ETSI TS 103 887 V0.3.0 (May-2025)

Smart Body Area Network (SmartBAN);
Smart Coordinator

Reference
<Workitem>

Keywords
<keywords>

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:
https://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 by generally accepted engineering or other professional standards and applicable regulations.
No recommendation as to products 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

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Contents

Intellectual Property Rights 7
Foreword 7
Modal verbs terminology 7
Executive summary 8
Introduction 8
1 Scope 9
2 References 9
2.1 Normative references 9
2.2 Informative references 9
3 Definition of terms, symbols, and abbreviations 10
3.1 Terms 10
3.2 Symbols 10
3.3 Abbreviations 10
4 SmartBAN Architecture 11
4.1 General description 11
4.2 Architecture Overview 11
4.3 Data Transport Architecture 11
4.3.0 Introduction 11
4.3.1 Physical channels 12
4.3.2 Transport channels 12
4.3.3 Logical channels 13
4.4 Methodology 13
4.4.0 Introduction 13
5 Smart Coordinator core architecture 15
5.1 Introduction 15
5.2 Smart coordinator resource manager protocol 15
5.3 Security protocol 16
5.4 Discovery protocol 16
5.5 Baseband protocol 16
5.6 Link Control Signaling protocol 16
6 Smart Coordinator Frame format 18
6.1 Basic components 18
6.2 Conventions 18
6.3 General SC frame format 19
6.3.0 SC Header 20
6.3.1 Frame Control field 20
6.3.1.1 MAC Addressing Mode subfield 21
6.3.1.2 ACK Type subfield 21
6.3.1.3 Cipher suite subfield 21
6.3.1.4 SC Frame Type subfield 22
6.3.1.5 SC Subtype frame subfield 22
6.3.1.6 Fragments subfield 23
6.3.1.7 More Data subfield 23
6.3.1.8 IE present subfield 23
6.3.2 Addressing fields 23
6.3.2.1 Destination Address field 23
6.3.2.1 Source Address field 24
6.3.2.2 Remote Destination Address field 24
6.3.3 Sequence Control field 24
6.3.3.1 Fragment Number field 24
6.3.3.2 Sequence Number field 24
6.3.4 QoS Control field 25

6.3.4.1 Traffic ID subfield 25
6.3.4.2 End of Service subfield 26
6.3.4.3 ACK Indicator subfield 26
6.3.4.4 Aggregate SCDU subfield 27
6.3.4.5 Group TX Limit subfield 27
6.3.4.6 Group TX Requested subfield 27
6.3.4.7 Buffer State subfield 27
6.3.4.8 Queue Size subfield 27
6.3.5 Frame Body field 27
6.3.6 FCS field 27
6.4 SC frame types 28
6.4.0 General 28
6.4.1 Control frames 28
6.4.1.1 Format of Control frames 28
6.4.1.2 BlockACK.Request frame format 28
6.4.1.2.1 Block Control subfield 29
6.4.1.2.2 Block Information subfield if Multi-TrafficID=0 29
6.4.1.2.3 Block Information subfield if Multi-TrafficID=1 30
6.4.2 Data frames 30
6.4.2.1 Data frame format 30
6.4.2.2 Addresses 30
6.4.2.3 Other MAC Header fields 32
6.4.2.4 Frame Body field 32
6.4.3 Management frames 32
6.4.3.1 Format of Management Frames 32
6.4.3.2 Discovery Frame Body format 32
6.4.3.2.1 The BAN ID subfield 33
6.4.3.2.2 Capability Information subfield 33
6.4.3.3 Disassociation frame body format 33
6.4.3.4 Association Request body frame format 34
6.4.3.5 Association Response Frame Format 37
6.4.3.5.1 QoS Map subfield 37

7 Smart Coordinator Service Definition 41
7.1 Overview of SC services 41
7.1.1 Data service 41
7.1.1.1 General 41
7.1.1.2 Determination of UP 41
7.1.1.3 Security services 41
7.1.2 MSDU ordering 41
7.1.3 MSDU format 42
7.1.4 SC service interface role 42
7.1.5 Provision of the SC service 42
7.2 SC data service architecture 43
7.3 Smart Coordinator data service specification 45
7.3.1 General 45
7.3.2 UNITDATA.request 45
7.3.2.1 Function 45
7.3.2.2 Semantics of the service primitive 45
7.3.2.3 When generated 46
7.3.2.4 Effect of receipt 46
7.3.3 MA-UNITDATA.indication 46
7.3.3.1 Function 46
7.3.3.2 Semantics of the service primitive 46
7.3.3.3 When generated 47
7.3.3.4 Effect of receipt 47
7.3.4 UNITDATA-STATUS.indication 47
7.3.4.1 Function 47
7.3.4.2 Semantics of the service primitive 47
7.3.4.4 When generated 48
7.3.4.5 Effect of receipt 48

8 Cybersecurity protocol 49
8.1 General 49
8.2 Cybersecurity set up 50
8.2.1 Introduction 50
8.2.2 Credentials of wearables and medical implants 50
8.3 Authenticated channel for registration of devices 51
8.3.1 Authentication of devices to the manufacturer's repository 52
8.3.2 Authentication of manufacturer's repository to device 52
8.3.3 Authentication phase accomplished 53
8.4 Cryptographic dependencies 53
8.4.1 General 53
8.4.2 Oblivious Pseudorandom Function 53
8.4.3 Cryptographic Hash Function 54
8.4.4 Key Derivation Function 54
8.4.5 Stream cipher 54
8.4.6 Lightweight block cipher 54
8.5 Asymmetric Password Authenticated Key Exchange 54
8.5.1 Public parameters and components 54
8.5.2 Registration protocol 55
8.5.3 Login protocol 55
9 Support for 5G services 57
9.1 Introduction 57
9.2 Overview of 5GCN 57
9.3 Support for non-3GPP access networks 58
9.3.1 General 58
9.3.2 Untrusted non 3GPP access 60
9.3.2.1 General 60
9.3.2.2 Summary of connection protocols 61
9.3.2.3 Prerequisites for Untrusted Non-3GPP Access 61
9.3.2.4 Steps Connection Process 62
9.3.2.5 Protocol description from SmartBAN coordinator to 5GCN via N3IWF 63
9.3.2.5.1 General 63
9.3.2.5.2 Initial connection set up 63
9.3.2.5.3 SmartBAN coordinator establishes IPSec Tunnels with IKEv2 63
9.3.2.5.4 IPSec Child SA Activation 65
9.3.2.5.5 5G Registration & PDU Session Setup 65
9.3.2.6 Summary of security 66
9.3.3 Trusted non-3GPP access network 66
9.3.3.1 General 66
9.3.3.2 Wireless access with TNGF 66
9.3.3.2 Protocol description from SmartBAN coordinator to 5GCN via TNGF 67
9.3.2.5.1 General 67
9.3.2.5.2 Initial connection set up 67
9.3.2.5.3 EAPOL-Start (Trigger EAP-AKA') 67
9.3.2.5.4 RADIUS Authentication (AP ↔ 5GCN) 67
9.3.2.5.5 5G Key Derivation 68
9.3.2.5.6 TNGF Registration 68
9.3.2.5.7 PDU Session Establishment 69
9.3.2.5.8 User Plane Activation 69
9.3.2.6 Wireless access with TWIF 69
9.3.2.7 Protocol description from SmartBAN coordinator to 5GCN via TWIF 71
9.3.2.7.1 General 71
9.3.2.7.2 TWAP (L2) 71
9.3.2.7.3 Authentication Protocols 72
9.3.2.7.4 5G Core Signaling (Control Plane) 72
9.3.2.7.5 User Plane Protocols 73
Annex A (normative): Management Information Base (MIB) 75
Annex (informative): Bibliography 76

Annex (informative): Change History 77

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations about 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).

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

Foreword

This Technical Specification (TS) has been produced by the ETSI Technical Committee SmartBAN (SmartBAN).

The contents of the present document are subject to continuing work within the TC SmartBAN and may change following formal TC approval. Should the TC change the contents of the present document, it will be re-released by the TC with an identifying change of release date and an increase in version number as follows:

Version *x. y. z*

where:

x the first digit:

0: presented to the TC for information.

1: presented to the TC for approval.

2: or greater shows an approved document under change control.

y the second digit is incremented for technical changes, corrections, or updates.

z the third digit is incremented for editorial changes.

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.

Executive summary

TBD

Introduction

TBD

1 Scope

The present document specifies the functional requirements and procedures to implement as a smart coordinator of a SmartBAN ad-hoc network. The smart coordinator assembles the required protocols for the interaction of the SC layer with higher layers, security manager, and bridge to infrastructure networks.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or nonspecific. 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 that 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 103 326 v1.2.1 (SmartBAN); “Enhanced Ultra-low Power Physical Layer”.

[2] ETSI TS 103 325 v1.1.1 (SmartBAN); “Low Complexity MAC for SmartBAN”.

[3] NIST FIPS PUB 202: “SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions”.

[4] NIST ASCON

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or nonspecific. 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 about a particular subject area.

[i.1] ETSI TS 103 645 “Cyber Security for Consumer Internet of Things”.

3 Definition of terms, symbols, and abbreviations

3.1 Terms

For the present document, the following terms apply:

Smart coordinator: Device operating at the link layer that provides an interface to the MAC layer for operation over multiple hubs for coexistence, a bridge to infrastructure domains, and cryptographic material and primitives management.

3.2 Symbols

For the present document, the [following] symbols [given in ... and the following] apply:

3.3 Abbreviations

For the present document, the following abbreviations apply:

ECC	Elliptic Curve Cryptography
TSN	Time Sensitive Networking
QoS	Quality of Service
MLDE	MAC Layer Data Entity
MLME	MAC Layer Management Entity
PLDE	PHY Layer Data Entity
PLME	PHY Layer Management Entity
MAC	Medium Access Control
SAP	Service Access Point

4 SmartBAN Architecture

4.1 General description

4.2 Architecture Overview

SmartBAN has a layered architecture. The core architecture of SmartBAN is shown in Figure 1, and comprises the following components:

— PHY and MAC layers*:* These are the layers responsible for performing low-level operations like transmission and reception of radio signals, discovering devices in the vicinity, exchanging data packets by managing access to the shared radio resources, handling priority, and low-power modes.

— Smart Coordinator layer: This layer is part of the link layer or layer 2 (L2) and is responsible for the security protocol, discovery protocol, making associations, scheduling, flow control, an interface to upper layers, and a bridge to infrastructure networks at L2.

— Upper Layers*:* These layers make use of the functionality provided by the lower layers to provide more complex functionality, like segmentation of data information, and tasks of MMI (Man Machine Interface), so that end users can make use of the SmartBAN functionality, among others.

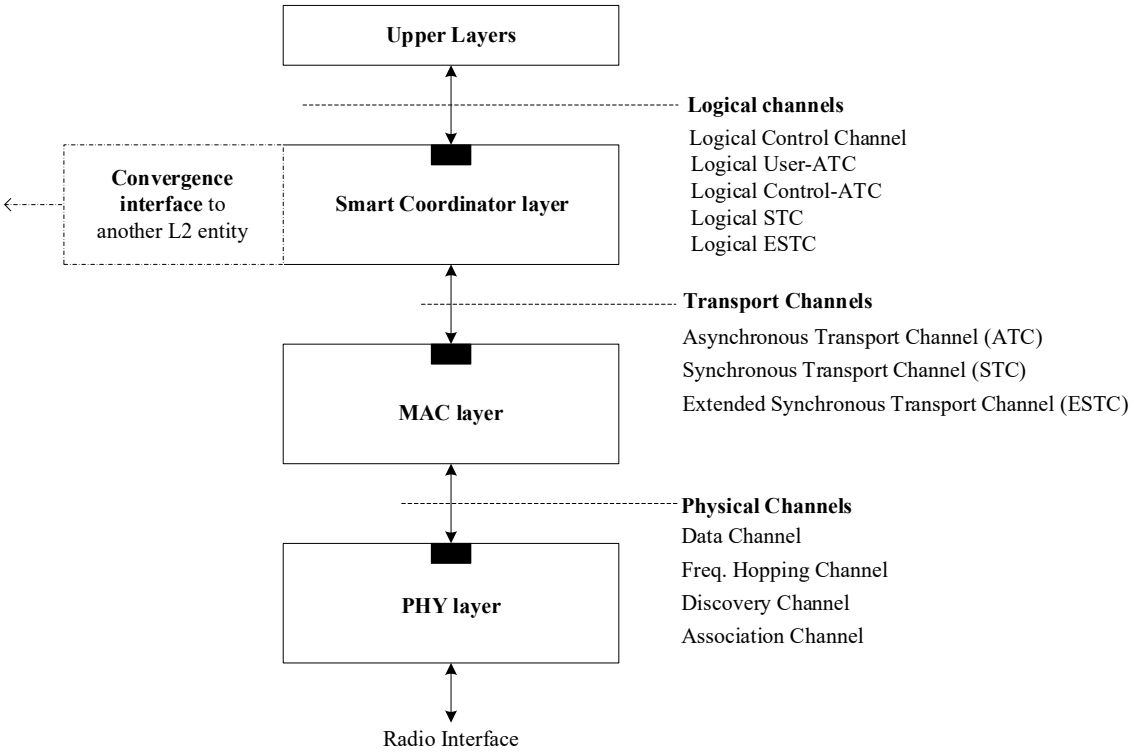


Figure 1 — SmartBAN core and transport architectures.

4.3 Data Transport Architecture

4.3.0 Introduction

SmartBAN operational modes follow the same generic transport architecture shown in Figure 1. The SmartBAN transport architecture includes a sub-division distinguishing between logical links and transport links. This sub-division provides a general concept of a logical link, normally associated with an application and type of data traffic, that provides an independent transport between two or more devices.

4.3.1 Physical channels

The PHY layer constructs the baseband signal to be transmitted by the radio interface over a radio channel, henceforth known as the physical channel.

The physical channel is subdivided into time units called “time slots”. Each time slot is X µsec with half duplex transmission using the Time Division Duplex (TDD) scheme. A data packet may occupy several time slots depending on the packet’s length. An optional frequency hopping scheme is used for interference mitigation to improve reliability, such that packets are transmitted on the next pseudo-random central frequency band. The frequency hop occurs once per packet.

Four physical channels are specified as follows:

- Data channel (DC): This channel is used for data communication between devices in a SmartBAN.
- Frequency Hopping Channel (FHC): This is similar to the Data Channel, but for devices that have frequency hopping enabled.
- Scan Channel (SC): This channel is used for the discovery of devices.
- Association Channel (AC): This channel is used for creating a communication session between discovered devices.

A device shall use only one physical channel at a time.
A physical channel defines a physical link as a baseband-to-baseband connection between two entities at the physical layer. Note that up-conversion mixes a baseband signal onto the carrier signal that is fed to the antenna's output.

There can be only one physical link between the Smart Coordinator and a wearable or implant, henceforth known as a device. However, there could be more than one logical link on top of a physical link.

Note that SmartBAN does not support direct communication between two devices.

With the support of TS 103 326 and TS 103 325, the Smart Coordinator shall employ Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA), while optionally multi-use multiple access to support multiple concurrent operations. Using the combination of FDMA and TDMA makes SmartBAN able to support large numbers of devices and improve reliability.

