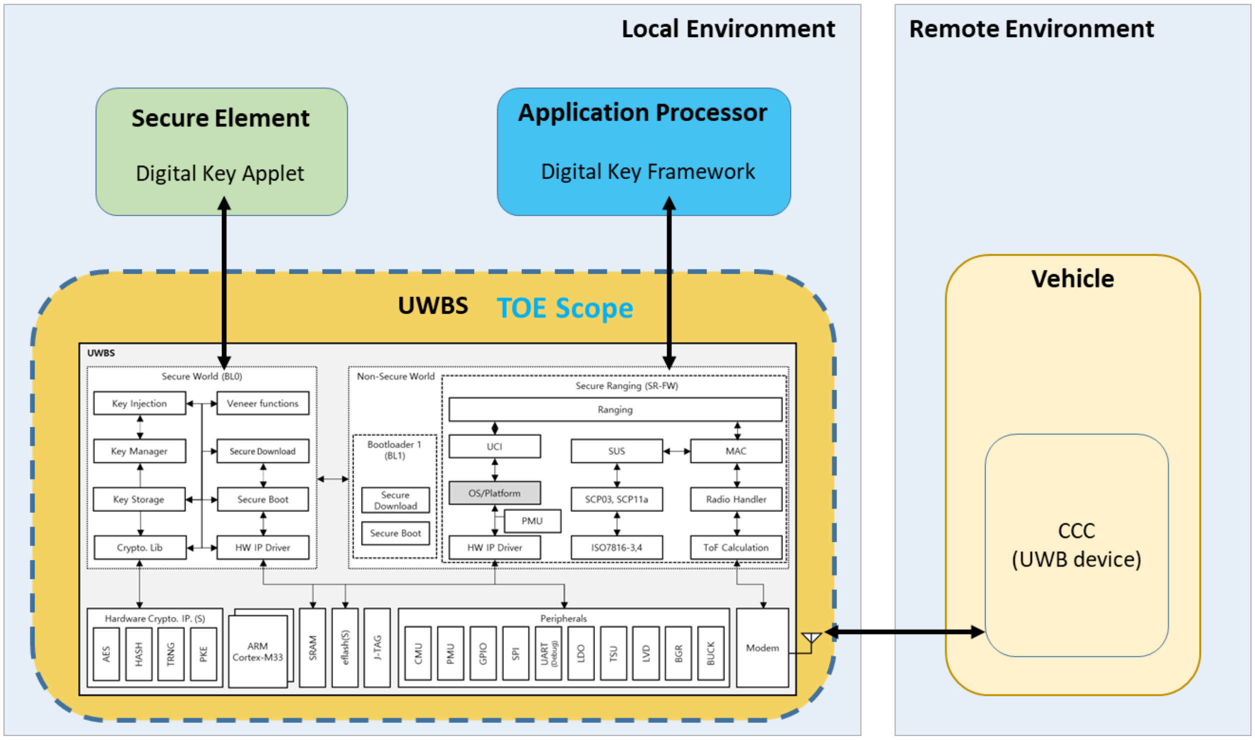


Figure 1. UWB module components and scope

The UWB module consists of hardware and firmware. The firmware is usually divided into three parts. First one is a BL0, which is immutable part, which typically includes at least the code performing the product initialization and update BL1, and second one is BL1, which is mainly used to update secure ranging firmware (SR-FW), which can be modified and updated during the product lifecycle.

The physical scope includes the product hardware components and the logical scope includes the product BL0, BL1 and secure ranging firmware (SR-FW).

- Isolation of Secure environment and Non-secure environment based on Arm TrustZone
- Hardware cryptography accelerators (symmetric, asymmetric, secure hash, KDF, etc.)
- Digital True Random Number Generator (DTRNG)
- Device configuration information, which can be used for identification of the platform. It includes device ID and manufacturing information
- Disable JTAG
- Secure boot which supports chain of trust from bootloader to firmware
- Firmware update that support integrity, confidentiality and authenticity using encryption and verification of the signature
- Secure communication between S3JU100 and SE, S3JU100 and Vehicle UWB by applying secure channel protocol defined in standard such as Global Platform and Car Connectivity Consortium

- Secure key management

The TOE provides the following hardware components and interfaces[1]:

List of S3JU100 hardware components and interfaces

Component / Interface	Description	Identification
Communication ports	Secure Element: SPI, GPIO. Application Processor: SPI, GPIO Vehicle: CCC PHY Radio (Modem)	See Table 2
Debug port	JTAG, UART	
Memories	SRAM and NVM(embedded Flash)	
Crypto IPs	TRNG, AES, SHA2/HMAC, Public Key Engine, CRC16/32	
Power Management	BUCK, LDO, LVD, BGR, PMU	
Clock Management	CMU (PLL)	
Temperature Measure	TSU	
CPU	ARM Cortex-M33 with TrustZone™	

The S3JU100 provides the following software components and interfaces[2]:

List of S3JU100 software components and interfaces

Component / Interface	Description	Identification / Version
BL0	Secure boot, secure bootloader 1 downloading, Crypto library, eFlash driver and TrustZone™ control	See Table 2
BL1	Secure boot, secure ranging firmware downloading	See Table 2
SR-FW	Secure ranging based on CCC standard Secure UWB service for communicating Secure Element 802.15.4z MAC and PHY for communicating UWB in Vehicle over the Air through radio frequency	See Table 2
Peripheral drivers	SPI driver, GPIO driver	
Communication protocols	Secure Element: SCP03 and SCP11a Vehicle: Secure ranging protocol defined in [CCC] Application Processor/DKF: UWB Command Interface (UCI)	See [6], [7] and [8]
<Others>	Temperature Control Unit, Power Management Unit including reset control.	See [5]

[1] Hardware interfaces are hardware modules and physical ports exposed to the environment.
[2] Software interfaces are the logical features exposed to the environment (including firmware).

