ETSI TS 103 864 V1.1.1 (2023-01)

TECHNICAL SPECIFICATION

Cyber Security;
Security Threats and related Requirements
for Consumer Sensor Hubs

Reference

DTS/CYBER-0060

Keywords

cyber security, data

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

With the increasing development of sensors and consumer device technologies, more and more diversified consumer device application based on sensors capabilities are meeting the needs of the users. Many of these applications are based on traditional motion MEMS sensors (accelerometer, gyroscope, and magnetometer). These sensors are more and more present in the consumer device even for the most common functionalities such as movement tracing, automatic screen adjustment based on the light sensor (environment light and proximity light sensor) and detection of the environment characteristics (e.g. atmospheric pressure, temperature and altitude).

Sensitive data-based application scenarios are also available such as activity recognition applications, gesture recognition, user recognition, and motion status recognition based on ambient audio and video data. Many of these sensor functions depend on the aggregation processing of a large number of sensors' data.

Today there are multiple platforms/modules that can implement the sensor data aggregation and processing function, different architectures can be used to implement the sensor hub but the same security requirements need to be supported regardless these differences.

A sensor hub is a microcontroller unit/coprocessor/digital signal processor that helps to integrate data from different sensors or other chips (Wi-Fi®, Bluetooth®, GNSS, etc.) and process them. A sensor hub is a key components for the user data management, pre-processing and presentation to the application. Considering that the processed data is related with personal information, its security requirements need to be carefully defined. The aim of such requirements is to:

- guarantee the security of data relevant to sensor hub (data storage);
- guarantee the secure proper handling of the data within the sensor hub (data processing);
- determine which data can be transferred from the sensor hub to the device applications and secure such transfer on the sensor hub interface (data transfer and use).

1 Scope

The present document describes the security threats and specifies the related security requirements of sensor hubs used in consumer devices.

The present document focuses on hardware implementations of a sensor hub regardless if it is implemented on a dedicated chip or as a part of a SoC. It provides a set of requirements applicable to a sensor hub regardless if it will be evaluated as a single component or as part of a product. Existing standards related to a product in which the sensor hub is integrated (e.g. ETSI TS 103 732 [1] or ETSI EN 303 645 [2]) can be used to evaluate the product while being complemented by the sensor hub's specific requirements defined in the present document. The present document is considering only sensors that are integrated in the same device as the sensor hub; the case where a sensor is physically separate from the sensor hub and it is connected to it through a wired or wireless interface is out of scope.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 103 732; "CYBER; Consumer Mobile Device Protection Profile".

[2] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 102 165-1 "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

sensor hub: microcontroller or auxiliary processor that helps to obtain, integrate, and process data from different sensors and chipsets

threats: As defined in ETSI TS 102 165-1 [i.1].

3.2 Symbols

Void.

3.3 Abbreviations

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

BLE	Blue Tooth Low Energy
GNSS	Global Navigation Satellite System
DDR	Double Data Rate DRAM
DRAM	Dynamic Random Access Memory
HAL	Hardware Abstraction Layer
IoT	Internet of Thing
MCU	Microcontroller Unit
MEMS	Micro-Electro-Mechanical System
OS	Operating System
SDK	Software Development Kit
SI	Sensor hub Interface
SoC	System on Chip
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TPM	Trusted Platform Module
Wi-Fi	Wireless Fidelity

4 Sensor Hub description

4.1 Introduction

The sensor hub can comprehensively process the collected sensor information based on the requirements of different applications and send the processing result to the upper-layer applications.

The sensor stack of a consumer device in most of the cases includes a sensor hub, useful to perform some so-called low-level computation at low power while the main processor can be in a suspend mode. Figure 1 shows a possible consumer device sensor stack representation.

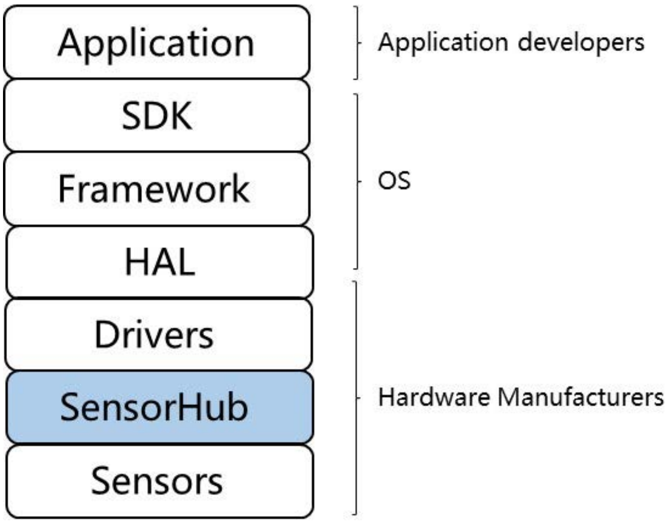

Figure 1: Consumer device sensor stack

How the sensor hub is materialized depends on the architecture. It is sometimes a separate chip, and sometimes included on the same chip as the SoC.