- According to the channelization specified in TS 102 326, x radio channels are used in the FDMA scheme. Three channels may be used as scan channels and 37 channels may be used as data channels. The Smart Coordinator uses a channel selection algorithm to choose a radio channel for each time slot. The quality associated with each channel is monitored, and the system adapts to the conditions encountered, ceasing to use channels that are found to be experiencing problems, perhaps due to coexistence with other wireless devices operating in the same frequency band. This has the benefit of making SmartBAN communications dependable in busy radio environments.
- A TDMA-based polling scheme is used in which one device transmits a packet at a predetermined time and a corresponding device responds with a packet after a predetermined interval. As mentioned before, the radio channel is subdivided into time slots. Data is transmitted in packets that are positioned in these time slots.

4.3.2 Transport channels

A transport channel is formed on a physical channel to transfer control signals and synchronous or asynchronous user data coming from higher layers. Analogous to a physical link, a logical link is formed onto a transport channel.

The Smart Coordinator generates the creation, modification, and release of logical links and associated transport channels using a link layer protocol (the name is TBD). Such protocol controls functions such as enabling cyber-security on the logical link for confidentiality and data integrity protection, transmitting power adaptation on the physical link, and QoS settings for a logical link.

The following three Transports Channels are specified as follows:

— Asynchronous Transport Channel (ATC): This channel is used to carry control signals, user data, and broadcast data. It provides a [packet-switched] datagram connection between the Smart Coordinator and all devices that are active in the SmartBAN. The default ATC connection is created when a device joins a SmartBAN. This transport is used to send data in bursts whenever data is ready and whenever a time slot is available and not reserved for the Synchronous Transport Channel (see next bullet).
Only one single ATC is created between the Smart Coordinator and a device. Hence, higher-layer protocols shall multiplex their data on an ATC. Moreover, the ATC supports packet retransmissions to ensure data integrity when the packets are delivered to the application on the receiver side.

— Synchronous Transport Channel (STC): This channel provides support for the continuous transfer of data. The scheduling protocol reserves and maintains time slots on the physical channel to guarantee continuous transmission of data. STC links carry x kb/s of information data in both directions (synchronous transmission). If a data packet is corrupted or lost during transmission, it is not retransmitted as the target data traffic requires a time-bounded latency. Unlike the ATC, the STC does not support multiplexed logical links on top. Hence, there is no further layering of any stack components above the STC. However, the Smart Coordinator can support an ATC and an STC simultaneously, if required. One practical example is when connecting to a wearable on a headband. The Smart Coordinator establishes both an ATC to carry commands (increase/decrease sampling, disconnect, etc.), while the STC is used to carry the neuro recording traffic.

— Asynchronous-Synchronous Transport Channel (ASTC): This channel is used when reserving time slots (similar to the STC) but with the possibility of limited retransmission. Moreover, the data traffic may be symmetric or asymmetric. For example, it is possible to use 3-slot packets in one direction and 1-slot packet in the reverse direction. The ASTC provides better reliability by providing a limited number of retransmissions of packets that get corrupted or lost. The retransmission slots are allocated right after the reserved slots and are only used if the timing constraints of the data traffic are still met.

4.3.3 Logical channels

The logical channels are supported on top of the transport channels. Five types of logical links are specified as follows:

— Logical Control Channel (LCC): The information of this channel is carried in the corresponding layered packet header. It contains low-level information like acknowledgment/repeat mechanisms (ARQ), flow control, and payload data characterization.

— Logical User-Asynchronous Transport Channel (LUATC): This channel is used by the Smart Coordinator for transferring asymmetric traffic of user data and the upper layers.

— Logical Control- Asynchronous Transport Channel (LCATC): This channel carries the control information between the Smart Coordinator protocols and devices.

— Logical Synchronous Transport Channel (LSTC): This channel is used by the Smart Coordinator for transferring symmetric traffic with bounded latency of user data and the upper layers.

— Logical Asynchronous-Synchronous Transport Channel (LASTC): This channel is used by the Smart Coordinator for transferring either symmetric or asymmetric traffic with bounded latency of user data and the upper layers.

4.4 Methodology

4.4.0 Introduction

In summary, above the physical radio channel, there are concepts of links (physical channels), transport channels, logical channels, and associated protocols. The hierarchy is shown in Figure 1.

With the support of a physical channel, a physical link (channel) is formed between devices. The active physical link provides bidirectional packet transport between the Smart Coordinator and devices (wearables or implants) for the

exchange of data. In addition, the physical link provides a unidirectional packet transport for discovery. The Smart Coordinator may serve several physical links at a time via the multiple access described in TS 103 325.

The physical link is used as a transport for one or more logical links that support asynchronous or synchronous traffic. Traffic on logical links is multiplexed onto the physical link by the Smart Coordinator scheduler coordinating the radio resources.

Devices that are active in a SmartBAN start with an asynchronous logical transport connection by default. The Smart Coordinator Control Layer protocol coordinates the operation of devices in the SmartBAN and provides services to manage the lower layers (PHY and MAC).

In addition, the Smart Coordinator Control Layer carries out fragmentation and de-fragmentation of data over-the-air, multiplexing, and de-multiplexing of multiple channels over a shared logical link and supports the security manager protocol. The different logical channels support different application data transport requirements. Each logical channel has several characteristics. These characteristics include flow control, acknowledgment/repeat mechanisms, sequence numbering, scheduling for data traffic, discovery, and cybersecurity mechanisms. Hence, the Smart Coordinator supports protocols for multiplexing, segmentation/reassembly of Service Data Units (SDUs) from/to upper layers, retransmissions and flow control, scheduling, fragmentation/recombination of Protocol Data Units (PDUs) from/to the MAC layer, encryption, decryption, authentication of SDUs.

Note: Encapsulation of SDU into PDUs. Protocol Data Units (PDUs) are packets exchanged between peer entities in the same layer. Service Data Units (SDUs) are packets handed to a lower layer by an upper layer. A PDU is typically an SDU with an additional header or trailer that carries the information of the upper layer protocol. We say that the SDU is encapsulated into the PDU.

5 Smart Coordinator core architecture

5.1 Introduction

Figure 2 illustrates the core architecture of the Smart Coordinator, functions, and protocols.

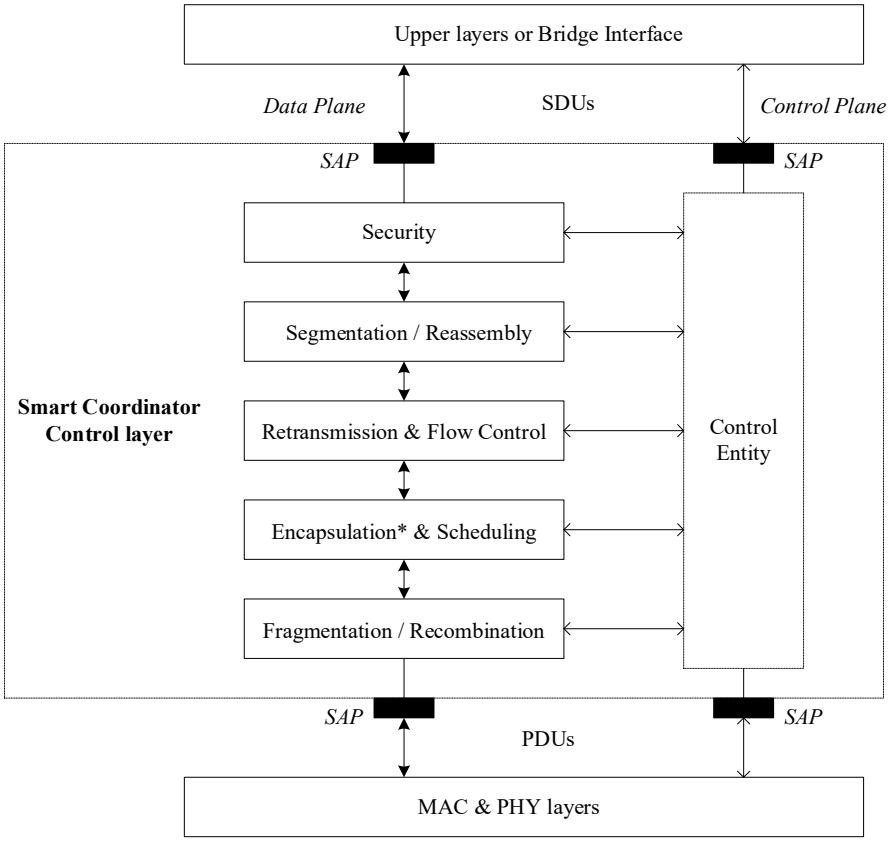


Figure 2 — Smart Coordinator core architecture.

5.2 Smart coordinator resource manager protocol

The Smart Coordinator resource manager is responsible for creating, coordinating, and closing logical channels for the transport of service protocols and application data streams from upper layers. It interacts with a device to create these logical channels and connect their endpoints to the appropriate entities as well as the general control of logical channel and associated transport channel attributes such as the enabling of encryption on the transport channel, and adapting of transmit power on the physical link.

Also, it is responsible for managing the ordering of submission of PDU fragments to the MAC layer and relative scheduling between channels to ensure that logical channels are not denied access to the physical channel due to the exhaustion of resources in the Smart Coordinator and radio interface (the Smart Coordinator does not have limitless buffering and the radio interface does not have infinite bandwidth).

Editor note: Check if another figure may be required.

Editor note: Check if cybersecurity primitives are applied on the logical or transport channel.

5.3 Security protocol

The Security Protocol generates encryption keys, and identity keys and establishes secure unicast sessions without relaying in a trusted 3rd party or Public Key Infrastructure (PKI). The security protocol operates over a dedicated transport channel. Also, it generates random addresses and resolves random addresses to known device identities.

Note: This TS assumes devices are equipped with a hardware security module (HSM) to store cryptographic keys, and secrete material (random nonces) and perform security primitives.

Editor note: Check if secure multicast sessions may be required.

5.4 Discovery protocol

The discovery function is responsible for operations that are not directly related to data transport, such as inquiring about the presence of nearby SmartBAN devices, connecting to SmartBAN devices, or making SmartBAN devices discoverable by other devices.

5.5 Baseband protocol

The baseband protocol is responsible for the access to the wireless medium with two main functions:

— A scheduler grants time and frequency resources on the physical channels to the entities that have negotiated a communication session.
— An association procedure negotiates access to a SmartBAN. The association procedure commits to delivering a certain QoS that is required to provide a user application with an expected performance based on TS 103 326 and TS 103 325, including data and privacy protections.

The association procedure for SmartBAN access and scheduling functions takes into account the current status of connected devices in a SmartBAN and the use of the wireless medium to carry out inquiries, make connections, be discoverable, or take probe readings from unused carriers during the adaptive frequency hopping mode.

5.6 Link Control Signaling protocol

The Link Control Signaling protocol is responsible for the segmentation and reassembly of SmartBAN data packets to be delivered and received by the radio interface via the MAC layer. The Link Control Signaling protocol monitors the link quality and takes necessary actions to maintain a stable connection. This includes error detection and correction mechanisms, retransmission of lost packets, and adaptation to changing radio frequency conditions.

It works in close conjunction with the scheduling function, which is used for flow control, acknowledgment, and retransmission of data or control packets. The interpretation and control of these signals are associated with the baseband protocol's scheduler.

A summary of the protocol stack is shown in Table 1.

Table 1 — Protocol stack responsibilities.

Layer/Protocol	Responsibility
PHY layer	Defines the aspects of SmartBAN that are related to the use of the radio interface, including modulation schemes, frequency bands, channel use, transmitter and receiver characteristics.
MAC layer	Defines air interface packet format, bit stream processing procedures such as error checking, a state machine, and protocols for over-the-air communication and link control of sharing the wireless medium.

Smart Coordinator Resource Manager protocol, Discovery protocol, Link Control Signaling protocol	Defines several distinct ways of using the underlying PHY and MAC layers for connectionless, connection-oriented, and asynchronous communication defined as logical and transport channels. Performs segmentation and reassembly of framed PDUs or fragmentation and recombination of unframed PDUs. Defines the functional interface for bi-directional communication of commands and data packets between the Smart Coordinator and nodes, and unidirectional communication for discovery or to be discovered.
Security protocol	A protocol of security procedures to establish secure communication sessions without relying on a trusted 3rd party or public key infrastructure.

The behavior of the Smart Coordinator Control Layer is better understood as a state machine.

Editor note: Add packet formats or packet structure for the logical channel, transport channel, and associated links to be passed to the MAC.

Editor note: Add figures to show the chain processes (PHY channel to logical channel)

Editor note: Add control and management packets.

Editor note: Add the protocols' description and procedures (exchange of data procedure, ordering, ACKs, flow control, etc.).

Editor note: Add state machine.

Editor note: Add bridge to infrastructure initial approach.

Editor note: Check the mapping of MAC addresses to random addresses defined in the MAC.

Editor note: Check interaction between discovery and data communication (periodicity, priority, etc.)

Editor note: Check impact on performance: latency. Other KPIs?

6 Smart Coordinator Frame format

6.1 Basic components

A device compliant with the SmartBAN standard shall be able to properly construct for transmission and decode a subset of the frames specified in this clause upon validation using the frame check sequence following reception. The particular subset of these frames that a compliant device constructs and decodes is determined by the functions supported by that particular device.

Each frame consists of the following basic components:

— A SC Header (SCHR), which comprises frame control, duration, MAC addresses, sequence control information, and QoS control information.

— A variable length Frame Body, which contains data information specific to the frame type and subtype;

— A frame check sequence (FCS) that contains a 32-bit CRC based on ITU-T Recommendation V.4.

6.2 Conventions

Structures defined in the Smart Coordinator layer are described as a sequence of components (e.g., fields, subfields, elements and sub-elements) in specific order. Each figure and table in clause 6 illustrate the components of a SC frame and in the order in which they are passed to the MAC layer, from left to right and then from top to bottom.

Unless specified otherwise, a number in a field is encoded as an unsigned integer.

A field or subfield within the figure depiction of a frame format that includes a decimal value within parentheses indicates that this field or subfield is set to the indicated value upon transmission.

In figures, all bits within fields are numbered, from 0 to k, where the length of the field is $k + 1$ bits. Bits within numeric fields that are longer than a single bit are depicted in increasing order of significance, i.e., with the lowest numbered bit having the least significance. The octet boundaries within a field can be obtained by taking the bit numbers of the field modulo 8. Octets within numeric fields that are longer than a single octet are depicted in increasing order of significance, from lowest numbered bit to highest numbered bit. The octets in fields longer than a single octet are sent to the Network Interface Controller (NIC) in order from the octet containing the lowest numbered bits to the octet containing the highest numbered bits.

Any field containing a Cyclic Redundancy Code (CRC) is an exception to this convention and is transmitted commencing with the coefficient of the highest-order term. There are other exceptions; these are explicitly indicated in the description of the field in question.

Values specified in decimal are coded in natural binary unless otherwise stated. Values in tables are shown in decimal notation.

The 48-bit MAC addresses are assigned as ordered sequences of bits. The bit 0 is always transferred first, while bit 47 of the MAC address is always transferred last.

Transmission and processing of bits in fields is made on an octet basis as indicated in Figure 3. The order of transmission and processing per octet starts from the Least Significant Bit (LSB) to the Most Significant Bit (MSB).