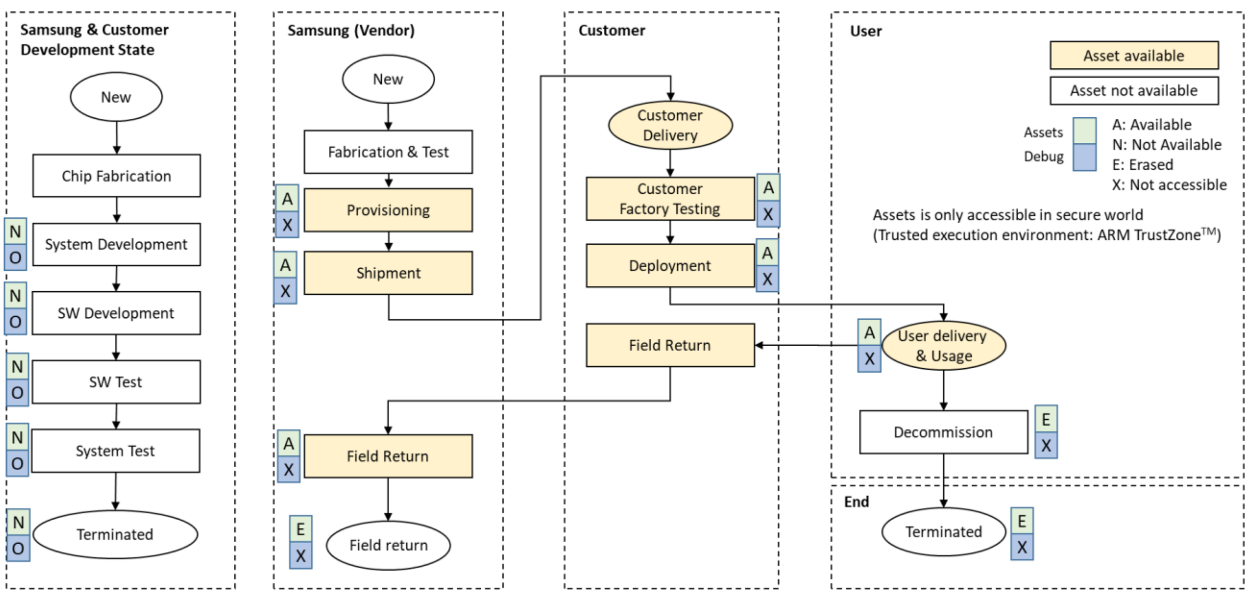
3.5.2 Life Cycle

This UWB module supports a security Life-Cycle state model. The current Life-Cycle state determines the device's debug functionality and asset availability.

The LC_STATE flag values stored in the non-volatile area control the Life-Cycle state. The LC_STATE value decreases according to the Live Cycle State, and when it progresses to the next state value, it cannot be changed to the previous value that is controlled by firmware running inside the secure world protected by TrustZone.

Bootloader 0 is responsible for checking the Live-Cycle State. Depending on the Live-Cycle state, Bootloader 0 decides which boot flow to use. If the part is in the disposal stage or has an invalid Life-Cycle state, Bootloader 0 is supposed to lock the part.

Figure 2 shows the availability of both Assets and Debug functionality. And provisioning shall be done in secure way during manufacturing process. In this step, a Key used in secure firmware downloading is injected, and this Key has a different value for each device. Please refer to Chapter 12 in [5].



Note that the vendor (Samsung) states are only reachable by Samsung, either before delivery of the product, or after return of the product by the customer.

Figure 2. Lifecycle overview

3.5.3 Usage and environment

The UWB module considered in this profile is integrated into a smart device, into which it communicates with:

- the Digital Key applet part of a Secure Element,
- the Digital Key framework run by the regular operating system of the smart device on the Application Processor,
- the vehicle through its UWB RF interface.

This UWB module is involved in a subpart of the overall vehicle access system; it handles the secure ranging calculation involving both UWB modules of mobile device and vehicle for the exchange of ranging data.

The prior ranging session establishment is handled by other components (DKF, DKA, BLE) of the system and is out of the evaluation scope covered by this profile.

Only the operations related to secure ranging calculation performed by the UWB module are in the evaluation scope, including the handling of communications with the other components, in particular transfers between the Secure Element and the UWB module of data to be part of the ranging calculation.

The figure below represents a simplified view of the overall exchanges during a secure ranging session:

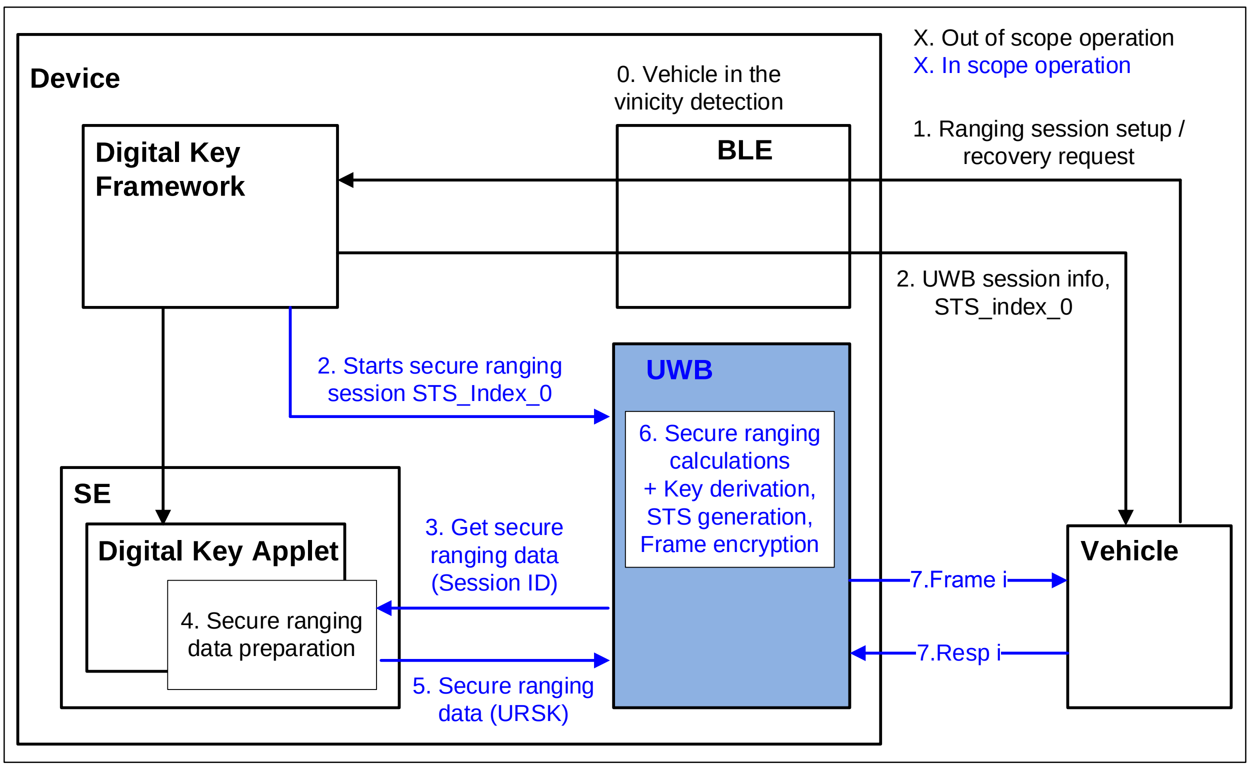


Figure 3. Secure ranging session flow

Note: Additional information about steps and interactions between the UWB module and other modules is described in detail in [1].

3.5.3.1 Communications context

No protection of the communications between the DKF and the UWB module is required; however, data received from the DKF shall be checked by the UWB module, in particular the STS_Index0 (larger than last STS index). This requires the claim of the SFR 5.2.8 Generic security platform feature.