4.2 Functions and Architecture

Based on the requirements of different terminals and service scenarios, the sensor hub architectures can be classified into two types:

- built-in MCU; and
- external MCU.

The sensor hub and the sensors considered in the present document are all included in the same device (e.g. a smartphone).

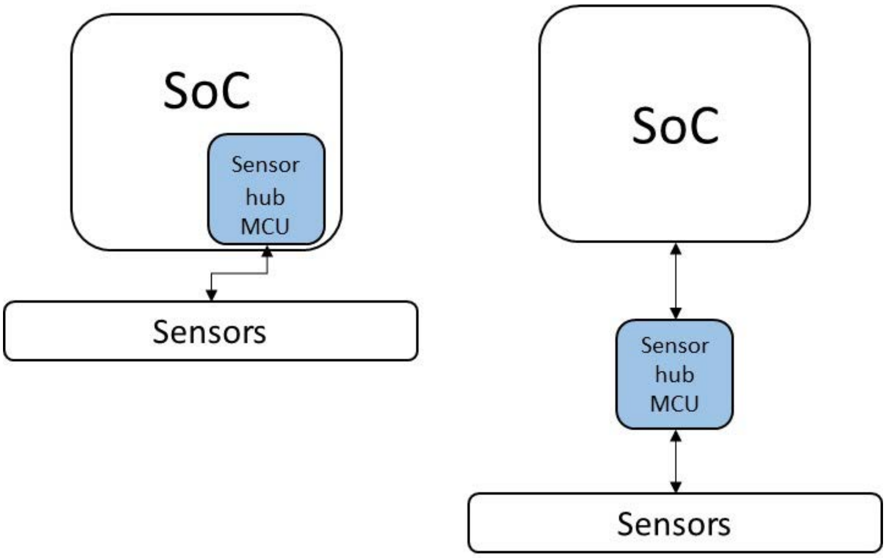

Figure 2: Sensor hub architectures

The sensor hub mainly includes the following functional modules:

- data and algorithm processing module;
- driver management module;

- microkernel OS;
- storage.

Figure 3 shows the functional module architecture.

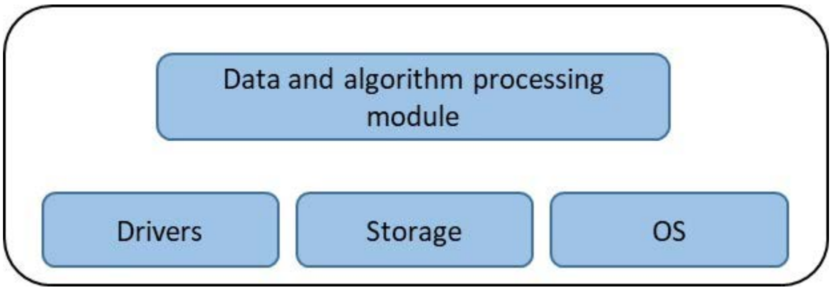

Figure 3: Sensor hub functional modules

The functions of each module are as follows:

- data and algorithm processing module: processes the input sensor hub data based on application requirements;
- driver management module: manages the driver, power supply, and configuration of sensors;
- microkernel OS: An operating system based on the microkernel architecture. A microkernel consists of a group of software programs that are minimized and responsible for providing various mechanisms and functions required for implementing an operating system;
- storage: a module that provides storage functions on the sensor hub.

4.3 Sensor hub interfaces

As shown in Figure 4, the sensor hub supports three types of interfaces.