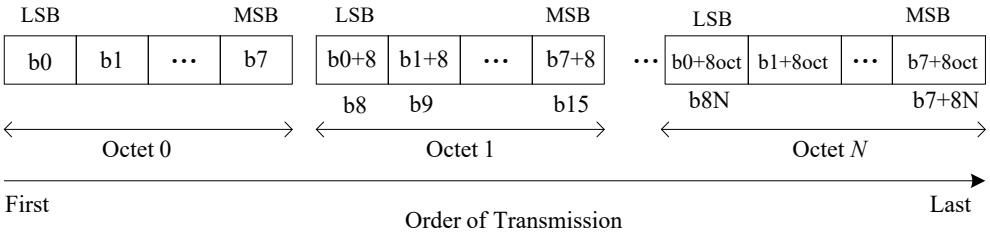


Figure 3—Representation of transmission and processing of bits in Fields.

Bits in concatenated octets are indexed as $b(m+8oct)$, where m=0, 1,…,7; and oct=0,…,N is the octet number in a Field starting from zero (see Figure 3).

Time intervals are given in terms of integer values of the Time Unit (TU) defined as 1024 microseconds or 1 TU = 10^{-6} (2^{10}) sec.

The TU maintains intervals that are easy to implement in hardware with a 1 MHz clock (dividing the clock signal in half ten times rather than using a PLL or digital divider).

According to the TCP/IP layering model, SC frames are encapsulated in MAC frames as shown in Figure 4.

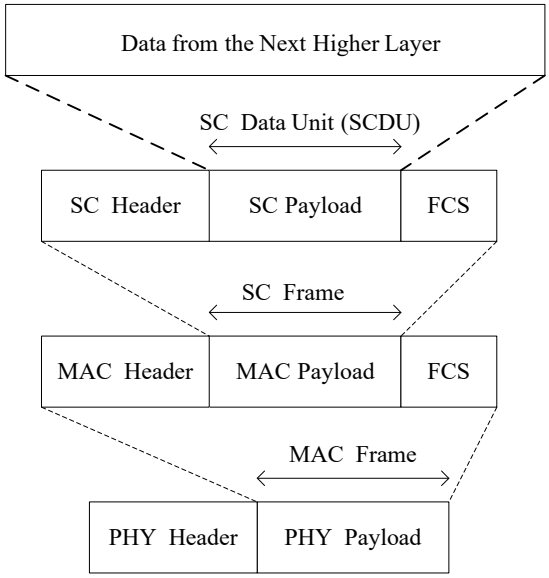


Figure 4 —Smart Coordinator frame encapsulation.

6.3 General SC frame format

The SC frame format comprises a set of fields that occur in a fixed order in all frames. Figure 5 depicts the general SC frame format.

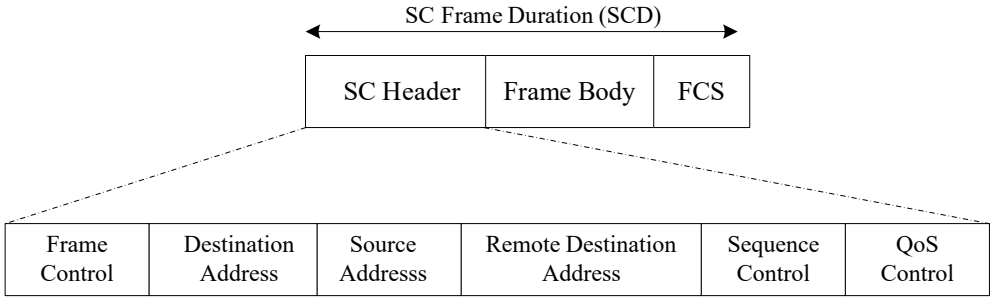


Figure 5—SC frame format

6.3.0 SC Header

SC Header fields description.

6.3.1 Frame Control field

The Frame Control Field is sub-divided into the sub-fields represented in Table 2.

Table 2—Frame Control field

Octet	Bits	Field name	Description
0	b0	Protocol Version	It shall be set to 0 as the first version of the SC layer.
	b1–b2	MAC Addressing Mode	It shall be set according to Table 3 to indicate the appropriate MAC addresses for unicast, multicast, broadcast and bridge mode. MAC addresses will be mapped to the simplified addresses indicated in the MAC specification.
	b3–b4	ACK Type	It shall be set according to Table 4 to indicate the acknowledgment frame requirement for the current received frame.
	b5–b7	Cipher suite	It shall be set according to Table 5.
1	b8–b9	SC Frame Type	See 6.3.1.4
	b10–b12	SC Frame Subtype	See 6.3.1.5
	b13	More Fragments	See 6.3.1.6
	b14	More Data	See 6.3.1.7
	b15	Payload IE present	It shall be set to 1 if Information Element is present.

6.3.1.1 MAC Addressing Mode subfield

Table 3—MAC Addressing Mode encoding

b1–b2	Description
00	The Destination Address field is set to all 1s (broadcast). The recipient SC entity may ignore parsing the Destination Address field.
01	The Destination Address field contains a MAC address of either a SC or a node.
10	The Destination Address field contains the MAC address of a bridge device, and the Remote Address field contains the MAC address of the remote recipient SC entity.
11	Reserved. MAC filtering returns an error.

6.3.1.2 ACK Type subfield

Table 4—ACK Type subfield encoding

b3–b4	ACK Type description
00	No acknowledgment (N-ACK)
01	Block acknowledgment (B-ACK)
10	Reserved
11	Reserved

6.3.1.3 Cipher suite subfield

TBD

Table 5—Cipher Suite subfield encoding

b5–b7	Description
000	
001	
010	
011	

6.3.1.4 SC Frame Type subfield

Table 6— SC Frame Type encoding

b8–b9	SC Type frame description
00	Management
01	Control
10	Data
11	Reserved

6.3.1.5 SC Subtype frame subfield

Table 7— SC Frame Subtype encoding

Type field	b10–b12	Subtype frame description
Management	000	Reserved
Management	001	Security Association
Management	010	Security Disassociation
Management	011	Disassociation/De-authentication
Management	100–111	Reserved
Control	000	R2S (Request 2 Send)
Control	001	TF (Trigger Frame)
Control	010	TFA (Trigger Frame Association)
Control	011	Block ACK Request
Control	100	Block ACK
Control	101–111	Reserved
Data	000	Data
Data	001	Null
Data	010–111	Reserved

6.3.1.6 Fragments subfield

The More Fragments subfield is set to 1 in all Data or Management frames that have another fragment of the current SC frame to follow. Otherwise, it is set to 0.

6.3.1.7 More Data subfield

The More Data subfield is set to 1 to indicate that at least one additional buffered SC frame is present at the for the same device: wearable, or implant or coordinator or bridge. Otherwise, it is et to 0.

6.3.1.8 IE present subfield

The IE Present field shall be set to 1 if IEs are contained in the frame. Otherwise, it is set to 0.

6.3.2 Addressing fields

Each Address field shall contain a 48-bit MAC address as defined by the IEEE Registration Authority for 48-bit Extended Unique Identifier (EUI-48).

MAC addresses can be either universally administered addresses (EUI-48) or locally administered addresses. A universally administered address is uniquely assigned by the IEEE-SA Registration Authority to a Network Interface Controller (NIC) vendor. A locally administered address is defined by software or operators of a system, overriding the EUI-48 address burnt in the NIC attached to a device complying with the SmartBAN specifications.

A MAC address is one of the following types:

1) *Individual or Unicast address*: The MAC address assigned to a device complying with the SmartBAN specifications.

2) *Multicast address*: A locally administered MAC address associated with one or more logically related devices complying with the SmartBAN specifications.

3) *Broadcast address*: A predefined or reserved address that indicates that the conveying MAC frame does not have a destination Unicast or Multicast address. All 1s are interpreted to be the Broadcast address.

Note that once a SmartBAN network is set up, the MAC address types are mapped onto the simplified MAC addresses in TS 103 325 v.1.2.1.

6.3.2.1 Destination Address field

The Destination Address field depends on the MAC Addressing Mode field as indicated in Table 8.

Table 8—Destination Address field encoding

MAC Addressing Mode field value	Destination Address field description
00	The Destination Address field is set to all 1s (broadcast).
01	The Destination Address field contains the MAC address of either a SC or a node.
10	The Destination Address field contains the MAC address of a bridge device.

11	Not used.

6.3.2.1 Source Address field

The Source Address field contains the Unicast address that identifies the transmitting SC entity of the conveying SC frame.

6.3.2.2 Remote Destination Address field

The Remote Address field depends on the MAC Addressing Mode field.

Table 9— Remote Address field encoding

MAC Addressing Mode field value	Remote Destination Address field description
00	Not used.
01	Not used.
10	The Remote Address field contains the MAC address of a device in a external network.
11	Not used.

6.3.3 Sequence Control field

The Sequence Control field consists of two subfields, the Sequence Number and the Fragment Number.

Table 10—Sequence Control field encoding

Octet	Bits	Field name	Description
0	b0–b3	Fragment number	Indicates the number of each fragment of an SC frame
	b4–b7	Sequence number	Indicates the sequence number of the SC frame
1	b8–b15		

6.3.3.1 Fragment Number field

The Fragment Number field indicates the number of each fragment of a SC frame. The fragment number is set to 0 in the first or only fragment of an SCDU and is incremented by one for each successive fragment of that SCDU. The fragment number remains constant in all retransmissions of the fragment.

6.3.3.2 Sequence Number field

The Sequence Number field indicates the sequence number of the SC frame. The Sequence number field is set to 0 in the first SCDU transmitted and incremented by one for each successive SC frame in a communication session.

Each fragment of an SC frame contains a copy of the sequence number assigned to that SC frame.

6.3.4 QoS Control field

The QoS Control field identifies the Traffic Class (TC) to which the SC frame belongs and other QoS related information about the SC frame that varies by frame type, subtype, and type of transmitting device.

Table 11— QoS Control field encoding

Octet	Bits	Field name	Description
0	b0–b3	Traffic ID	Identify the user priority (UP) and traffic Access Category (AC) of a QoS data frame
	b4	End Of Service	If b4 is set to one, it indicates the end of a service period, and b8–b15 indicates the Queue size (see x)
	b5–b6	ACK Indicator	Indicates the type of ACK
	b7	Aggregate SC frames	If a bridge device is used
1	b8–b15	Group TX Limit	Indicate the GAP granted by the Group Coordinator
	b8–b15	Group TX Requested	GAP request by a Group member for the next Group TX period
	b8-b15	Buffer State	The SC uses this to indicate the buffer state for a given node
	b8–b15	Queue Size	A node uses this to inform its SC how much-buffered traffic it has to send.

NOTE: the use of subfields b8–b15 depends on the transmitting device and subtype frame (see clause x).

6.3.4.1 Traffic ID subfield

The Traffic ID subfield identifies the Traffic Class of the conveying SC frame.

The SC layer defines eight User Priorities (UP) for data traffic. These user priorities aligned with the IEEE 802.1D Std, which is required to define a bridge between SmartBAN networks and external infrastructure networks.

Table 12— User Priority reference

User Priority	IEEE 802.1D designation	Description
7	Network Control (NC)	Time and safety-critical traffic needed to maintain and support the network infrastructure
6	Voice (VO)	Time-critical, characterized by less than 10 ms delay
5	Video (VI)	Time-critical, characterized by less than 100 ms delay
4	Controlled Load (CL)	Non–time-critical but loss-sensitive, such as streaming multimedia or application-critical traffic; are usually used for applications that

		require reservation mechanisms or admission control decisions
3	Excellent Effort (EE)	Non−time-critical but loss-sensitive; for best-effort services delivered to the most important applications
2	Best Effort (BE)	Non−time-critical and loss-insensitive. This is the most common traffic type
1	Spare (−)	
0	Background (BK)	Non-time-critical and loss insensitive, but of lower priority than best effort; includes bulk transfers and other data transfers that are permitted on the network but that should not impact the use of the network by other users and applications

Traffic ID for SmarBAN includes four Access Categories (AC) of data traffic. Those address the data traffic from layers above the SC layer. The AC classification from lowest to highest: Background (AC−BK), Best Effort (AC−BE), Video (AC−VI), and Voice (AC−VO). Each AC has a different priority queue to prioritize SC data frames.

Higher priority packets from layers above the SC layer have a higher priority to be sent because the SC scheduler waits less before sending the higher priority packets, i.e., the contention backoff duration is lower, a shorter contention window, and a longer GAP duration.

Table 13 — Traffic ID subfield encoding

b0−b3	Description
0000−0111	The User Priority value of a SC frame
1000	The AC value of an SC frame is AC−VO
1001	The AC value of an SC frame is AC−VI
1010	The AC value of an SC frame is AC−BE
1011	The AC value of an SC frame is AC−BK
1100−1111	Reserved

The Traffic ID indication for decimal values 8−11 in Table 13 is used by layers above the SC layer to distinguish SC frames for parameterized Quality of Service (QoS) for a particular traffic specification. These Traffic ID values are assigned to SC frames in higher layers.

6.3.4.2 End of Service subfield

The EOS subfield is used by a SC or Group Coordinator to indicate the end of the current service period or Group transmission period when bit b4 is set to one.

6.3.4.3 ACK Indicator subfield

The ACK Indicator subfield identifies the ACK policy upon the delivery of the SC frame.

Table 1— ACK Indicator subfield encoding

b5–b6	ACK policy	Description
00	Normal ACK	The recipient SC entity returns an ACK frame upon receipt of the SC frame, according to the procedures defined in clause x.
01	No ACK	The recipient SC entity takes no action upon receipt of the SC frame.
10	Block ACK	The recipient SC entity takes no action upon the receipt of the SC frame, except for recording its reception state, and waits for a BlockAckReq (block ACK request) to which it responds using the procedure described in clause x.
11	Reserved	

NOTE: The Normal ACK and No ACK indications are passed to the MAC layer in TS 103 325 v.1.2.1.

6.3.4.4 Aggregate SCDU subfield

An aggregated SCDU is present.

6.3.4.5 Group TX Limit subfield

The Group TX Limit subfield indicates the Group Access Period (GAP) granted by the Group Coordinator for a given QoS. If the SC frame is not part of a Group transmission (see clause x), this field is set to all 0s.

6.3.4.6 Group TX Requested subfield

The Group TX Requested subfield indicates the duration, in units of 0.1 msec requested by a group member for the next Group TX period for the specified Traffic ID. If the SC frame is not part of a Group transmission (see clause x), this field is set to all 0s.

6.3.4.7 Buffer State subfield

The Buffer State subfield is used by an SC used to indicate the buffer state for a given node if b8 is set to one. In such case, b9-b10 indicates the AC of the highest priority traffic remaining that is buffered at the coordinator.

6.3.4.8 Queue Size subfield

The Queue Size subfield indicates the amount of buffered traffic for a given Traffic ID at the node sending the SC frame. The Queue Size subfield is present if bit 4 of the QoS Control field is set to 1.

In case of multi SmartBANs operation, the Group Coordinator scheduler may use this information to determine the next Group TX duration assigned to a BAN. The Queue Size subfield is set to the total size, rounded up to the nearest multiple of 256 octets, and expressed in units of 256 octets.

6.3.5 Frame Body field

The Frame Body field is a variable-length field that contains information specific to individual frame types and subtypes. The minimum length of the frame body is 0 octets. The maximum length of the frame body is 2304 octets.