The DKA/SE ensures the secure storage of long-term cryptographic keys and the generation and temporary storage of session keys (or derived key for session key generation in UWB module) which are then used by the UWB module for the security of these services. The communications between the DKA/SE and the UWB module shall be protected to ensure the integrity and the confidentiality of the Ranging Session Key, or (d)USRK. This requires the claim of the SFR 5.2.3.1 Secure communication support – UWB-SE.

The communication between the mobile UWB module and the vehicle UWB module shall be protected. This requires the claim of the SFR 5.2.3.2 Secure communication support – UWB-Vehicle.

Note: the communications between the DKF and the vehicle involves the STS_index_0 which is a sensitive asset used to (re)start a session; this is done under a Bluetooth LE channel established between the vehicle and the device, however without involving the UWB module, therefore this is out of the scope of the evaluation covered by this profile.

3.5.3.2 Physical access

It is considered that the user mobile devices integrating S3JU100 will be executed in an environment where they can become physically accessible to an attacker for a sufficient amount of time to perform the physical attacks defined in Appendix A.2. However, it is assumed that the device owner shall do at least minimum actions for protecting it against attackers. This is related to the claim of the SFR 5.2.4.1 Physical attacker resistance in line with the agreed assurance level targeted. S3JU100 has a protection function or HW IPs which can protect or making less sensitive it from the physical attacks described in Appendix A.2 such as remote attacks and local attacks.

The physical scope is the part of S3JU100 silicon chip as shown in Figure 4. The hardware components and interfaces are listed in Chapter 1 of [4].

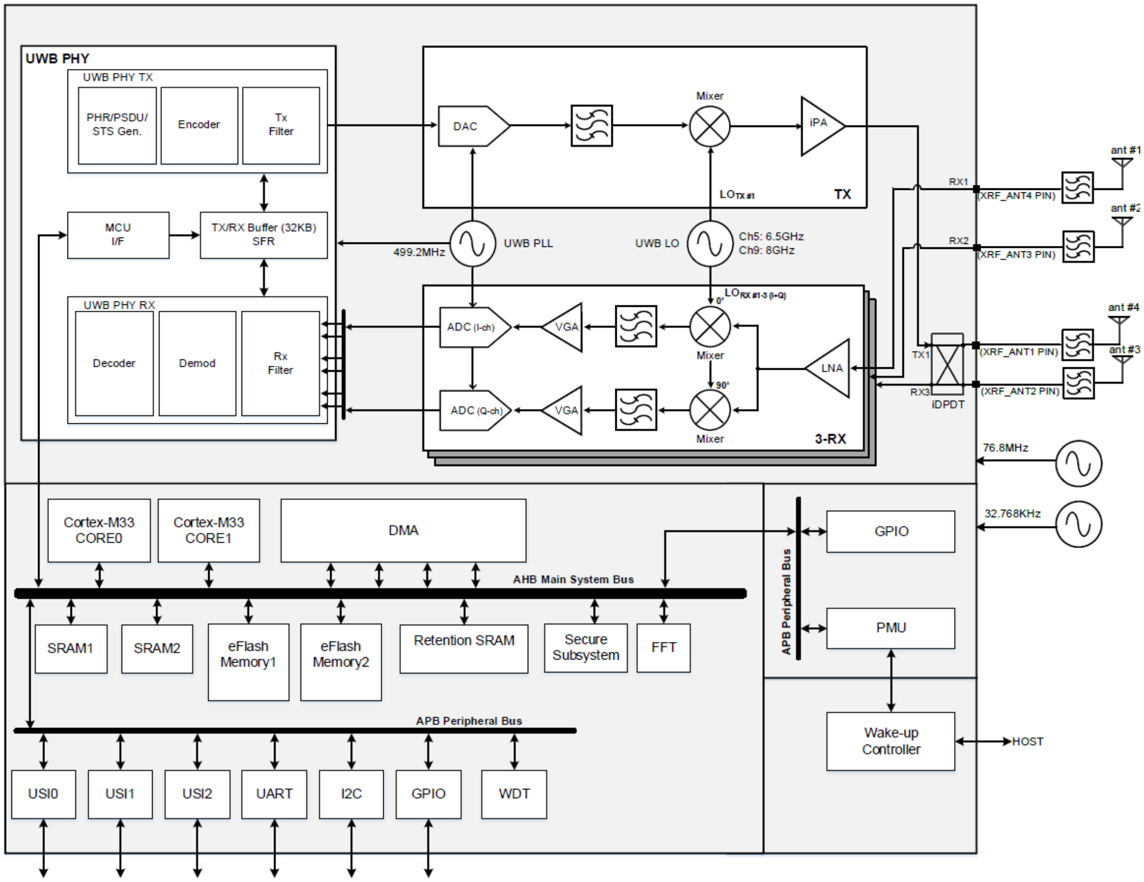


Figure 4. S3JU100 Hardware Architecture

Table 4. Hardware information

Component / Interface	Description
CPU	Two Arm cortex-m33 core with TrustZone™ running at a frequency 200MHz
On-chip Memory	512KB Flash 256KB RAM 20KB EGRAM (Low Power RAM)
Cryptographic Accelerator	AES(ECB/GCM)/CMAC, DTRNG, SHA2/HMAC, PKE, CRC
Interface	HOST Interface: SPI eSE Interface: SPI JTAG for debugging UART for debugging
Peripherals	Timers and Watchdog Timer GPIO, DCXO, TSU (Temperature Sensor Unit)
UWB Controller	CH5 and CH9 frequency bands, BPRF and HPRF support

3.5.3.3 Logical access

S3JU100 is a component integrated into a mobile device in which attacker can try to load untrusted code. S3JU100 supports the secure firmware update function to prevent untrusted code from being loaded. Additionally, S3JU100 supports a secure booting function to ensure the integrity of the firmware running inside it. Therefore, using this function, it can be sure that only trusted firmware will operate within the S3JU100. As also, S3JU100 support secure booting function to ensure the integrity of the firmware which is executed inside the S3JU100. As a result, the firmware which is executed inside the S3JU100 can be said trusted firmware only.

The logical scope is the part of S3JU100 firmware which includes secure bootloader (Read only), secure firmware update, secure ranging firmware as illustrated in Figure 5.