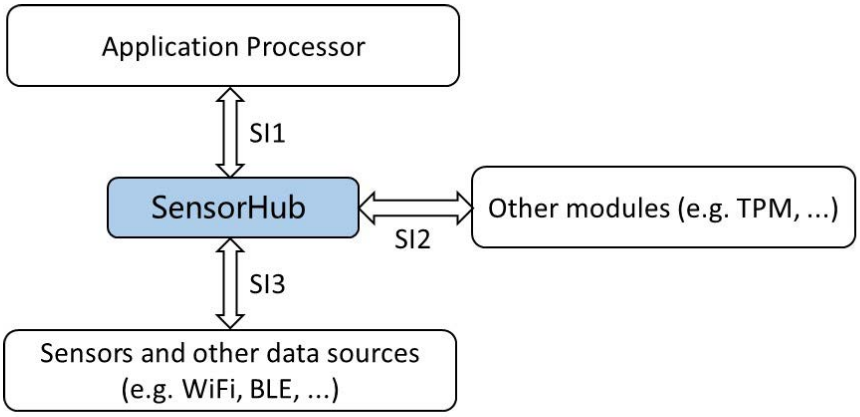
Application Processor
SI1
SensorHub
SI2
Other modules (e.g. TPM, ...)
SI3
Sensors and other data sources (e.g. WiFi, BLE, ...)

Figure 4: Sensor hub interfaces

SI1: the interface between the sensor hub and the application processing module to implement requests and responses between applications and sensor hub.

SI2: the interfaces between the sensor hub and other modules in the security domain, such as interface between the sensor hub and the TPM, to implement data transmission between the sensor hub and the TPM.

SI3: the interfaces between the sensor hub and the different data sources, enabling the sensor hub to obtain data from components such as sensors or chips.

4.4 Data Type

4.4.1 Introduction

The data considered in the present document refers to the data that is processed by the sensor hub and is related to application service functions. This type of data can be associated with the users, therefore they need to be handled granting their security and privacy. The sensor hub considers three different data categories related to the different data processing steps: raw data, process data, and result data.

4.4.2 Raw data

4.4.2.1 General

Raw data refers to unprocessed data received by the sensor hub trough interface SI3 from components such as sensors and chips. Based on the sensors and chipset involved in the data collection, this data can include the sensor data, location data, and other information type data.

4.4.2.2 Sensor data

The sensor data include but are not limited to: motion data, optical data, pressure data, geomagnetic data, and others data. Table 1 lists some examples of sensors and the possible related applications.

Table 1: Types and functions of sensor

Sensor type	Sensor	Function	Application
Pressure	Barometer	Perceive barometric value of the area	Calculates the altitude of the consumer device to assist in positioning.
Temperature	Thermometer	Perceive temperature value of the area or of the body	Provide temperature value for eHealth applications or the temperature of the area for weather applications.
Motion	Accelerometer	Acceleration value of the measured object	Pedometer, mobile terminal gesture recognition, etc.
	Gyroscope	The angular velocity of the calculated object at the time	Photo image stabilization and auxiliary positioning.
Geomagnetic sensor	Magnetometer	Magnetic field strength around the measured object	Compass, auxiliary positioning, etc.
Photoelectric sensor	Proximity light	Distance to the proximity of the perceived object	Automatic screen on or off.
	Ambient Light	Perception of ambient light	Adjusting the screen brightness of a mobile terminal.
Environmental multimedia information sensor	Ambient audio and video sensor	Audio and video data collected by sensors around the terminal environment	Assists user status recognition and gesture recognition.
	Ultrasonic sensor	Use of ultrasonic data from terminals acquired by sensors	Terminal proximity functions.

4.4.2.3 Location data

Location data includes location information such as cell information and GNSS data. There are two types of position data components: coarse position data and precise position data. Cell information belongs to coarse location data, and GNSS data belongs to precise location data. Both can be used for positioning, track recording, and geo-fencing event identification.

4.4.2.4 Other Information Types

There are data other than the foregoing data processed by the sensor hub such as a peer BLE/WLAN device status.

NOTE: The BLE/WLAN device status at the peer end can be used for locating faults.

4.4.3 Processing data

Process data is temporary data generated by the sensor hub based on raw data processing, for example, location data recorded during trace generation.

4.4.4 Result data

The result data is the outcome data from the raw data or processing data by sensor hub, such as step counting data, or activity recognition. The result data are then delivered to the requested application on the application processor trough interface SI1.

Data delivered singly or in batches directly to the application processor from the sensor hub can be either raw data or result data, such as trace generation data.

4.4.5 Data classification

To enable the sensor hub to provide a complete security protection mechanism for the data processed by itself, data are classified into three levels based on the impact of the leakage on user privacy. This classification is in line with those defined in ETSI TS 103 732 [1].