NOTE: It allows the encapsulation of SC frames in sets of 256 octets to layers above the SC layer.

6.3.6 FCS field

The FCS field contains a 32-bit CRC. The FCS field value is calculated over the SC Header and the Frame Body field.

The 32−bit CRC is calculated using the following standard generator polynomial of degree 32:

$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

The FCS field content is obtained by the following:

1) Let $M(x) = b_0 x^{k-1} + b_1 x^{k-2} + \ldots + b_{k-2} x + b_{k-1}$ be a message in polynomial representation consisting of k bits.

2) Multiply $M(x)$ by x^{32}, giving the polynomial $x^{32} \times M(x)$.

3) Divide $x^{32} \times M(x)$ modulo 2 by the generator polynomial $G(x)$ to obtain the remainder polynomial: $R(x) = r_0 x^{31} + r_1 x^{30} + \ldots + r_{30} x + r_{31}$.

4) The FCS field content is given by the coefficients of the remainder polynomial starting with r_0 and finishing with r_{31}.

5) At the receiver, the initial remainder is preset to all 1s.

6.4 SC frame types

6.4.0 General

The standard defines three SC frame types: Data frames, Control frames, and Management frames:

— Data frames transport information from a SC entity to another SC entity or to a Bridge entity.

— Control frames intend to perform clearing operations in the SC entity. To speed up the delivery of data a block ACK frame is added as an alternative to the positive acknowledgment of received data at the MAC level. Control and Data frames work together to deliver data reliably.

— Management frames perform supervisory functions such as association to join a group BAN, or an external network via a bridge or dissociation to leave the group BAN, or external network via a bridge.

6.4.1 Control frames

6.4.1.1 Format of Control frames

Control frames do not contain the Frame Body field. In the description of Control frames, an “immediately previous” frame, refers to a frame whose reception concluded within the Short Interframe Space (SIFS).

6.4.1.2 BlockACK.Request frame format

The format of the BlockACK.Request frame is shown in Figure 6.

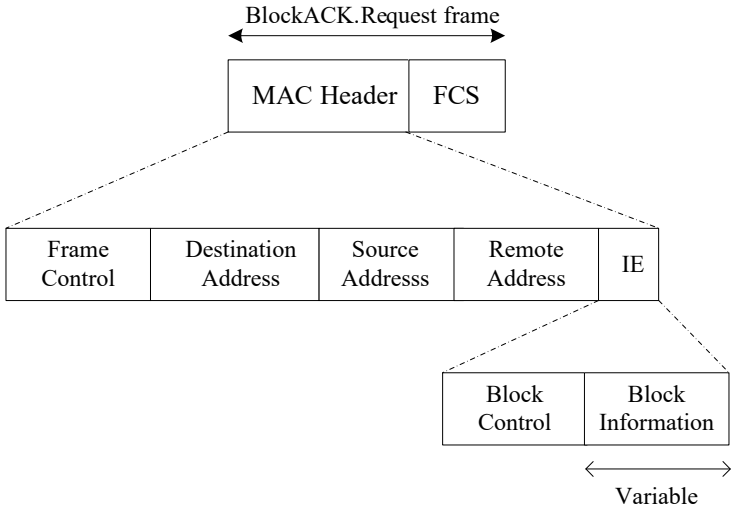


Figure 6 — BlockACK.Request frame format

The Receiver Address field contains the address of the recipient device. The Transmitter Address field holds the address of the device transmitting the BlockACK.Request frame.

6.4.1.2.1 Block Control subfield

Table 14— Block Control subfield

Octet	Bits	Subfield	Description
0	b0	Multi-TrafficID	b1=1, it indicates the data frames to be acknowledged contain a different Traffic ID. Otherwise, b1=0 (all data frames to be acknowledged have the same Traffic ID).
	b1-b4	TrafficID_Info	If b0=0, it contains the Traffic ID for which a BlockACK frame is requested. If b0=1, it indicates the number of Traffic IDs present in the BlockACK.Request frame.

6.4.1.2.2 Block Information subfield if Multi-TrafficID=0

Table 15— Block Information subfield if Multi-TrafficID=0

Octet	Bits	Subfield	Description
0	b0-b3	Fragment Number	Fragment number
	b4-b7	1st Sequence Number	It contains the sequence number of the first SCDU or A-SCDU for which this BlockACK.Request frame is sent.
1	b8-b15		

6.4.1.2.3 Block Information subfield if Multi-TrafficID=1

Table 16 — Block Information subfield if Multi-TrafficID=1

Octet	Bits	Subfield	Description
0	b0-b3	Traffic ID	1st Traffic ID
	b4-b7	Reserved	
1	b8-b11	Fragment Number	Fragment number for 1st Traffic ID
	b12-b15	It contains the sequence number of the first SCDU or A-SCDU for 1st Traffic ID for which this BlockACK.Request frame is sent.	
2	b16-b23		
….			
The 3 octet block repeats for the number of traffic IDs indicated in TrafficID_Info.			

6.4.2 Data frames

6.4.2.1 Data frame format

The format of a Data frame is defined in Figure 7.

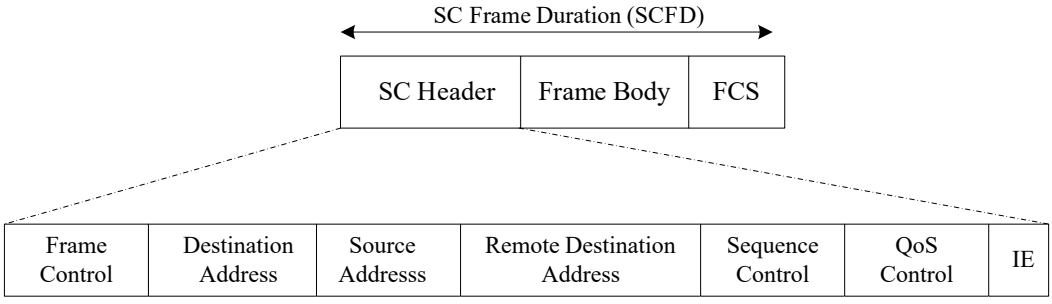


Figure 7 — Data frame format

6.4.2.2 Addresses

Data frames can be exchanged between a SC and a node of the same BAN, or between a SC and another SC, or between a SC and a device in a external network via a bridge at the Link Layer according to the IEEE 802.1D (bridges), IEEE 802.1Q (VLAN) and IEEE 802.1P (priority traffic) standards.

When a Data frame carries an SCDU the Destination Address, Source Address and Remote Address fields are set up depending on the subfields “To Bridge” and “From Bridge” in the Frame Control field according to Table 17.

The Destination Address field contains the MAC address for the destination SC entity of the conveyed SCDU or A-SCDU in the Frame Body field.

An aggregate SCDU (A-SCDU) encapsulates a number of SCDUs (data from higher layers) into one SC frame. This reduces overhead as only one ACK is required. Also, this is designed to speed up communication between a number of nodes in the SmartBAN to an external network via the SC.

The Source Address field contains the MAC address of the SC entity that initiated the transmission of conveyed SCDU or A-SCDU in the Frame Body field.

A device uses the content of the Source Address field to send the acknowledgment if an ACK is requested.

NOTE: higher layer protocols resolve the MAC addresses for the SC Layer. The SC Layer maps the MAC addresses onto the simplified MAC addresses in TS 103 325 v.1.2.1.

Table 17 — Address fields content

From Bridge	To Bridge	Destination Address	Source Address	Remote Address
0	0	15.6ma NIC	15.6ma NIC	Reserved
0	1	Remote DA NIC	15.6ma NIC	Bridge NIC
1	0	15.6ma NIC	Remote SA NIC	Bridge NIC
1	1	Reserved	Reserved	Reserved

NIC: Network Interface Controller. DA: Destination Address. SA: Source Address.

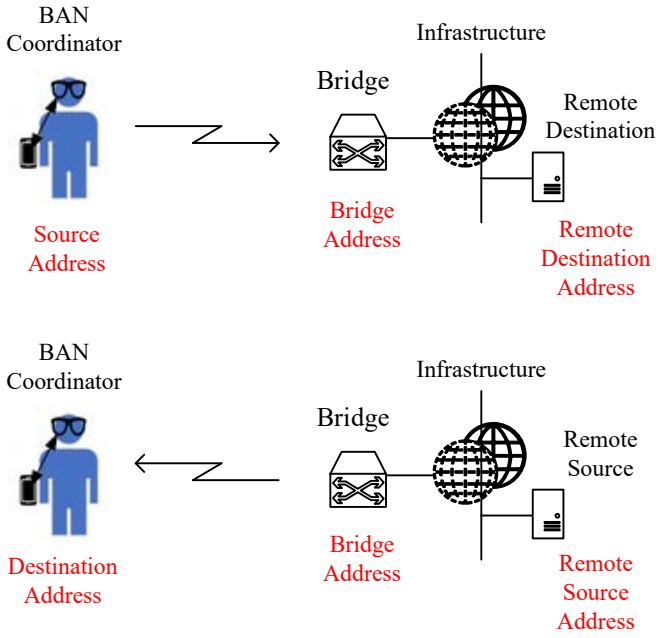
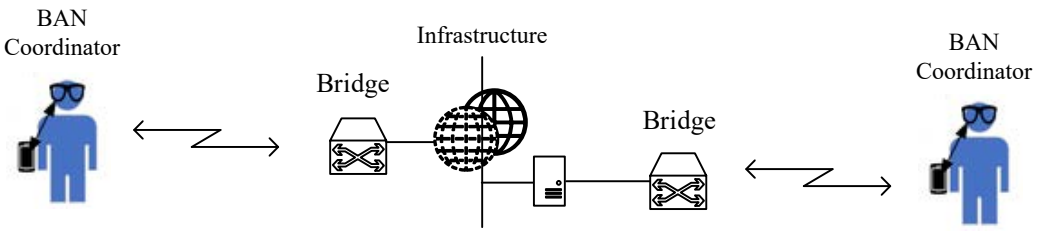


Figure 8 — Illustration of SC addressing fields for SmartBAN external access.



To be discussed:

6.4.2.3 Other MAC Header fields

The Sequence Control field is defined in 6.3.3.

The QoS Control field is defined in 6.3.4. The presence of the QoS Control field is indicated in the Frame Control field[1].

6.4.2.4 Frame Body field

The frame body consists of either the SCDU or A-SCDU after any encapsulation for security. The presence of an A-MSDU is indicated in the QoS Control field.

For Data frames of subtype Null, the Frame Body field is null.

The maximum length of the Frame Body field can be found from the maximum SCDU length plus any overhead from encapsulation for encryption.

6.4.3 Management frames

6.4.3.1 Format of Management Frames

The format of a management frame is defined in Figure 9.

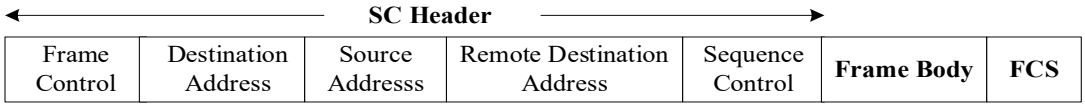


Figure 9 — Management frame format

6.4.3.2 Discovery Frame Body format

The Frame Body of a Discovery frame contains the information shown in Table 18.

Table 18 — Discovery Frame Body encoding

Octet	Field name	Description
0–7	Timestamp	This field represents the timing synchronization function (TSF) timer of the conveying MAC frame.
8–9	Discovery Interval	It represents the number of time units (TUs) between target Discovery frame transmission times.

[1] QoS is consired an optional feature due to legacy considerations of already deployed systems without QoS.

16	BAN ID	See 6.4.3.2.1
17	Capability information	See 6.4.3.2.2

6.4.3.2.1 The BAN ID subfield

The BAN ID consists of the first 16 octets of the output of the Secure Hash Algorithm 3 (SHA3) with 224-bit output[2]. The input to SHA3 is the first timestamp concatenated with the hub's 48-bit MAC address.

6.4.3.2.2 Capability Information subfield

Table 19 — Capability Information subfield encoding

Bits	Capability Information	Description
b136	Group Coordinator	The device is a group coordinator.
b137	QoS	The device has QoS capabilities
b138	Spectrum* Measurements	Spectrum measurements enable. TBD
b139	Link* Measurements	Link measurements enable. TBD
b140	Traffic Indication Map**	Traffic Indication Map is present.
b141–b143	Reserved	

* Spectrum Measurements and Link Measurements measure channel qualities and radio performance. It enables a BAN or Group BAN to learn the wireless environment and use wireless resources such as spectrum, power, and bandwidth more effectively.

** The Traffic Indication Map identifies the devices for which traffic is pending and buffered in the hub.

6.4.3.3 Disassociation frame body format

The Disassociation frame body contains the information shown in Table 20.

Table 20 — Disassociation Frame body

Octet	Description
1	Reason Code

[2] SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.

The Reason Code indicates the reason for the generation of an unsolicited Dissociation frame.

Table 2—Reason code encoding

Value	Description
0	Reserved.
1	Unspecified reason.
2	Invalid authentication: Previous authentication is no longer valid.
3	Leaving network: The sending device is leaving (or has left) the SmartBAN
4	Leaving group: The sending coordinator is leaving (or has left) the Group BAN
5	Inactivity: Disassociated due to inactivity
6	SmartBAN at capacity: Disassociated because the SC is unable to handle more devices
7	Group at capacity: Disassociated because the group coordinator is unable to handle more SmartBANs.
8	Not authenticated: Device requesting (re)association is not authenticated with responding SC
9	Not enough bandwidth: Disassociated because SC lacks sufficient bandwidth for this QoS.
10	Missing ACKs: Disassociated because an excessive number of frames need to be acknowledged, but are not acknowledged due to SC activity and/or poor channel conditions.
11	Exceeded GTX: Disassociated because the group member is transmitting outside the limits of its Group allocation period.
12	Timeout: Requested from device due to timeout.
13-256	Reserved

NOTE: The deauthentication frame has the same frame format.

TBD disassociation due to security failures.

6.4.3.4 Association Request body frame format

The Association frame body contains the information shown in Table 21.

Table 21 — Association Request body frame encoding

Octet	Bits	Field name	Description
0–1		Capability Information	Capability information of device requesting association (See)
2–18		BAN ID	Requesting association to BAN identified with BAN ID

		Supported rates	Supported rates of device requesting association, according to PHY MIB (See Annex X)
		QoS capability I (coordinator)	The subfield is present (see Table 24) if QoSOption1Implemented in MIB is true. Otherwise, absent.
		QoS capability II (non-coordinator)	The subfield is present (see Table 25) if QoSOption2IImplemented in MIB is true. Otherwise, absent.
		Supported Channels	List of supported channels of device requesting association (see x)
		Cipher Suite Capability	TBD
		Public Key	TBD
		Key Session	TBD

A SC requests association with another SC entity or a device in an external network.