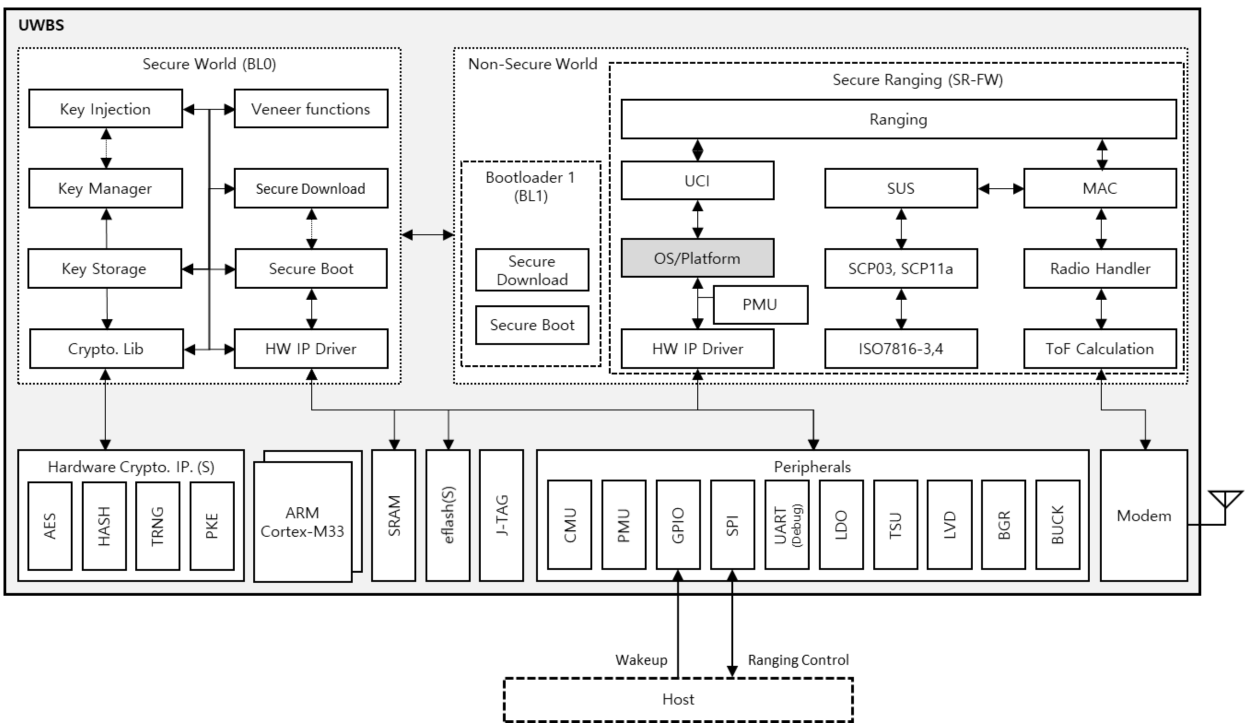


Figure 5. Logical Scope of Certification

3.5.3.4 Physical form factor

In Smartphone or IoT, S3JU100 is soldered to the PCB surface using surface mount technology (SMT) for system configuration with other chips or modules. This connection simultaneously performs the role of mechanical fixation as well as electrical signal transmission. In this process, since the S3JU100 is configured as the package of the Ball type and is mounted on the PCB, it is not possible to directly probing the signal of the Ball using an electronic device such as an oscilloscope. Physical attacks, such as probing signals or fault attacks, require the S3JU100 chip to be physically separated from the PCB.

3.6 Required Non-Platform Hardware/Software/Firmware

S3JU100 has no additional non-platform features.

4 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

For the UWB module to fulfill its security requirements, the operational environment shall implement the following objectives:

- The device manufacturer is expected to respect integration and usage manual and security guidance described in Table 5.
- <session keys> shall be executed and/or stored securely in a Secure Element ensuring authenticity, integrity and confidentiality of data to be transferred to the UWB module for secure ranging calculation.
- The Secure Element shall be able to establish a secure channel with the UWB module as it is required in [1] to ensure the authenticity, the integrity and the confidentiality of the sensitive material during the transfer.
- The Secure Element shall be bound to the UWB module to allow mutual authentication. The binding material which shall be provisioned during manufacturing shall be protected in integrity and confidentiality.
- UWB module development and manufacturing environments implement processes ensuring the protection of <binding keys, secure booting/secure downloading keys>.

Table 5. Security Objectives for the Operational Environment

Title	Description
Platform identity verification	The operating system or host application code checks the version of the platform components as described in Chapter 4 in [5]
Secure Booting	The platform should be able to check the integrity of the code. It is described in Chapter 5 in [5]
Secure downloading	he platform must ensure the integrity, confidentiality, and authenticity of the code downloaded for updates. It is described in Chapter 6 in [5]
Secure channel	The Secure Element shall be able to establish a secure channel with the S3JU100 to ensure the authenticity, the integrity and the confidentiality of the sensitive material during the transfer. Refer to [6] and [7]
Secure binding	The Secure Element shall be bound to the S3JU100 to allow mutual authentication. The binding material which shall be provisioned during manufacturing shall be protected in integrity and confidentiality. Refer to Chapter 8 and 13 in [5]
Secure use	Users ensure the secure and correct use of the platform.
Key Injection	UWB module development and manufacturing environments implement processes ensuring the protection of keys used for secure operation. Refer to Chapter 13 in [5]
Cryptographic Operation	Cryptographic operation is executed in the isolated environment inside the S3JU100 name as secure world of TrustZone. Refer to Chapter 10 in [5]
Software isolation	The operational environment must not allow the deployment of untrusted code. That means that all code running on the product is

	known to the product vendor and the product vendor can confirm that the code cannot harm the claimed security features. Code download is only done via secure update of platform as described in Section 5.2.2.1. All code is digitally signed. Refer to Chapter 6 in [5]
Physical protection	The operational environment must protect the S3JU100 against physical access of attackers as described in Section 6.

5 SECURITY REQUIREMENTS AND IMPLEMENTATION

REQ In this chapter, the Security Target shall define the Security Assurance Level claimed and the list of Security Functional Requirements in the scope of the evaluation; this list shall be compliant with the security features listed in the product description.

5.1 Security Assurance Requirements

The claimed assurance requirements package is SESIP3 as defined in [2].

5.1.1 Flaw Reporting Procedure (ALC_FLR.2)

In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), including a process to report flaw and generate any needed update and distribute it, the developer has defined the following procedure:

Samsung operates a process with its Product Security Incident Response Team (PSIRT), which provides the following guidelines for work.

1) Register (Receiving vulnerability reports)

PSIRT receives reports of potential vulnerabilities, recognizes the potential vulnerability risk, and creates issues according to established processes. In addition, quality team and security expert check additional information on vulnerabilities and deliver it to the development team.

Semiconductor Product Security | Samsung Semiconductor Global

2) Analysis (Evaluation and Solution)

Based on the collected data, the development team analyzes the vulnerabilities and reproduces the phenomenon reported in the report. The development team accurately defines the flaw found and presents solutions to compensate for them. The development team reviews whether this solution satisfies all operating conditions, checks if there is a side-effect, and prepares a final report. The development team delivers the final report and solution to security experts and PSIRT.