The sensor hub supports the following classification of user data assets:

- Low: the disclosure of the data will have no impact on the user privacy, e.g. pressure value.
- Medium: the disclosure of the data will have a limited impact on the user privacy, e.g. step count data or user posture.
- High: the disclosure of the data will seriously affect the user privacy e.g. sensitive health data.

5 Security threats

5.1 Assets

The assets to be protected within the sensor hub are listed hereafter:

- Data stored in the sensor hub such as raw data, process data and result data.
- Stored credential for the sensor hub access.

5.2 Threats

5.2.1 General

The sensor hub is a built-in or an external MCU (see clause 4.2) and the threats can be enforced on its interfaces described in clause 4.3.

5.2.2 Eavesdrop

An entity (e.g. a malicious or poorly programmed application or local agent able to access in some way the sensor hub interfaces) is capable to read communication between the sensor hub and other entities and thereby access confidential data assets in transit.

5.2.3 Modify communications

An entity can intercept the communication between the sensor hub on its interfaces and thereby modify data assets in transit.

5.2.4 Modification of the sensor hub algorithms used to process data

An entity (e.g. a malicious application) can modify the algorithms used by the sensor hub to process data and therefore alter the result. Data provided to the application processor are wrong, leading to unintended information disclosure or denial of service.

6 Security requirements

6.1 General requirements

Provision 6.1-1: Sensor hub shall be implemented in a hardware isolated secure execution domain.

NOTE: As described in clause 4.2 the sensor hub can be either build-in in a SoC or be an external discrete component.

Provision 6.1-2: The integrity of the sensor hub algorithms used to process raw data shall be verified.

Provision 6.1-3: If the sensor hub is part of a consumer mobile device Provision 6.1-2 shall be enforced by the software integrity requirements defined in ETSI TS 103 732 [1].

Provision 6.1-4: If the sensor hub is part of an consumer IoT device Provision 6.1-2 shall be enforced software integrity provisions defined in ETSI EN 303 645 [2].

6.2 Data collection and process requirements

Provision 6.2-1: When collecting data the sensor hub shall not collect more data than requested by the application.

EXAMPLE: When an application requests not to monitor the heart rate continuously, the sensor hub collects heart rate data only the time needed to answer the exact request.

Provision 6.2-2: Raw data, processing data and result data shall be processed within the sensor hub secure execution domain.

6.3 Data storage requirements

Provision 6.3-1: Raw data, processing data and result data shall be securely cached within the sensor hub.

EXAMPLE: Data is stored in the sensor hub secure DDR or encrypted in the sensor hub.

Provision 6.3-2: If raw data processing is over, the sensor hub shall delete the raw data.

6.4 Data transfer requirements

Provision 6.4-1: The sensor hub shall implement an authorization mechanism to enable an application to request data. Access of unauthorized applications to the sensor hub data shall be blocked.

Provision 6.4-2: The sensor hub shall transfer to applications only raw data and processing data which need to be presented to the user (such as trace data) and the result data. Raw data and processing data which do not need to be presented to the user shall not be transferred out of the sensor hub to applications or other devices with the exception of under the user's permission.

6.5 Sensor hub interfaces

Provision 6.5-1: The sensor hub interfaces with the application processor (SI1) and with other modules (SI2) shall be protected to avoid unwanted disclosure of data.

Provision 6.5-2: The sensor hub interfaces with the application processor (SI1) and with other modules (SI2) shall be protected against replay attack.

Annex A (informative): Possible sensor hub implementations

A.1 Introduction

The present document defines the security requirements of the sensor hub used in consumer devices.

This annex explains the possible relationship between the requirements defined in the present document and those defined in ETSI TS 103 732 [1] and ETSI EN 303 645 [2] when the sensor hub is respectively included in a consumer mobile device or in a consumer IoT device.

A.2 Sensor hub in consumer mobile device

When the sensor hub is included in a consumer mobile device it is part of the TSF when ETSI TS 103 732 [1] is used to evaluate the consumer mobile device security.

The following table shows how the requirements of the present document may be covered by the ETSI TS 103 732 [1].