Table 22— QoS Capability I field

Octet	Bits	Field name	Description
0	b0-b3	Update count	Incremented by one every time there is a change in QoS during a session.
	b4	Queue request	
	b5	GTX request	
	b6-b7	Reserved	

Table 23— QoS Capability II field

Octet	Bits	Field name	Description
0	b0	AC_VO Flag	It is set to 1 in [Re]Association Request frames to indicate the type of traffic AC_VO generated by a node or bridge. Otherwise, it is set to 0.
	b1	AC_VI Flag	It is set to 1 in [Re]Association Request frames to indicate the type of traffic AC_VI generated by a node or bridge. Otherwise, it is set to 0.
	b2	AC_BK Flag	It is set to 1 in [Re]Association Request frames to indicate the type of traffic AC_BK generated by a node or bridge. Otherwise, it is set to 0.

	b3	AC_BE Flag	It is set to 1 in [Re]Association Request frames to indicate the type of traffic AC_BE generated by a node or bridge. Otherwise, it is set to 0.
	b4-b5	Max Buffer	It indicates the maximum number of buffered MSDUs the node is prepared to receive during any session triggered by the node (see x)
	b6	More ACK	A node can process ACK frames with the More Data bit in the Frame Control field equal to 1 and remains in the awake state. Otherwise, it is set to 0.
	b7	Reserved	

The type of traffic (AC_VO, AC_VI, AC_BK, AC_BE) is used by a coordinator to associate such AC with the node. Also, it indicates the type of traffic (AC_VO, AC_VI, AC_BK, AC_BE) is trigger-enabled AC and delivery-enabled AC.

NOTE: Delivery-enabled AC enables the coordinator to deliver data from such AC to a node or bridge triggered or requested by the node or bridge.

NOTE: Trigger-enabled AC enables a Data frame from a node or bridge to trigger a session with such AC if one is not in progress.

Table 24—Max Buffer subfield

b4–b5	Description
00	The node is prepared to receive all buffered MSDUs.
01	The node is prepared to receive a maximum of two MSDUs per session
10	The node is prepared to receive a maximum of four MSDUs per session.
11	The node is prepared to receive a maximum of six MSDUs per session.

Table 25— Supported Channels field

Octet	Bits	Field name	Description
0	b0–b1	Channelization Plan	Frequency band channelization (see Annex x)
	b2–b7	The supported channel number from the channelization plan is indicated as *i*–2 if bit b_i is set to 1 for *i*=2,3,..,15. Otherwise, it is set to 0. For example if bit b2=1, then the channel number 0 (2–2) is supported by Channelization Plan Annex x.	
1	b8–b15		

Table 26 — Channelization Plan subfield

b0–b1	Description

00	Frequency band channelization 1 (See Annex x)
01	Frequency band channelization 2 (See Annex x)
10	Reserved.
11	Reserved.

6.4.3.5 Association Response Frame Format

The Association frame body contains the information shown in Table 27.

Table 27— Association Response body frame encoding

Octet	Bits	Field name	Description
0–1		Capability Information	Capability information of device requesting association (See 6.4.3.2.2)
2–18		Device ID	Assigned ID to the device (node SC, or bridge).
		Supported rates	Supported rates by the coordinator (see MIB)
		QoS Map	The subfield is present (see Table 31) if QoSMapActiveted in MIB is true. Otherwise, absent.
		Supported Channels	List of supported channels of device requesting association (see Annex x)
		Cipher Suite Configuration	TBD
		Public Key or Digital Certificate	TBD
		Key Session	TBD

6.4.3.5.1 QoS Map subfield

The QoS Map field is transmitted from a coordinator to a node in a (Re)Association Response frame to provide the mapping of higher layer QoS constructs to User Priorities (UPs) to be used for transmission of Data frames. The QoS Map field maps the higher layer priority from the Differentiated Services Codepoint (DSCP) field used with the Internet Protocol onto User Priority as defined by this standard. The QoS Map field is shown in Table 28.

The DSCP List field contains zero or more DSCP subfields (see Table 28) with a maximum value of 10.

Table 28—QoS Map field

Number of Octets	Subfield	Description
1	N	List length
2	DSCP_1	See Table 29
	…	
2	DSCP_N	
2	UP0_2_DSCP	
2	UP_1_DSCP	
2	UP_2_DSCP	
2	UP_3_DSCP	
2	UP_4_DSCP	
2	UP_5_DSCP	
2	UP_6_DSCP	
2	UP_7_DSCP	

Table 29 — DSCP_n subfield

Number of Octets	Subfield	Description
1	DSCP Value	The DSCP value is in the range 0 to 63, or 255
1	UP	The UP value is in the range 0 to 7

When a node begins transmission of a Data frame containing the Internet Protocol, it matches the DSCP field in the IP header to the corresponding DSCP value contained in this field.

The node attempts to match the DSCP value to a DSCP_n subfield. If successful, it uses the corresponding UP value (Table 28). If unsuccessful, the node attempts to match the DSCP value of the UP*m*_2_DSCP subfield and uses *m* as the UP if successful; otherwise uses a UP of 0.

The DSCP value is between 0 and 63, or 255.

<<

Information to be moved to the SC Functional Description. Presented here for discussion.

Packets and frames of different networks have types have different priorities. For example, SC frames carry UP or DSCP priorities, VLAN frames on wired networks carry 802.1p priorities[3], and IP packets carry DSCP priorities[4]. The SC and other network devices must configure priority mapping to retain the priorities of frames or packets that traverse different networks.

Figure 10 illustrates an example of priority mapping between SC frames, and VLAN frames over Ethernet and IP packets in the upstream direction. The SC performs priority mapping of SC frames as follows:

a) Maps the UP or DSCP priority of SC frames to the DSCP or 802.1p priority of tunnel packets[5].
b) Maps the user priority of SC frames to the DSCP or 802.1p priority of Ethernet packets.
c) Maps the DSCP priority of SC frames to the DSCP priority of Ethernet packets.

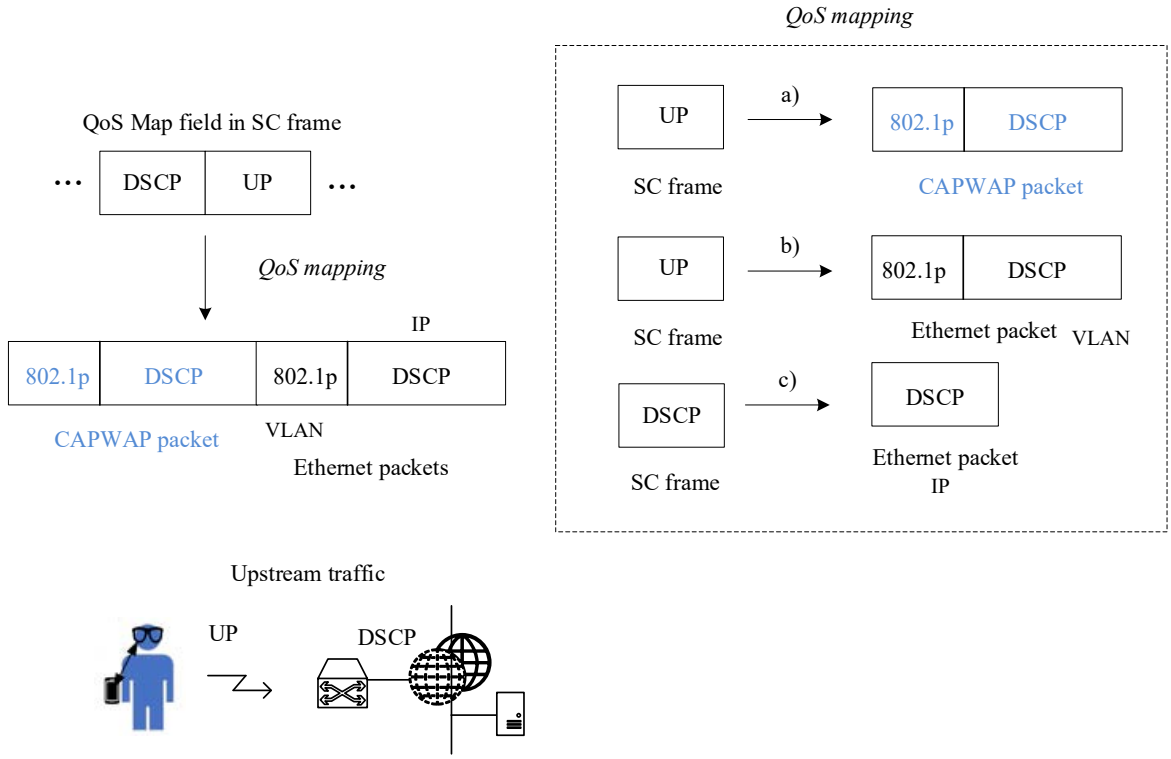


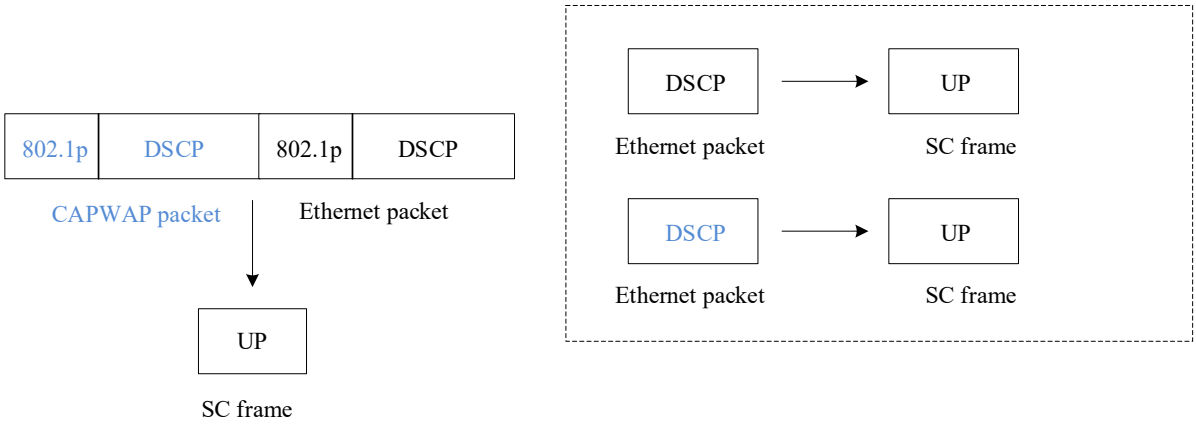
Figure 10 — Upstream

In the downstream direction, the bridge forwards Ethernet packets from the Internet to the SC directly or through a tunnel. The SC maps the DSCP priority of the Ethernet packets to the user priority of SC frames.

[3] The IEEE 802.1p Std defines the priority of VLAN frames.

[4] DSCP priority determines the priority of packets based on the ToS (Type of Service) field in their IP header.

[5] CAPWAP (Control and Provisioning of Wireless Access Points) is a protocol that enables an access controller to manage a collection of wireless termination points



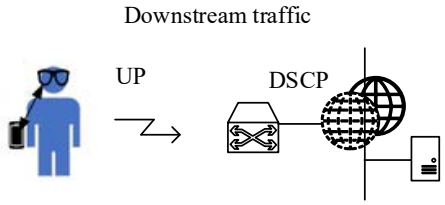


Figure 11— Downstream

---

7 Smart Coordinator Service Definition

7.1 Overview of SC services

7.1.1 Data service

7.1.1.1 General

The SC data service provides the ability to exchange MSDUs per LLC sublayer entities or IEEE 802.1Q bridge ports. To support this service, the local SC uses the underlying PHY-level services to transport an MSDU to a peer SC entity, where it is delivered to the corresponding LLC sublayer or bridge port.

The MSDU transport is on a best-effort basis by default. However, the QoS facility uses a traffic identifier (TID) to specify differentiated services on a per-MSDU basis.

Group-addressed transport is part of the data service provided by the SC. Due to the characteristics of group communication, group-addressed MSDUs might experience a lower QoS, compared to that of individually addressed MSDUs.

All SCs differentiate their MSDU delivery according to the designated traffic category of individual MSDUs. The access category of each MPDU is designated by the current QoS policy.

The SC uses a set of rules that tends to cause higher UP MSDUs to be sent before lower UP MSDUs. The SC sublayer entities determine the UPs for MSDUs based on the TID values provided with those MSDUs.

7.1.1.2 Determination of UP

Complying devices support QoS with eight priority values, referred to as User Priorities (UPs). The values of a UP are intergers from 0 to 7 and are identical to the IEEE 802.1D™ priority tags.

An MSDU with a particular UP is said to belong to a traffic category (TC) with that UP. The UP is provided with each MSDU at the medium access control service access point (MAC SAP) in the UP parameter.

For the transmission of an MSDU that was provided to the Internal Sublayer Service (ISS) SAP, the UP is determined by the convergence function based on the priority parameter of the UNITDATA.request primitive (recommended mappings depend on targeted use cases).

7.1.1.3 Security services

The scope of the security services is limited to hub-to-device for secured frame transmissions. The security services are provided by the MAC layer as shown in the reference model, Figure X, as follows:

a) Data confidentiality and integrity;
b) Authentication;
c) Access control.

During the authentication exchange, both parties exchange authentication information as described in clause 8. The security services rely on information from non-SC management or system entities. Such management entities communicate through a set of SC layer management entity (MLME) interfaces and the SC Information Base (SCIB) attributes.

7.1.2 MSDU ordering

The services provided by the SC support the reordering of MSDUs. However, the SC does not intentionally reorder MSDUs except when is necessary to improve the likelihood of successful delivery based on the current operational mode. The MSDUs are reordered to improve the likelihood of successful delivery based on the current operational mode of the designated recipient device and to fulfill the priority parameters specified in the UNITDATA.request primitive of the individual MSDUs.

The effects of this reordering for the set of MSDUs received at the SC service interface of any device are:

a) A change in the delivery order of group-addressed MSDUs, relative to individually addressed MSDUs originating from a single source device address

b) The reordering of MSDUs with different Traffic ID (TID) values originating from a single source address.

c) There shall be no reordering of individually addressed MSDUs with the same TID value and addressed to the same destination.

d) The SC shall meet the MSDU reordering requirements of IEEE Std 802.1AC-2016.

e) If MSDUs are reordered, the recipients shall reorder the MSDUs such that the integrity of the information is maintained.

7.1.3 MSDU format

Logical Link Control (LLC) sublayer entities use the SC sublayer service to exchange MSDUs with other LLC sublayer entities. The standard uses the Ethertype Protocol Discrimination (EPD) to differenciate the next higher protocol delivering or receiving MSDUs from the SC.

7.1.4 SC service interface role

The SC service interface performs destination-address filtering, access to the convergence function, and, access to the bridge ports if enabled as shown in Figure 12.

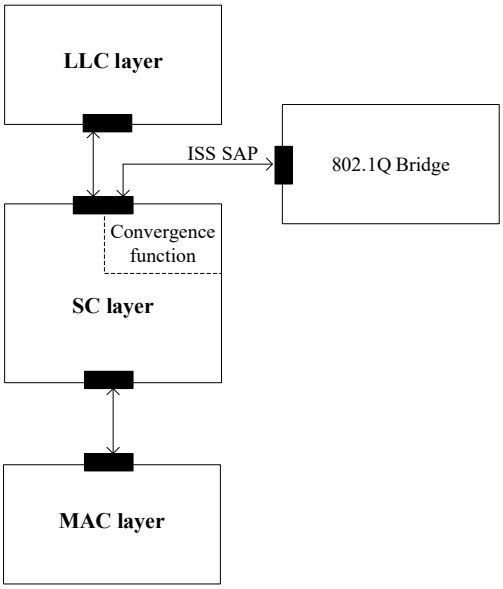


Figure 12—Reference model of the SC Convergence Function.