3) Completion (Notice and CVE ID)

Based on the final report, security experts and the product manager of the development team explain the flaws to customers and provide security patches. PSIRT determines the description through vulnerability type, attack type, impact, CVE (Common Vulnerabilities and Exposures) rating, and scoring. Thereafter, a CVE ID is generated through PSIRT and registered in Semiconductor Product Security | Samsung Semiconductor Global-CVEID

according to the process.

5.2 Mandatory Security Functional Requirements

5.2.1 Identification and attestation of platform and applications

5.2.1.1 Verification of platform identity

Requirement

The platform provides a unique identification of the platform, including all its parts and their versions.

Refinement

Assets and protections related to this SFR are:

Assets for Verification of Platform Identity SFR

Asset	Protection required	Comments
UWB module Platform Identity	Integrity	The modification of the platform id is impacting the user configuration management.

Rational

The platform identification of S3JU100 can be done through data stored in the eflash at the time of chip manufacturing. Data stored in the eflash area can be uniquely identified through platform ID (CHIP ID), revision number. The version information of BL0, BL1 and SR-FW is also stored in code area and can be identified. To check this information, the firmware of S3JU100 supports API and a specific command set to read it over UCI (UWB Command Interface) command. A detailed information is described in clause 4.2.3 of [5].

5.2.1.2 Verification of platform instance identity

Requirement

The platform provides a unique identification of that specific instantiation of the platform, including all its parts.

Refinement

Assets and protections related to this SFR are:

Assets for Verification of Platform Instance Identity SFR

Asset	Protection required	Comments
UWB module Platform Instance Identity	Integrity	The modification of the platform instance id may impact the pairing/binding of the UWB module with the SE.

Rational

The S3JU100 platform instance identity can be verified through a specific UCI (UWB command Interface) command. It supports two instances. One is device instance and the other is a secure element instance of binding.

To check this information, the firmware of S3JU100 supports API and a specific command set to read it over UCI (UWB Command Interface) command. A detailed information is described in clause 4.2.3 of [5].

5.2.1.3 Secure initialization of platform

Requirement

The platform ensures its integrity and authenticity during platform initialization. If the platform integrity or authenticity cannot be ensured, the platform will go *to <BL0 Secure downloading, BL1 Secure downloading and Exception & Hold>*.

Refinement

Assets and protections related to this SFR are:

Assets for Secure Initialization of Platform SFR

Asset	Protection required	Comments
UWB module firmware	Integrity, authenticity	Firmware running on UWB module and playing a central role in the computation. and execution of the secure ranging protocol. Modification of this asset would allow the attacker full control of secure ranging operation leading to getting the illegal access to the vehicle.

Rational

The S3JU100 firmware ensures integrity and authenticity through secure functions as below.

Secure booting: Integrity and authentication are checked through CMAC verification during booting from RoT (BL0). If it fails, it jumps to secure downloading state and reports security fail to the host

JTAG is disable to protect un-authorized access and the protection function prevents the modification of the BL0 (RoT) code. Both features ensure the integrity and authenticity of the BL1 and SR-FW.

TrustZone activation and SAU configuration in BL0. It can prevent un-authorized access to the secure world

S3JU100 has a secure boot chaining from BL0 to BL1 and SR-FW. JTAG is disabled and CPA lock is applied during manufacturing process in production. For more information about secure booting, JTAG disable and eflash CPA lock function. Please refer to Chapter 5 of [5].

5.2.2 Product Life Cycle: Factory reset / Install / Update / Decommission

5.2.2.1 Secure update of platform

Requirement

The platform can be updated to a newer version in the field such that the confidentiality, integrity and authenticity of the platform is maintained.

Refinement

Assets and protections related to this SFR are:

Assets for Secure Update of Platform SFR

Asset	Protection required	Comments
UWB module firmware and software	Integrity, Authenticity	Firmware and software running on UWB module and playing a central role in the computation and execution of the secure ranging protocol. Modification of this asset would allow the attacker full control of secure ranging operation leading to getting the illegal access to the vehicle. Boundary between Firmware and Software is implementation dependent and should be defined in the Security Target.
UWB module firmware and software version	Anti-rollback	Firmware and software can only be updated to a version greater or equal to the current version.

Rational

The S3JU100 ensures the confidentiality, integrity and authenticity of the firmware running within the S3JU100 through its secure downloading feature. The S3JU100 consists of two bootloaders (BL0 and BL1) and one firmware (SR-FW). BL0 is injected during the manufacturing process and cannot be changed in the field. BL0 does self-check (CMAC) during booting process, so it can guarantee integrity. BL1 and SR-FW guarantee confidentiality, integrity, and authenticity through the secure downloading function. See more in Chapter 5 of [5].

In addition, since JTAG is disabled, SR-FW can only be changed through secure downloading function. The details of the secure downloading function are described in the security technical note. A SR-FW version check function has been added to prevent rollback during the secure downloading process. Details on SR-FW version checking are available in Chapter 6 of [5].

5.2.3 Secure communication

5.2.3.1 Secure communication support – UWB-SE

Requirement

The platform provides one or more secure communication channel(s).

The secure communication channel authenticates *mutually the Secure Element (SE) and the UWB module(S3JU100)* and protects against *disclosure, modification, replay* of messages between the endpoints, using *<GlobalPlatform SCP03 or SCP11a>.*

Refinement

Assets and protections related to this SFRs are:

Assets for Secure Communication Support SFR (UWB – SE)

Asset	Protection required	Comments
UWB-SE session key	Integrity, confidentiality	Key used to establish a trusted channel between the UWB module and SE. Modification or disclosure of this asset would allow the illegal access to data exchanged under the secure channel.
UWB-SE key material (aka binding key)	Integrity, confidentiality	Material used to generate the session key; may include further data like a UWB module ID (if existing). Modification or disclosure of this asset would allow the illegal access to data exchanged under the secure channel.
Active URSK or derived material (URSK, mURSK, MUPSK1, mUPSK2, Salt, Salted Hash)	Confidentiality	Material for the security of the active UWB Ranging Session between one vehicle and one device. This asset shall be securely exchanged between UWB module and SE under the UWB-SE secure channel; the disclosure of this data would allow attacker to emulate ranging session and modify distance measurements. Note: integrity disturbance not resulting in confidentiality loss (e.g. by DFA) is not a security issue and is then not required here (see Section A.1).

Rational

The S3JU100 supports the Global Platform SCP03 and SCP11a secure channel protocols for secure communication with the SE, enabling authentication and encryption between S3JU100 and SE to protect exchanged data. The S3JU100 has the following protection functions for assets defined by SFR:

1) UWB-SE Session Key

• Create and receive a secure channel through implementation of the Global Platform SCP03 specification.

• Generate a UWB-SE session key using the binding key and KDF defined by Global Platform.

• The UWB-SE session key is not stored separately and is deleted at the end of the session.