Table A-1

The present document	ETSI TS 103 732 [1]	Comments
Provision 6.1-1	Not covered	The TOE includes the hardware platform, physical enclosure and peripheral components such as sensors and the display but it does not mandate the way the sensor hub is implemented. Provision 6.1-1 is added in the TOE Security Target.
Provision 6.1-2	**FPT_TST.1 TSF**	**O.SELF_PROTECTION** and **O.SECURE_BOOT** cover this requirement.
Provision 6.2-1	Not covered	Provision 6.2-1 is added in the TOE Security Target.
Provision 6.2-2	Not covered	Provision 6.2-2 is added in the TOE Security Target.
Provision 6.3-1	Not covered	Provision 6.3-1 is added in the TOE Security Target.
Provision 6.3-2	Not covered	Provision 6.3-2 is added in the TOE Security Target.
Provision 6.4-1	**FDP_ACF.1**	**O.ACCESS_CONTROL** covers this requirement.
Provision 6.4-2	Not covered	The TOE does not specify behaviors between its own hardware components, therefore provision 6.4-2 is added in the TOE Security Target.
Provision 6.5-1	**FTP_ITC.1**	The Security Target declares SI1 and SI2 interfaces to be secure.
Provision 6.5-2	**FTP_ITC.1**	The Security Target declares SI1 and SI2 interfaces to be secure.

A.3 Sensor hub in consumer IoT device

When the sensor hub is included in a consumer IoT device it can be considered as part of the consumer IoT device when it is evaluated against ETSI EN 303 645 [2].

Table A-2 shows how the requirements of the present document can be covered by the ETSI EN 303 645 [2].

Table A-2

The present document	ETSI EN 303 645 [2]	Comments
Provision 6.1-1	Not covered	
Provision 6.1-2	**Provision 5.7-1**	
Provision 6.2-1	**Provision 6-4**	
Provision 6.2-2	Not covered	
Provision 6.3-1	Not covered	
Provision 6.3-2	Not covered	
Provision 6.4-1	**Provision 5.8-2**	This provision may be used assuming that the application requesting data to the sensor hub is an associated service.
Provision 6.4-2	Not covered	
Provision 6.5-1	**Provision 5.8-1** **Provision 5.8-2**	This provision may be used considering that the data are transferred within the IoT device components.
Provision 6.5-2	**Provision 5.8-1** **Provision 5.8-2**	This provision may be used considering that the data are transferred within the IoT device components.

A.4 Example of a sensor hub implementation in a SoC

This clause describes a possible implementation of a sensor hub in a SoC and shows the relation with the provisions provided by the present document in clause 6.

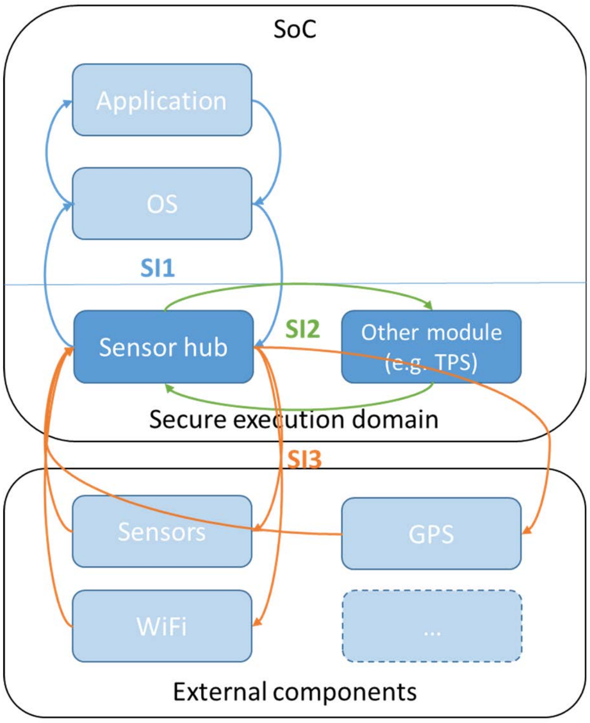

Figure A-1: Sensor hub in a SoC

The sensor hub resides in the secure execution domain of the SoC (see clause 6.1) and it is connected to the non-secure part of the SoC through the SI1 interface. The only way applications can request data to the sensor hub is through the OS and the data provided to the applications are only those processed by the sensor hub (see clause 6.4). The processing, storage and management of the data retrieved by the external component are done only in the sensor hub (see clauses 6.2 and 6.3). The sensor hub can be connected to other modules in the secure execution domain through the SI2 interface. This can allow the sensor hub to exploit services provided by a TPM for example.

History

Document history		
V1.1.1	January 2023	Publication