7.1.5 Provision of the SC service

The SC service supports delivery services of MSDUs in an IEEE Std 802.1Q network via the convergence function to provide access to the wireless medium using a ISS SAPs.

The SC can give access to the wireless medium to an IEEE 802.1Q network. Figure 2 shows an example involving a SC and other generic IEEE 802 Local Area Network (LAN) or Wide Area Network (WAN).

The SC provides services mapped onto one or more ISS SAPs by the Convergence Function. Each Internal Sublayer Service SAP is then mapped onto an Enhanced Internal Sublayer Service (EISS) SAP by the IEEE 802.1Q Media Independent Function. The EISS SAP provides EISS services to the relay entity of a VLAN bridge component (IEEE 802.1Q MAC Relay Entity).

SmartBAN specifications do not specify the details of IEEE 802.1Q Media Independent Function, the ISS SAP function, the IEEE 802.1Q MAC Relay Entity, and the LLC layer. These entities are specified in other documents (refer to the Bibliography clause for more information). These entities are shown with dashed outlines in Figure 13. Entities specified by the SC are shown with solid outlines.

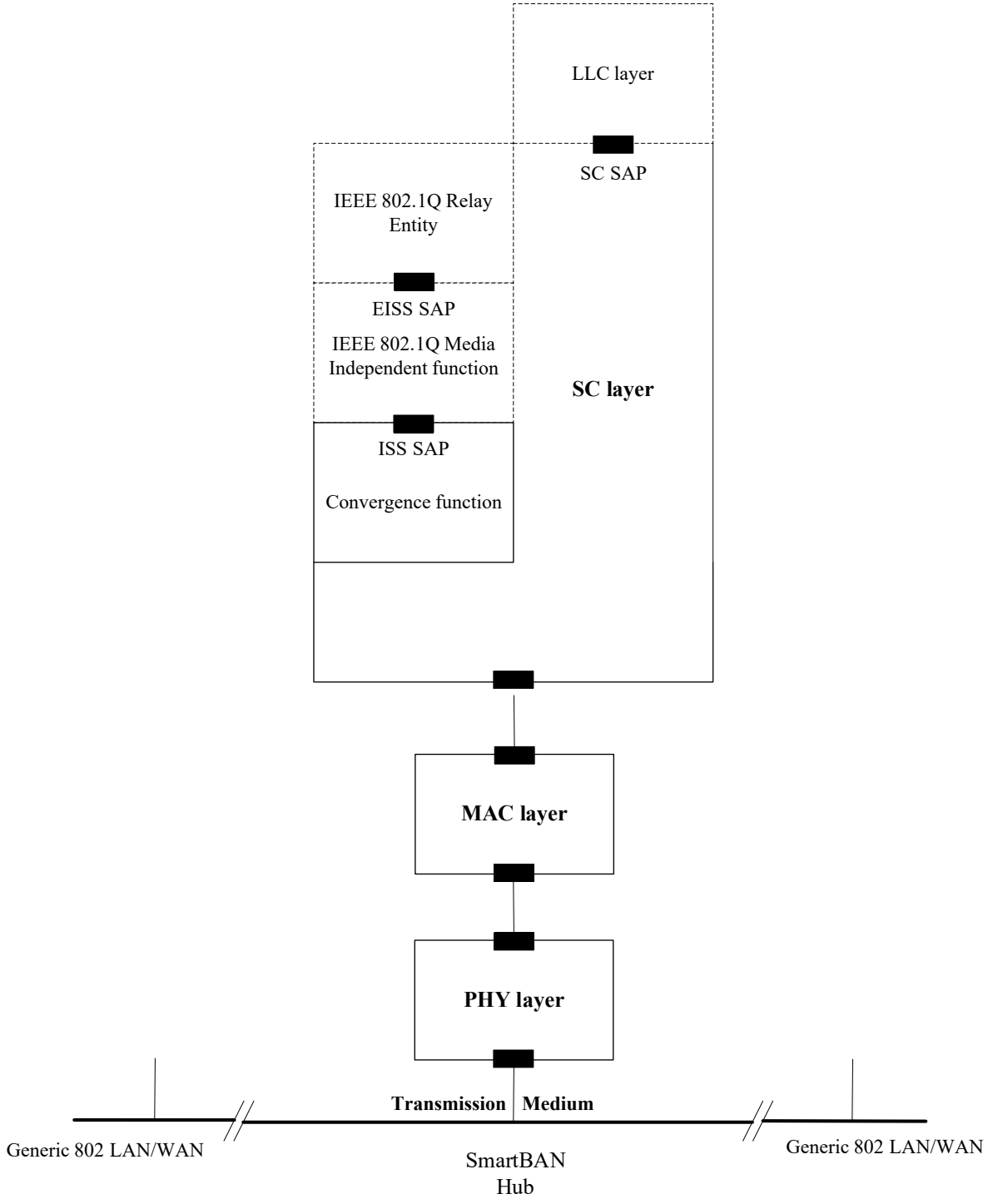


Figure 13—Example of bridging SmartBAN with IEEE 802 Stds.

7.2 SC data service architecture

The SC data plane architecture (i.e., processes that involve transport of all or part of an MSDU) is shown in Figure 14.

During transmission, an MSDU goes through the processes shown in the left-hand side of Figure 14. During reception, a received Data frame goes through the processes shown in the right-hand side of Figure 14. Then, MSDUs are delivered to the SC SAP or to an IEEE 802.1Q bridge port if Bridge functionality is present.

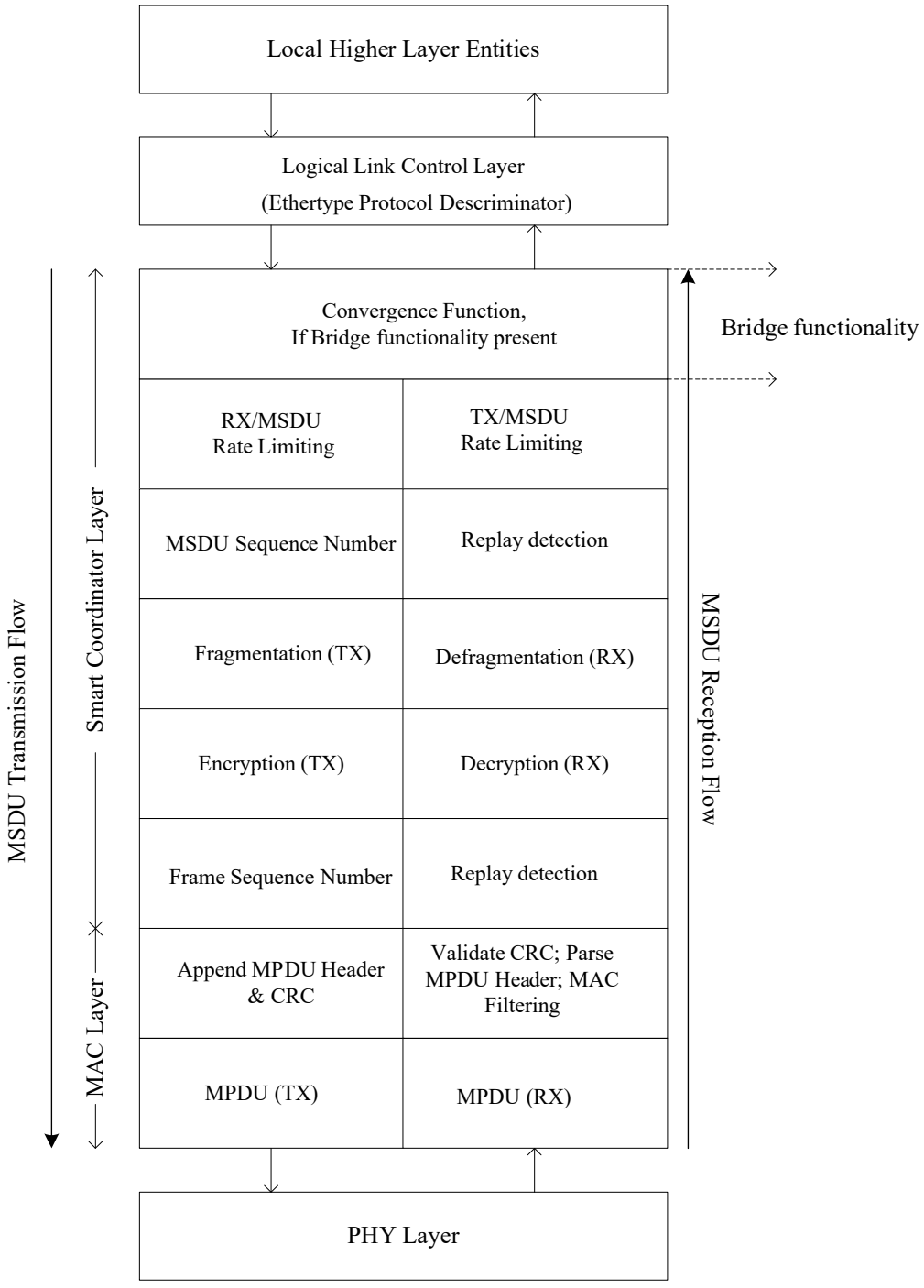


Figure 14—Smart Coordinator data architecture.

7.3 Smart Coordinator data service specification

7.3.1 General

The SC supports the following service primitives:

a) UNITDATA.request
b) UNITDATA.indication
c) UNITDATA-STATUS.indication

Each UNITDATA.indication primitive corresponds to the receipt of an error-free MSDU from the wireless medium. The UNITDATA.request primitive is invoked to transmit a MSDU to the wireless medium.

Those provide the elements necessary for the performance of data transfer between the SC SAP and the provision of MAC relay (bridging) in IEEE 802.1Q Bridges.

7.3.2 UNITDATA.request

7.3.2.1 Function

The primitive requests a transfer of an MSDU from the local LLC entity to another LLC entity, or multiple peer LLC entities (in the case of group addresses) or bridge port.

7.3.2.2 Semantics of the service primitive

The parameters of the primitive are as follows:

```
UNITDATA.request(
   source address,
   destination address,
   routing information,
   data,
   priority,
   drop eligible,
   service class
)
```

The *source address* (SA) parameter specifies the MAC address of the entity transmitting the MSDU.

The *destination address* (DA) parameter specifies either an individual MAC address (unicast) or a group MAC address (multicast) receiving an MSDU.

The *routing information* parameter specifies the route for the data transfer (a null value indicates source routing is not used). For SmarBAN implementations, the *routing* parameter shall be null.

The *data* parameter specifies the MSDU transmitted by the SC entity. [The length of the MSDU shall be less than or equal to the value shown in Table x.]

The *priority* parameter specifies the requested priority of the *data* to transfer. The allowed values of priority are described in X.

NOTE—For a bridge, the bridge port provides the priority. That priority might have been derived from a priority tag in the frame arriving on another port of the bridge or from the configuration of that port if the frame arrived untagged.

The *drop eligible* parameter if TRUE indicates weather the MSDU can be discarded in preference to other MSDUs for which the *drop eligible* is FALSE, when there are insufficient resources in the coordinator.

The *service class* parameter specifies the requested service class of the *data* to transfer. The allowed values of service class are described in X.

7.3.2.3 When generated

The LLC entity generates the primitive when an MSDU is to be transferred to a peer LLC entity or entities or to a peer bridge or bridges.

7.3.2.4 Effect of receipt

On receipt of this primitive, the SC entity determines whether it can fulfill the request according to the requested parameters.

A request that cannot be fulfilled according to the requested parameters is indicated to the LLC entity using the UNITDATASTATUS.indication primitive that describes why the SC entity was unable to fulfill the request.

If the request can be fulfilled under the requested parameters and according to the current state of the SmartBAN, the SC entity properly formats a frame and passes it to the PHY layer via the MAC layer for transfer to a peer SC entity or entities, and indicates this action to the LLC entity or bridge port using the UNITDATASTATUS. indication primitive with transmission status set to SUCCESFUL.

7.3.3 MA-UNITDATA.indication

7.3.3.1 Function

The primitive defines the transfer of an MSDU from the SC entity to the LLC entity or bridge port, or entities or bridge ports in the case of group addresses. In the absence of error, the contents of the data parameter are logically complete and unchanged relative to the data parameter in the associated UNITDATA.request primitive.

7.3.3.2 Semantics of the service primitive

The parameters of the primitive are as follows:

```
UNITDATA.indication(
   source address,
   destination address,
   routing information,
   data,
   reception status,
   priority,
   drop eligible,
   service class
)
```

The *source address* parameter is the MAC address specified by the SA field of the incoming MAC frame.

The *destination address* parameter is either a MAC address or a group address as specified by the DA field of the incoming MAC frame.

The *routing information* parameter specifies the route that was used for the data transfer. The SC entity shall set this field to null.

The *data* parameter indicates the MSDU received by the SCC entity, or data transfer.

The *reception status* parameter is set to SUCESSS (all failures of reception are discarded by the SC entity and consequently without generating the UNITDATA.indication primitive).

The *priority* parameter specifies the receive processing priority that was used for the data transfer.

The *drop eligible* indicates whether the received MSDU was designated as drop eligible indicated in the control field of the incoming MAC frame.

The *service class* parameter specifies the receive service class that was used for the data transfer.

7.3.3.3 When generated

The SC entity carries the UNITDATA.indication primitive to the LLC entity (entities, bridge port or bridge ports) to indicate the arrival of a frame at the local SC sublayer entity. Frames are reported only if they are validly formatted at the MAC sublayer, received without error, received with valid (or null) security and integrity information, and their destination address designates the local MAC sublayer entity.

7.3.3.4 Effect of receipt

The effect of receipt of this primitive by the LLC layer or bridge port is dependent on the content of the MSDU.

7.3.4 UNITDATA-STATUS.indication

7.3.4.1 Function

This primitive provides status information to the local LLC layer from a preceding UNITDATA.request primitive.

7.3.4.2 Semantics of the service primitive

The semantics of the primitive are as follows:

```
MA-UNITDATA-STATUS.indication (
   source address,
   destination address,
   transmission status,
   provided user priority,
   provided service class
)
```

The *source address* parameter is a MAC address, as specified in the associated UNITDATA.request primitive.

The *destination address* is a MAC address, as specified in the associated UNITDATA.request primitive.

The *transmission status* parameter is used to pass status information back to the local requesting LLC layer entity. IEEE Std 802.15.3 specifies the following values for TransmissionStatus when delivery of the MSDU is attempted:

The *transmission status* parameter indicates the status information to the local requesting LLC layer entity or bridge port. SmartBAN specifies the following values for *transmission status*:

a) Successful.

b) Undeliverable (excessive data length).

c) Undeliverable (non-null source routing).

d) Undeliverable (unsupported user priority).

e) Undeliverable (unsupported service class).

f) Undeliverable (no SmarBAN hub available).

g) Undeliverable (cannot encrypt with a null key).

If the *transmission status* parameter is Successful, the *provided user priority* parameter specifies the user priority used for the associated *data* unit transfer from the preceding UNITDATA.request primitive. Otherwise, the *provided user priority* parameter is not present.

If the *transmission status* parameter is Successful, the *provided service class* parameter specifies the class of service used for the associated *data* unit transfer from the preceding UNITDATA.request primitive. Otherwise, the *provided service class* parameter is not present.