• The UWB-SE session key is used for data encryption/decryption and CMAC calculation for data integrity.

• When receiving session key via secure channel, session key is encrypted with CMAC attached for integrity verification.

2) UWB-SE key materials

• The binding key between UWB-SE is achieved through implementation of the Global Platform SCP11a specification.

• Inject UWB's public key pair and certificate into the process.

• UWB and SE create an SCP11a secure channel using each other's key materials.

• After creating the secure channel, UWB delivers the binding key to SE through secure channel.

• Store the bound binding key securely in the key storage.

3) Active URSK or derived material

• Extract URSK from data received safely from SE.

• Save and delete URSK after use - there is no set policy or implementation.

• Information derived after URSK is not managed nor transmitted.

• Receive only URSK from SE through secure channel and further key derivation and STS generation are done inside the S3JU100.

A more detailed description can be found in Chapter 8 of [5], [6] and [7].

5.2.3.2 Secure communication support – UWB-Vehicle

Requirement

The platform provides one or more secure communication channel(s).

The secure communication channel authenticates *mutually a remote Vehicle and the UWB module* and protects against *disclosure, modification, replay* of messages between the endpoints, using *CCC protocol as defined in section 20 - UWB MAC and Channel access, section 21 – UWB Phy and section 22 – UWB Security of* [1].

Refinement

Assets and protections related to this SFRs are:

Assets for Secure Communication Support SFR (UWB – Vehicle)

Asset	Protection required	Comments
UWB-Vehicle material	Confidentiality, integrity	Material used to establish a trusted channel between the UWB module and Vehicle. Modification or disclosure of this asset would allow the illegal access to data exchanged under the secure channel.
Timestamps	Confidentiality, integrity, authenticity	Modification of this asset would allow to reduce the range information by tampering with exchanged frames. Note: integrity disturbance not resulting in a lower value than the correct one is not a security issue and is then not required here (see Appendix A.1).
STSindex	Confidentiality, integrity, authenticity	Modification of this asset would allow to perform replay attacks. Disclosure would impact user privacy.

Disclosure of these assets can lead to a user privacy violation, which must be prevented.

Rational

The S3JU100 can protect the exchanged messages between the S3JU100 and the Vehicle UWB by using the secure ranging protocol presented in the CCC (Car Connectivity Consortium) standard [1], which prevents disclosure, modification, and replay of the messages.

The messages exchanged between the S3JU100 and Vehicle are encrypted based on the CCC protocol defined in Section 20 and Section 22 [1].

The parameters containing the STS index value of the pre-poll message defined in Table 20-3 and Table 20-4 of Section 20 [1] are encrypted with the mUPSK1 key according to the protocol definition.

The parameters containing the timestamp of the final data message defined in Table 20-5 and Table 20-6 of Section 20 are encrypted with the dUDSK key according to the protocol definition.

5.2.3.3 Secure communication enforcement

Requirement

The platform ensures that the communication with *end points listed in the table below* can only be done over the secure communication channel(s) supported by the platform using *the protocols and measures listed in the table below*.

Assets for Secure Communication Enforcement SFR

End points	Protocols and measures
Digital Key Applet (SE)	Global platform SCP03, SCP11a,
Vehicle UWB	Ranging protocol as defined in [1]

Refinement

Assets and protections related to this SFRs are the ones defined in the previous Secure Communication Support SFRs.

Rational

The S3JU100 supports Global Platform SCP03 and SCP11a for secure communication with the Digital Key Applet (SE). It also supports the secure ranging protocol defined in the CCC standard [1] for secure communication with UWB-Vehicle.

5.2.4 Extra attacker resistance

5.2.4.1 Physical attacker resistance

Requirement

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the other security functional requirements.

Rational

S3JU100 has the following functions to protect chips from external physical attacks referred in Appendix A.

• TSU (Temperature Sensor Unit): S3JU100 has temperature sensor unit which can measure the chip temperature.

• BUCK and LVD: The S3JU100 has an LVD (Low voltage detector) so that can detect the low voltage and reset the chip.

• The watchdog timer reset the chip when it detected a system hang.

• HW Reset function reset the chip if attacks detected.

• ARM TrustZone can make it possible to separate area between secure world and non-secure-world within BL0, BL1 and SR-FW so that a sensitive data such as cryptographic operation result, eflash control and some system control related registers are handled inside the secure world which can protect data from non-secure world code reads out the sensitive data.

A detailed information is described in Chapter 9 and 10 of [5].

5.2.4.2 Software attacker resistance: isolation of platform

Requirement

The platform provides isolation between the application and itself, such that an attacker able to run code as an application on the platform cannot compromise the other security functional requirements.

Rational

The S3JU100 consists of a bootloader (BL0 and BL1) and firmware (SR-FW). The SR-FW includes a ranging protocol for digital car key required by CCC standards [1] within it. The secure bootloader of the S3JU100 also uses the ARM Trust Zone feature to protect its own area and the area supporting secure functions as a secure area. The S3JU100 supports a secure boot chain based on RoT. It also supports secure firmware updates so that only authorized firmware can be downloaded. In addition, the debugging channel (JTAG) is disabled to protect the firmware from external access other than secure booting and secure firmware updates. A detailed information about secure booting, secure downloading, ARM Trust Zone configuration and JTAG disable function can be found in Chapter 5, 6, 10 and 11 of [5].

5.2.5 Cryptographic functionality

5.2.5.1 Cryptographic keyStore

Requirement

The platform provides a way to store *the binding key* such that not even the application can compromise the *confidentiality, integrity, authenticity* of this data. This data can be used for the cryptographic operations *Secure Communications Support UWB-SE*.

Rational

The key for binding with SE in S3JU100 is stored in encrypted form. In addition, when decrypting the binding key and using it for cryptographic operations, the calculations are performed in a secure area protected by the ARM TrustZone feature.

For more detail, please refer to Chapter 8 of [5].

5.2.6 Compliance functionality

5.2.6.1 Secure debugging

Requirement

The platform only provides <list of endpoints> authenticated as specified in <specification> with debug functionality.

The platform ensures that all user data stored, with the exception of <list of exceptions>, is made unavailable.

Refinement

All assets defined in other Security Functional Requirements and accessible through the Secure Debugging mechanism shall be protected against unauthorized access.

For debug functionality authentication, device specific credentials shall be used.

Rational

Conformance Rational:

The TOE uses JTAG and test mode for product test. In the JTAG case, TOE has a function to disable the JTAG port. In development phase, the JTAG port can be used for development purpose, and in production (commercial versions) phase, the JTAG is disabled at the Samsung factory during manufacturing process before shipping the products. The HW control register which can make JTAG disable is protected by the secure area of ARM TrustZone. For more details, please refer to Chapter 10 and 11 of [5]. Test mode is also used by production test. Each product uses a unique key to prevent key reuse.

5.2.6.2 Residual information purging

Requirement

The platform ensures that *the active URSK*, with the exception of *all other data*, is erased using the method specified in <*Security Technical Note [5]*> before the memory is used by the platform or application again and before an attacker can access it.

Rational

The URSK and other sensitive data used for calculating secure ranging in S3JU100 are cleared with random values or a specific pattern after use, and are also cleared when "session de-init command" is sent from host.

5.2.7 Proprietary functionality

5.2.8 Generic security platform feature

Requirement

The platform provides the *ranging calculation* according to *CCC, <No other standards/specifications>*.

Refinement

Next table shows the assets and protections related to this SFRs for CCC. If other standards are part of the evaluation scope, the Security Target shall add list of the related assets and required protection.

Assets for Secure Execution of Platform Feature SFR

Asset	Protection required	Comments
Active URSK or derived material (URSK, mURSK, mUPSK1, mUPSK2, Salt, Salted Hash)	Confidentiality	Material for the security of the active UWB Ranging Session between one vehicle and one device. Modification or disclosure of this asset would allow attacks to reduce measured distance. Note: integrity disturbance not resulting in confidentiality loss (e.g., by DFA) is not a security issue and is then not required here (see Appendix A.1).
Secure Ranging key materials (dURSK, dUDSK)	Confidentiality	All specific purpose key materials involved in secure ranging protocol. The lifetime of these keys is one ranging round. Disclosure of this asset would allow attacker to reduce distance. Note: integrity disturbance not resulting in confidentiality loss (e.g., by DFA) is not a security issue and is then not required here (see Appendix A.1).
STS	Confidentiality	Materials used for the generation of Scrambled Timestamp Sequence (STS) or the STS itself. Disclosure of this asset would allow attacker to reduce distance. Note: integrity disturbance not resulting in confidentiality loss (e.g., by DFA) is not a security issue and is then not required here (see Appendix A.1).
STS_Index	Integrity	Monotonic index used as input parameter for deriving the STS sequence on UWB module physical layer.

		Modification of this asset would allow attacker to reuse already exchanged STS and thus to reduce measured distance.
STS_Index0	Authenticity, integrity	First value of the monotonic index used as input parameter for deriving the STS sequence on UWB module physical layer. Replacement of this asset would allow attacker to reuse already exchanged STS and thus reduce measured distance.
Timestamps	Integrity, Confidentiality, authenticity	Used for computing distance. Modification of this asset would allow to reduce distance or determine user location. Disclosure of this asset can lead to privacy issue. Note: integrity disturbance not resulting in a lower value than the correct one is not a security issue and is then not required here (see Appendix A.1).
Session Time To Live	Integrity	Modification of this asset would allow increasing the duration of a session.

Rational

Other standard/specification is not included in the scope of evaluation

6 MAPPING AND SUFFICIENCY RATIONALES

Assurance Class	Assurance Families	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section 3	The ST reference is in Section 3.2, the platform reference in Section 3.3, the platform overview and description in Section 3.5.
	ASE_OBJ.1 Security requirements for the operational environment	Section Security Objectives for the operational environment	The objectives for the operational environment in Security Objectives for the operational environment refer to the guidance documents.
	ASE_REQ.3 Listed Security requirements	Section Security requirements and implementation	All SFRs in this ST are taken from [2]. Section Verification of platform identity is included. Section Secure update of platform is included.
	ASE_TSS.1 TOE Summary Specification	Section Security requirements and implementation	All SFRs are listed per definition, and for each SFR the implementation and verification are defined in Section Security requirements and implementation.
ADV: Development	ADV_FSP.4 Complete functional specification	Material provided to the evaluator.	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.

Assurance Class	Assurance Families	Covered by	Rationale
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	Material provided to the evaluator.	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Material provided to the evaluator.	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	Material provided to the evaluator.	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	Section Flaw Reporting Procedure (ALC_FLR.2)	The flaw reporting and remediation procedure is described.
	ALC_CMC.1 Labelling of the TOE	Material provided to the evaluator.	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ALC_CMS.1 TOE CM Coverage	Material provided to the evaluator.	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
ATE: Tests	ATE_IND.1 Independent testing: conformance	Material provided to the evaluator.	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.

Assurance Class	Assurance Families	Covered by	Rationale
AVA_VAN.3	AVA_VAN.3 Vulnerability analysis	N.A. A vulnerability analysis is performed by the platform evaluator to ascertain the presence of potential vulnerabilities.	The platform evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the platform evaluator assuming an attack potential of Enhanced-Basic.

APPENDIX A ATTACK METHOD

A.1 Threat analysis

The main unwanted event to be covered in the profile is the illegal access to the vehicle through the attack of the UWB module of a device associated to this vehicle.

Preventing the blockage of the access to the vehicle is not covered in this profile, therefore no availability of assets is required.

An attack shall be considered as successful if asset disclosure and related attack exploitation time is less than the lifetime of the asset; in particular, less than one ranging round duration for dURSK, less than one ranging slot duration for STS. Note that attacks which allow to extend the lifetime of assets, e.g. UWBS_STS_INDEX_REUSE, shall as well be considered

As opposed, an attack leading to a denial of service (e.g. through encrypted assets tampering), is not valid as it will only result in preventing the communication or accurate ranging. However, integrity disturbance leading to confidentiality loss is to be considered as part of the different UWBS_DISCLOSURE threat (see table below).

The following table lists all threats to be taken into consideration during the security evaluation.

Threats coverage by SFRs

Threats	Assets	SFRs
UWBS_DISCLOSURE_LOGICAL **UWBS_DISCLOSURE_PHYSICAL_NON-INVASIVE** **UWBS_DISCLOSURE_PHYSICAL_SEMI-INVASIVE** **UWBS_DISCLOSURE_PHYSICAL_INVASIVE** Attacker manages to get access to secret data such as keys or credentials by the attack means in the scope of this profile (see Appendix A.2)	Active URSK, all keys	Secure communication support – UWB-SE Secure communication enforcement Cryptographic keyStore Physical attacker resistance Software attacker resistance: isolation of platform Residual information purging Generic security platform feature Security Objectives for the operational environment
UWBS_REROUTING_SE_UWB_COMMUNICATION The communication between the SE and UWB module is rerouted.	Active URSK and/or some Secure Ranging Intermediate key materials	Secure communication support – UWB-SE Secure communication enforcement
UWB_SPOOFING As a consequence of Binding keys disclosure, the attacker is pretending to be the UWB module towards the SE, for instance by creating a rogue app to communicate with the SE, in order to	Binding keys	Secure communication support – UWB-SE Secure communication enforcement