7.3.4.4 When generated

The UNITDATA-STATUS.indication primitive is passed from the SC entity to the LLC entity or bridge port to indicate the status of the service provided for the corresponding UNITDATA.request primitive.

7.3.4.5 Effect of receipt

The effect of receipt of this primitive by the LLC entity or bridge port depends upon the type of operation employed by the LLC entity or bridge port.

8 Cybersecurity protocol

8.1 General

BANs are expected to play a key role by personalizing medical and non-medical applications. In the case of medical applications people can check healthcare-related indicators which enable continuous measure critical biomarkers for medical diagnostics, physiological health monitoring, fitness, and configuration of wearables (on-body devices) and medical implants (in-body devices).

Medical devices have evolved thanks to the development of electronics, biocompatible materials, and nanomaterials as accessories, integrated clothing, body attachments, and more specialized such as pacemakers, insulin pumps, or neurostimulators, which enable the monitoring of vital signals within the contexts of wearable and implanted sensors and systems developed specifically for monitoring health and fitness metrics. Another important emerging application is personalized medicine for a variety of chronic and acute diseases. BANs enable point-of-care at home providing rapid and patient-centered diagnostics and treatment.

The control and management of wearables and medical implants in BANs are done wirelessly. If such wireless links lack any cybersecurity mechanism, an intruder can perform passive and active attacks. The issue is more sensitive in an active attack as it can counterfeit commands to wearables or medical implants.

Due to the limited computational resources of BAN devices and the fact that the operation of BANs is self-contained with limited access to infrastructure, conventional cryptographic solutions cannot be applied directly. Indeed, some cryptographic functions may require access to a Public Key Infrastructure (PKI) as a trusted third party for authentication of devices to take part in secure BAN sessions.

Assuming lightweight crypto like stream-ciphers or the recent family of ciphers Ascon (authenticated encryption and hashing), and Elliptic Curve Cryptography (ECC) for relatively small key size and high security, still some cryptographic functions (generation of nonces, digital signatures, pseudorandom functions, etc.) and key management (generation, exchange, storage, use, destruction, replacement of keys and handling of security protocols) represent a significant increment of processing and power consumption for BANs.

Hence, the security protocols and primitives are mostly delegated to a personal device. Indeed, due to the proliferation of personal devices such as smartphones or tablets equipped with a modern operating system with state-of-the-art software and hardware to handle state-of-the-art cryptography and access to infrastructure via Wi-Fi or 5G, and 6G networks. We propose to use a personal device with a Key Management app to bootstrap cryptographic functions, key management, and secure storage per device and logs in a BAN.

In that manner, devices (wearables and medical implants) and smartBAN coordinators only need to implement a lightweight cipher. Moreover, a SmartBAN can work standalone without constant access to the Key management app.

The proposed use of a Key Management app in a personal device is for the first and one-time authentication of devices to participate in a BAN as it requires an authenticated channel via a PKI to support security guarantees []. Once the registration is done, the authenticated channel is no longer needed, and the Key Management app is used for support or configuration changes.

Afterward, an Authenticated Key Exchange (AKE) protocol generates the session key for unicast sessions. There are many AKE protocols in the literature. The specification uses a variation of the OPAQUE protocol [], an asymmetric password-authenticated key exchange (aPAKE) that supports mutual authentication in a client-server setting without reliance on a PKI and with security against pre-computation attacks upon server compromise.

In the BAN, the client is a wearable or medical implant, and the server may be either the Key Management app (during first registration) or the SmartBAN coordinator. The proposed protocol is a combination of two cryptographic protocols: Oblivious Pseudo-Random Function (OPRF) and aPAKE.

The aPAKE protocol is well suited for BAN networks because BANs are designed to work as self-contained networks with limited access to infrastructure. That is, secure connections in a BAN should not depend on always access to a PKI. The OPRF protocol protects against vulnerabilities of the aPAKE if the server is compromised and transforms a low-entropy password into a high-entropy secret for the AKE protocol.

The proposed security protocol for BAN networks consists of two phases: registration of credentials for wearables, medical implants, key management app, and SmartBAN coordinator; and logging in a BAN communication session via an authenticated key exchange protocol to derive the session key.

8.2 Cybersecurity set up

8.2.1 Introduction

The concept of cybersecurity of the SmartBAN coordinator is shown in Figure 12.

Figure 15—Cybersecurity system concept for SmartBAN coordinator.

The cybersecurity system consists of three main blocks:

— The first block is a SmartBAN equipped with the SmartBAN Coordinator. The coordinator handles the key management for confidentiality and integrity of messages in SmartBAN wireless links (authenticated encryption and verification of digital signatures) and a bridge interface to the Key management app (bridge link).

— The second block is the Key Management app installed in a personal device (smartphone or tablet) that is used for support of an *authenticated channel* for the first registration of wearables and medical implants via infrastructure such as 5G, 6G networks, or Wi-Fi. Also, the Key Management app may support the configuration of wearables or medical implants as well as the required key management such as generation, refreshment of keys, nonces, and pseudo-random functions among others, and secure storage of credentials for wearables, medical implants, and cryptographic material required by the proposed security protocol. In that manner, the SmartBAN stays as simple as possible by delegating cybersecurity tasks to the Key Management app. The SmartBAN coordinator supports a communication bridge to the Key Management app.

— The third block stands for a mutually authenticated protected channel (*authenticated channel* for short) from the SmartBAN to the Manufacturer's repository for verification of public keys and identities (device's serial number) for wearables and medical implants using the Key Management app and via Transport Layer Security (TLS) links to the Manufacturer's repository. This is a one-step process for the first registration of wearables and medical implants that requires an authenticated channel to set up the security guarantees that such devices are legit as well as their long-term public keys (identity keys). Once the registration phase is done, the authenticated channel is no longer needed anymore, and devices (wearables and medical implants) can log in securely into a BAN any number of times even after an outage or switch off.

Due to the limited power consumption and processing capabilities of wearables and special medical implants, conventional cybersecurity protocols based on digital certificates for mutual authentication may not be the best choice. Moreover, access to a PKI may not always be available in a BAN, yet the secure communication links in a BAN must be available. Hence, the proposed protocol assumes access to a PKI only for mutual authentication of devices (wearables and medical implants) used for the first time to the manufacturer’s repository (and so to the SmartBAN coordinator and Key Management app).

Indeed, the proposed protocol assumes that mutual authentication is only needed the first time a device, either a wearable or medical implant joins a BAN, known as registration. After successful registration, the cryptographic credentials of the devices, manufacturer's repository, Key Management app, and SmartBAN coordinator were authenticated and stored securely. In the second phase, devices can join or log in to a BAN many times without an *authenticated channel*. A consequence of the proposed protocol is that it does not require digital certificates, which is helpful to the limited resources of wearables and medical implants.

8.2.2 Credentials of wearables and medical implants

BAN devices (wearables and medical implants) have embedded a QR code and a set of asymmetric keys installed from fabrication. Indeed, the bundle keys installed during manufacturing on a medical implant or wearable device are given in Table 30 and Table 31 using ECC with Curve25519 and Ed25519 for digital signatures. Similarly, the bundle keys of the

Key Management App installed by default are given in Table 32. Encode(.) is a function that transforms a finite field element into a string of octets.

Table 30—Implant's keys installed during manufacturing.

Item	Description
$Priv_{IK.impl}, Pub_{IK.impl}$	Implant's Private and Public Identity Keys.
$Priv_{SPK.impl}, Pub_{SPK.impl}$	Implant's Private and Public Signed Pre-Keys.
$\sigma_{SPK,impl}$	Signature of $\text{Encode}\left(Pub_{SPK,impl}\right)$

Table 31—Wearable keys installed during manufacturing.

Item	Description
$Priv_{IK,wear}, Pub_{IK,wear}$	Wearable's Private and Public Identity Keys.
$Priv_{SPK.wear}, Pub_{SPK.wear}$	Wearable's Private and Public Signed Pre-Keys.
$\sigma_{SPK,wear}$	Signature of $\text{Encode}\left(Pub_{SPK,wear}\right)$

Table 32—Key Management App keys installed by default.

Item	Description
$Priv_{IK.app}, Pub_{IK.app}$	Key Management App's Private and Public Identity Keys.
$Priv_{SPK.app}, Pub_{SPK.app}$	Key Management App's Private and Public Signed Pre-Keys.
$\sigma_{SPK,app}$	Signature of $\text{Encode}\left(Pub_{SPK,app}\right)$

NOTE— The security protocol does not require public keys to be publicly available. They are not publicly available.

The QR code holds a web link to the Manufacturer's repository and a short, encrypted message c_1. The encryption cipher used the manufacturer's Public Identity Key $(Pub_{IK,manf})$, which is a long-term key. The encrypted message holds the device's Public Identity Key ($Pub_{IK,wear}$ or $Pub_{IK,impl}$), concatenated with the device's serial number known as $Model_{ID}$.

$$(weblink, c_1) \leftarrow \text{QR Code} \quad \textbf{(1)}$$

$$c_1 = E_{Pub_{IK,manf}}(Pub_{IK,wear} \,||\, Model_{ID}) \quad \textbf{(2)}$$

$$c_1 = E_{Pub_{IK,manf}}(Pub_{IK,impl} \,||\, Model_{ID}) \quad \textbf{(3)}$$

8.3 Authenticated channel for registration of devices

8.3.1 Authentication of devices to the manufacturer's repository

As shown in Figure 13, the Key Management app reads the QR code from a brand-new wearable or medical implant.

Figure 16—Authentication of devices to the manufacturer's repository.

The Key Management app takes the QR content (Equation 1), concatenates its public identity key $(Pub_{IK,app})$ and composes the message "Authentication. Request" (Equation 3). Finally, it sets a TLS link to the Manufacturer's repository using the cryptographic libraries of iOS or Android and finally sends the message:

$$\text{Authentication.Request}(weblink, c_1, Pub_{IK,app}) \quad \textbf{(4)}$$

The manufacturer's repository can decrypt c_1 with its private Identity Key $(Priv_{IK,manf})$ and check the device's $Pub_{IK,wear}$ or $Pub_{IK,impl}$ and $Model_{ID}$ against its internal database. If the validation is correct, the device is authenticated to the Manufacturer's repository, and consequently to the Key management app and Smart coordinator.

8.3.2 Authentication of manufacturer's repository to device

Once the device is authenticated, the repository composes an encrypted message c_2 using the app's identity key containing the device's Public Identity Key $(Pub_{IK,wear}$ or $Pub_{IK,impl})$ concatenated with its Public Identity Key $(Pub_{IK,manf})$, and pre-configured Additional Data AD as shown in Equations 5 or 6.

$$c_2 = E_{Pub_{IK,app}}\left(Pub_{IK,wear} \,||\, Pub_{IK,manf} \,||\, AD\right) \quad \textbf{(5)}$$

$$c_2 = E_{Pub_{IK,app}}\left(Pub_{IK,impl} \,||\, Pub_{IK,manf} \,||\, AD\right) \quad \textbf{(6)}$$

Finally, the manufacturer's repository sends the message:

$$\text{Authentication.Response}(c_2) \quad \textbf{(7)}$$

to the Key Management app via a TLS link as shown in Figure 14.

Figure 17—Authentication of the manufacturer's repository to the device.

The Key Management app can decrypt c_2 with its $Priv_{IK,app}$ and learn the device's $Pub_{IK,wear}$ or $Pub_{IK,impl}$, and manufacturer's $Pub_{IK,manf}$. If the authenticated decryption is successful the device and manufacturer's repository are authenticated to the Key Management app.

The Key Management app composes an encrypted message c_3 using the device's $Pub_{IK,wear}$ or $Pub_{IK,impl}$ containing the app's $Pub_{IK,app}$ manufacturer's $Pub_{IK,manf}$ and vendor's specific Additional Data AD as shown in Equations.

$$c_3 = E_{Pub_{IK,wear}}\left(Pub_{IK,app} \,||\, Pub_{IK,manf} \,||\, AD\right) \quad \textbf{(8)}$$

$$c_3 = E_{Pub_{IK,impl}}\left(Pub_{IK,app} \,||\, Pub_{IK,manf} \,||\, AD\right) \quad \textbf{(9)}$$

Finally, the Key Management app sends the message:

$$\text{Authentication.Response}(c_3) \quad \textbf{(10)}$$

to the device (wearable or medical implant) via the SmartBAN coordinator as shown in Figure 14. If the wearable or medical implant can decrypt c_3 successfully using $Priv_{IK,wearl}$ or $Priv_{IK,impl}$, the manufacturer's repository and the Key Management app are authenticated on the device.

8.3.3 Authentication phase accomplished

Once the mutual authentication of devices (wearables or medical implants), Key Management app, and Manufacturer's repository finishes successfully, all cryptographic credentials are set up and stored securely with the security guarantees that all parties are legit including pairwise identity keys. This phase is only needed the first time a wearable or medical implant joins a BAN.

After registration, devices (wearables or medical implants), Smart Coordinator, and Key Management app can set up secure communication links with state-of-the-art encryption, authentication, and integrity of data without the requirement to be connected to a trusted third party (PKI) for authentication of such SmartBAN components. That is, BANs can work standalone, and with the guarantee that devices are not communicating with a forged party, intruder, or attacker.

8.4 Cryptographic dependencies

8.4.1 General

The setup for devices (wearables and implants) and the SmartBAN coordinator is for the agreement that specifies the cryptographic dependencies and parameters required to run the cybersecurity protocol. The SmartBAN coordinator generates a pair of ephemeral keys ($Priv_{EK,SC}$, $Pub_{EK,SC}$) for the Authenticated Key Exchange (AKE), and chooses a seed ($Seed_{OPRF}$) of N_h octets for the OPRF. The SmartBAN Coordinator can use the ephemeral keys with multiple devices during a registration phase and generate a different OPRF seed for each device.

The proposed protocol depends on the following cryptographic primitives: Oblivious Pseudorandom Function (OPRF), Cryptographic Hash Function (SHA), Key Derivation Function (KDF), Stream cipher, and lightweight block cipher.

8.4.2 Oblivious Pseudorandom Function

A two-party protocol between a client and a server is an Oblivious Pseudo-Random Function (OPRF) if there exists some PRF family f_k, such that privately realizes the following functionality:

1) *Inputs*: The client holds an evaluation point x. The server holds a key k.
2) *Outputs*: The client outputs $f_k(x)$. The server outputs nothing.
3) $(k, x) \rightarrow \left(\perp, f_k(x)\right)$

More formally; Let p q be primes such that $q|p-1, n \in N$, $\mathrm{k} = (a_0, \dots, a_n) \leftarrow^{\mathrm{R}} Z_{n+1}^{q}$ and $g \in Z_p$ is an element of order p . The Naor-Reingold PRF with key k on input $x = x_1, x_2, \dots, x_n \in \{0,1\}^n$ is defined as follows:

$$f_k(x) = g^{a_0 \prod_{i=1}^{n} a_i^{x_i}} \quad \textbf{(11)}$$

Equation 11 means to raise g^{a_0} to a_i if and only if there is a bit of x is 1. The values of $f_k(x)$ on chosen inputs x_i are indistinguishable from randomly sampled elements from the prime group <g> and hence pseudorandom under the Decisional Diffie- Hellman assumption (DDH)[]. Moreover, a variant of Equation 11, the function:

$$f_k^H(x)H(x)^k \quad \textbf{(12)}$$

with hash function H is a PRF under the assumption that H produces uniformly random elements from a prime group <g>. Implicitly when setting $g^a \leftarrow H(x), f_k^H(x) = g^{ak}$ becomes a Diffie-Hellman value. Therefore, we refer to Equation 12 as HashDH. f_k^H can be obliviously evaluated with a blinded exponentiation protocol, depicted in Figure 15.