get the SE to send the URSK (and then inject it in another device).		
UWBS_SPYING_ON_SE_UWB_COMMUNICATION An attacker manages to spy on the communication between the SE and UWB module. Spying could be active/invasive and passive/non-invasive	Active URSK and/or some Secure Ranging Intermediate key materials	Secure communication support – UWB-SE
UWBS_CORRUPTION_OF_UWB_FIRMWARE Attacker executes malicious firmware on the UWB module which could allow extraction of sensitive assets. The attacker may have persistency on the UWB module.	All primary assets and binding key, firmware	Secure initialization of platform Secure update of platform Physical attacker resistance Software attacker resistance: isolation of platform
UWBS_UPDATE_UWB_CONFIGURATION Attackers modify the configuration used by the UWB system during ranging; e.g. UWB configuration used for the salted hash, or delays used during distance/ranging computation.	Ranging data, timestamps	Secure communication support – UWB-Vehicle Secure communication enforcement
UWB_RADIO_SNIFF An attacker may attempt to sniff the traffic between a device and a vehicle during an exchange on the UWB radio channel.	STS_Index, ranging data, timestamps	Secure communication support – UWB-Vehicle
UWB_RADIO_MITM An attacker may attempt to gain a MITM presence between a device and a vehicle during an exchange on the UWB channel.	STSindex, STS, ranging data, timestamps	Secure communication support – UWB-Vehicle Secure communication enforcement
UWB_RADIO_SPOOFING An attacker may attempt to spoof or impersonate a UWB module and start or manipulate a conversation with the other entity. E.g. change the STSindex, change time stamps, …	STSindex, STS, ranging data, timestamps	Secure communication support – UWB-Vehicle Secure communication enforcement
UWBS_ DOS An attacker may attempt to manipulate the UWB subsystem in some way to prevent the user from being able to use their DK.	All Assets	Physical attacker resistance Software attacker resistance: isolation of platform

UWBS_MANUFACTURING_INSIDER An insider with access to the UWB module development, manufacturing or UWB-SE binding, may attempt to manipulate the firmware or leak information about the firmware or the binding keys. Note: This covers the development phase of the UWBS and the manufacturing/production phase of the UWBS and the SE-UWBS integration phase.	UWB module firmware, binding keys	Security Objectives for the operational environment
UWBS_FIRMWARE_ROLLBACK An attacker may attempt to roll back the firmware of the UWB module to an older version that may have weaknesses.	UWB module firmware	Secure initialization of platform Secure update of platform
UWBS_BINDING_PROCESS_MANIPULATION An attacker may try to compromise the process of binding key generation or manipulating the binding key generation. If re-binding (in the field) is possible this threat applies respectively.	UWB module firmware, binding keys	Secure communication support – UWB-SE Cryptographic keyStore Security Objectives for the operational environment
UWBS_UNAUTHORIZED_DELETION_OF_KEY_MATERIAL An attacker deletes the UWB SE binding key material which prevents access to the car and hence threatens the availability of the car.	UWB module firmware, binding keys	Security Objectives for the operational environment
UWBS_REPLAY_UWB_RANGING_MESSAGES An attacker may try to replay observed UWB ranging messages or frames to the device or vehicle with the aim to manipulate the ranging result.	Timestamps	Secure communication support – UWB-Vehicle Residual information purging
UWBS_STS_INDEX_REUSE An attacker manipulates the STS index in order to reuse an STS index.	STS_Index0, STS_Index	Physical attacker resistance Software attacker resistance: isolation of platform Generic security platform feature
UWBS_ MANIPULATE_TIMESTAMPS An attacker modifies timestamps in UWB module to reduce the computed distance.	Timestamps	Physical attacker resistance Software attacker resistance: isolation of platform Generic security platform feature

UWBS_UNAUTHORIZED_ACCESS_SR_ASSET Attacker benefits from uncontrolled access to the UWB module interface from the AP to perform concurrent operations while the UWB module executes cryptographic computations for secure ranging (intermediate key derivation, ...). This may lead to tempering the assets or disclose the assets extracted from UWB module volatile memory.	UWB module software and firmware	Physical attacker resistance Software attacker resistance: isolation of platform Generic security platform feature
UWBS_UNAUTHORIZED_ACCESS_SR_CODE Attackers modify code of secure ranging functions in UWB module to give all access to lock/unlock and Engine Start. This is a more specific attack scenario of UWBS_DISCLOSURE_LOGICAL.	UWB module software and firmware	Secure initialization of platform Secure update of platform Physical attacker resistance Generic security platform feature
UWBS_PROTOCOL_DOWNGRADE An attacker may attempt to downgrade the protocol to an older version that has known weaknesses.	UWB module software and firmware	Secure update of platform

A.2 Attack means in scope

No attack requiring the destruction or visible physical modification of the device is in the scope of the evaluation as the attack would be noticed by the device owner.

A.2.1 Remote attacks

For those attacks listed in this section, the attacker does not need physical access to the UWB module. All remote attacks are always in scope.

A.2.1.1 Remote logical attacks

Attacker manages to get access to secret data such as keys or credentials by attacking the interfaces of the UWB module. For example, by:

- sending ill-formed messages (fuzzing the API, buffer overflows) to nominal interfaces of the UWB module (phone internal and UWB radio)
- attacking the FW upgrade method to modify the code
- managing to get access to memory content

A.2.1.2 Remote side channel attacks

Attacker manages via remote access to control or observe hardware behavior in the UWB module local environment in order to launch side channel analysis (e.g., analysis through power or cache measurements).

A.2.1.3 Remote fault attacks

Attacker manages via remote access to control hardware behavior in the UWB module local environment in order to launch fault attacks (e.g., clock, voltage glitching).

A.2.2 Local attacks

For those attacks listed in this section, the attacker needs physical access to the UWB module.

A.2.2.1 Local logical attacks

Attacker manages to physically access the mobile device and use local logical interfaces (e.g., via USB) to launch an attack.

A.2.2.2 Local non-invasive side channel attacks

Attacker manages to get access to secret data such as keys or credentials by having non-invasive local access to the UWB module to perform side channel analysis:

- Measuring signals such as power, electromagnetic radiation, clock, timing of events, or I/O lines during any information processing

The attacker has means to collect physical parameters of the UWB module.

A.2.2.3 Local non-invasive fault attacks

An attacker manages to perform an attack on UWB module physical parameters (such as voltage, clock, ...) to get access to secret data such as keys or credentials:

- modifying the behavior of a UWB module by injecting faults (e.g., electromagnetic fault injection (EMFI), power supply manipulation)

- manipulating signals such as power, electromagnetic radiation, clock, timing of events, or I/O lines during any information processing

A.2.2.4 Local semi-invasive and invasive attacks

Attacker has access to owner phone or friend phone and discloses secret data such as keys or certificates by:

- Physical probing of existing interfaces
- Modifying or accessing nominal interfaces

Note that destructive attacks, e.g., decapping, polishing, thinning are not considered exploitable. Indeed, user can disable UWB access to car, if device is missing for a few hours or found damaged.