Figure 18—Blinded exponentiation in the HashDH PRF protocol.

A variant of Equation 12 named 2HashDH [], where the client adds an outer hash H_2 and outputs:

$$f_k^{2H}(x) = H_2(x, H_1(x)^k) \quad \textbf{(13)}$$

Updatable OPRFs or key rotation enables periodically changing the secret key to mitigate the risk and impact of key exposure. An OPRF is called updatable if there is an efficient (maybe interactive) procedure that lets the client update previously computed PRF values to a new key. Such property is independent of the evaluation process and rather a property of the PRF. The natural PRF construction that satisfies these requirements is $f_k(x) := H(x)_k$, This approach is compatible with all OPRFs that produce outputs of the form Xk (for arbitrary X), but unfortunately does not work with the more popular 2HashDH variants.

8.4.3 Cryptographic Hash Function

8.4.4 Key Derivation Function

8.4.5 Stream cipher

8.4.6 Lightweight block cipher

8.5 Asymmetric Password Authenticated Key Exchange

8.5.1 Public parameters and components

Security parameter τ.

Group G of prime order q; $|q| = 2\tau$ and generator g. G^* denotes $G\backslash\{1\}$).

Hash function $H_2(\cdot,\cdot)$ with range $\{0,1\}^{2\tau}$.

Hash to Elliptic Curve $H_1(\cdot)$ with range G.

OPRF function is defined as $F_k(x) = H_2(x, H_1(x)^k)$ for key k $\in \mathbb{Z}_q$.

8.5.2 Registration protocol

Once the authentication phase has finished successfully, the cryptographic credentials of devices (wearables, implants), smart coordinator, and Key Management app are verified and safe to use. Also, during the authentication phase, all devices have populated their keys' table with all respective public keys.

The registration phase consists of the implementation of the OPRF protocol $f_k(x) = H_2(x, H_1(x)^k)$, where x is a password, PIN code, biometric, or token (henceforth denominated as password for short) stored in a wearable or implant provided by the user during the authentication phase via the SmartBAN coordinator to the wearable or implant, and k is the OPRF key provided by the Key Management app. Hence, the password provided by the wearable or implant is not known to the Key Management app, and the key provided by the Key Management app is not known to the wearable or implant. Consequently, if an attacker breaches the Key Management app (or personal device), the wearable's or implant's password or hash will not be stored there and the attacker will not be able to reproduce the OPRF protocol to recover the session key.

The Registration protocol is implemented using the following messages: Registration.Request(.), Registration.Response(.) and Record(.) are shown in Figure 16.

Figure 19—Registration phase.

1. Upon receiving an association response from the SmartBAN Coordinator, the device U (wearable, implant) picks $r \leftarrow_R \mathbb{Z}_q$ and sends $a = \left(H_1(x)\right)^r$ and ID_{wear} (or ID_{impl}) is denoted as ID_U to the Key Management app (S) via the SmartBAN Coordinator.
2. Upon receiving a from U, S picks $k_s \leftarrow_R \mathbb{Z}_q$ and sends $b = a^{k_s}$ and ID_S .
3. Upon receiving b from S, U computes $rwd = H_2(x, b^{1/r}) = H_2(x, H_1(x)^{k_s})$; $Env = E_{rwd}(Priv_U, Pub_S)$ and sends Env to S. Registration ends in U.
4. Upon receiving Env, S records in the SmartBAN Coordinator: $ID_U, Env, Pub_U, k_s, Priv_S = Credentials_U$. Registration ends in S.

After the one-time registration protocol ends, the devices' cryptographic credentials (wearables or implants) are stored in the SmartBAN Coordinator.

8.5.3 Login protocol

After registration, devices (wearables, implants) can join secure SmartBAN sessions at any time, even if they were switched off.

To start a secure session, devices and the SmartBAN Coordinator reproduce the OPRF protocol, but this time to recover the encrypted keys for an AKE protocol exchange without requiring to be online (access to a PKI via WiFi or 5G, 6G infrastructure). The Login protocol can run standalone with the security guarantees that an attacker cannot hack such a session even if the SmartBAN coordinator gets compromised.

The Login protocol is implemented using the following messages: Login.Request(.), and Login.Response(.) are shown in Figure 17.

Figure 20—Login phase.

1. Upon receiving an association response from the SmartBAN Coordinator, the device U (wearable, implant) picks $r \leftarrow_R \mathbb{Z}_q$ and sends $a = \left(H_1(x)\right)^r$, and ID_U to the SmartBAN Coordinator.
2. Upon receiving *a* and ID_U from *U, S* retrieves $Env, Pub_U, k_s, Priv_S \leftarrow Credentials_U$; sends *Env*, $b = a^{k_s}$ to *U* and finally computes $Shared.Key = \mathrm{AKE}(Priv_S, Pub_U)$. Login ends in *S*.
3. Upon receiving *Env*, *b* from *S, U* computes $rwd = H_2(x, b^{1/r}) = H_2(x, H_1(x)^{k_s})$; $Priv_U, Pub_S = D_{rwd}(Env)$; $Shared.Key = \mathrm{AKE}(Priv_U, Pub_S)$. Login ends in *U*.

At the end of the Login protocol, a wearable or implant and the SmartBAN coordinator share the same secret key, which is used to derive a session key.

9 Support for 5G services

9.1 Introduction

5G systems enable access to service-agnostic systems over the 5G radio air interface, extending 5G services to non-3GPP systems. This convergence will be emphasized in future 6G systems for massive IoT, including industrial and medical applications. 5G integrates 3GPP and non-3GPP access networks to adopt vertical domains that employ heterogeneous access networks, known as 5G Non-Public Networks (NPNs). This seamless interworking between 5G access and other medical access technologies minimizes operational costs for SmartBAN applications and the widespread adoption of 5G and future 6G networks.

Non-3GPP access to the 5GNC provides data services to end-devices, consisting of procedures for authentication, authorization, and data session establishment, which involves protocols for the exchange of messages between 5GNC components, the non-3GPP access network, and end-devices (another SmartBAN coordinator or medical service provider).

9.2 Overview of 5GCN

The 5GCN is a collection of interconnected Network Functions (NFs) that provide core functionalities. Each NF exposes its services to other NFs, acting as a service producer. On the receiving end, NFs as consumers can use the services offered by other NFs. This model that exposes and makes services available characterizes the so-called Service-Based Interface (SBI).

The point-to-point communications links between NFs are reference points operating under a communication protocol. The reference point representation describes how NFs interact with each other.

This framework defines the 5GCN as a producer and consumer model or Service-Based Architecture (SBA).

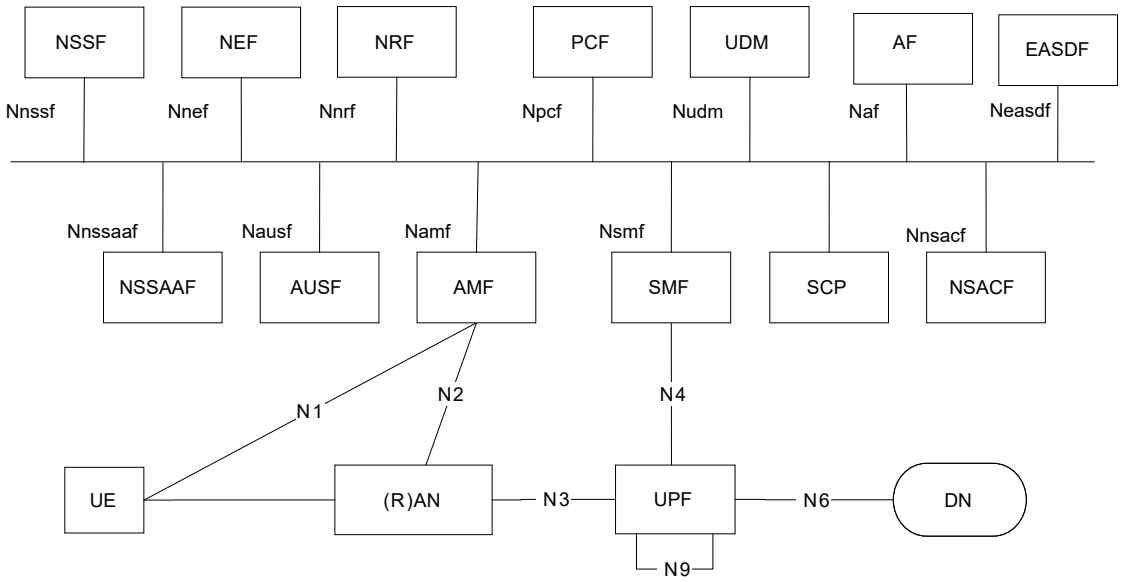


Figure 21—5G Service Base Architecture

For a UE to establish and maintain transport sessions for data, it requires continuous communication with the 5GCN for control and management tasks. Hence, the 5G SBA is divided into user plane and control plane NFs (Figure 21), where

reference points can be a the PHY and Link layers concerning the OSI model, while others are at the Network layer or upper layers concerning the OSI model.

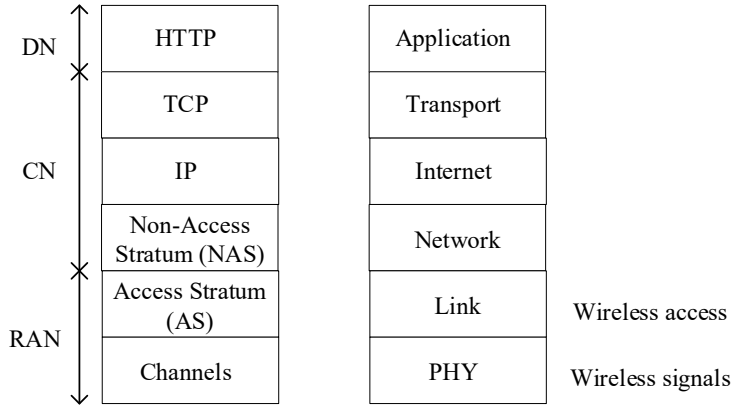


Figure 22—5G layering model compared to a variation of the OSI model.

NOTE — RAN: Radio Access Network. CN: Core Network. DN: Data Network.

However, the interaction of NFs (Figure 21) in the UP and CP over the 5G layering model (Figure 22) is not easy to imply and requires the comprehension of several 3GPP standard documents.

For example, considering the reference points as the interface of NFs exposing and consuming services, the NAS signaling between UE and Access and Mobility Function (AMF) is performed via N1. The N2 interface is the point-to-point communication between gNodeB and AMF for transferring session management messages. The N3 interface between gNodeB and User Plane Function (UPF) is used for exchanging packets in UP, whereas N11 is used for AMF and Session Management Function (SMF) interactions. SMF employs the N4 interface to send packet detection rules and forward them to UPF. Finally, the N6 interface connects UPF and Data Network (DN), which is the Internet or 5G services. This is only a brief overview. Details can be found in the 3GPP standards.

9.3 Support for non-3GPP access networks

9.3.1 General

The 5GCN specifies the connectivity of UE via a non-3GPP access network, for the following types of access: untrusted, trusted, and wireline. The SmartBAN coordinator, henceforth denominated as User Equipment (UE) in the context of support for non-3GPP access networks, can be connected to the 5GCN via the non-3GPP access network described in TS 23.501 and TS 23.502.

A Public Land Mobile Network (PLMN) may advertise the type of non-3GPP access network it supports. Therefore, a UE can discover the non-3GPP access networks that can provide 5GCN connectivity.

The SmartBAN Coordinator under an untrusted non-3GPP access network shall be connected to the 5G Core Network via a Non-3GPP InterWorking Function (N3IWF), whereas under a trusted non-3GPP access network, the SmartBAN coordinator shall be connected to the 5G Core Network via a Trusted Non-3GPP Gateway Function (TNGF). Both the N3IWF and the TNGF interface with the 5G Core Network CP and UP functions via the N2 and N3 interfaces, respectively.

The SmartBAN coordinator shall establish an IPsec tunnel with the N3IWF or with the TNGF to register with the 5G Core Network over non-3GPP access as described in TS 23.502. The N1 NAS signalling over non-3GPP accesses shall be protected with the same security mechanism applied for N1 over a 3GPP access.

Figure 23 shows the 5G functions that are relevant for non 3GPP access network.

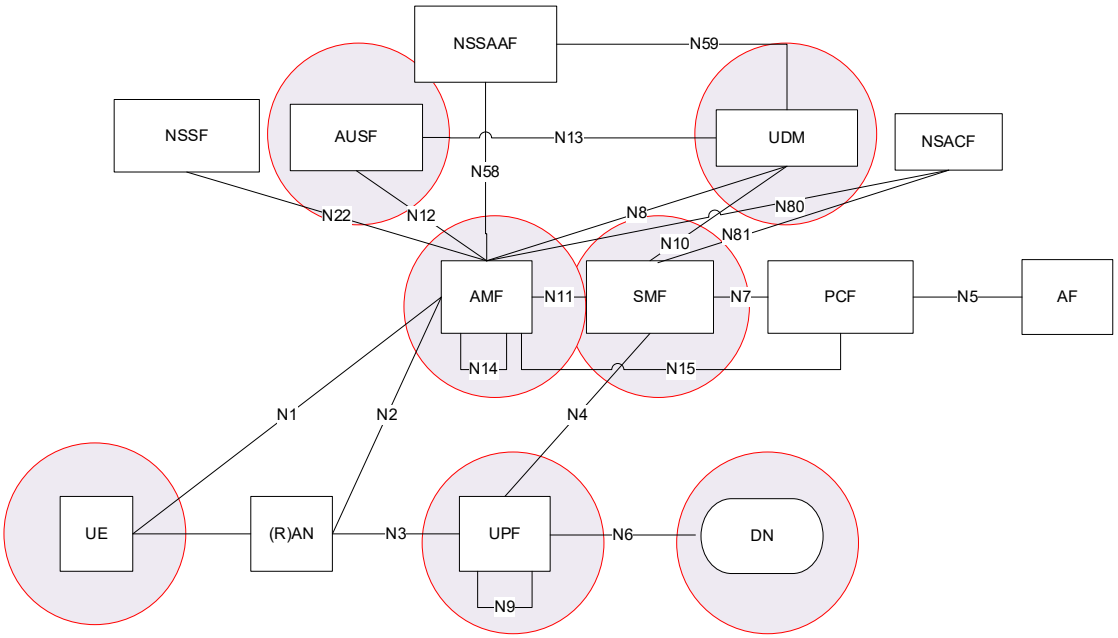


Figure 23—5G core network functions relevant for non 3GPP acesss use cases.

Another important access in 5G is Wireline 5G Access Network (W-5GAN) that includes the support of Massive IoT and Critical IoT. The W-5GAN is connected to the 5GCN via a Wireline Access Gateway Function (W-AGF). The W-AGF interfaces the CP and UP functions via N2 and N3 interfaces, respectively.
The SmartBAN coordinator supports the scenario of 5G Residential Gateway (5G RG) connected via the Next Generation Radio Access Network (NG RAN) as illustrated in Figure 24.

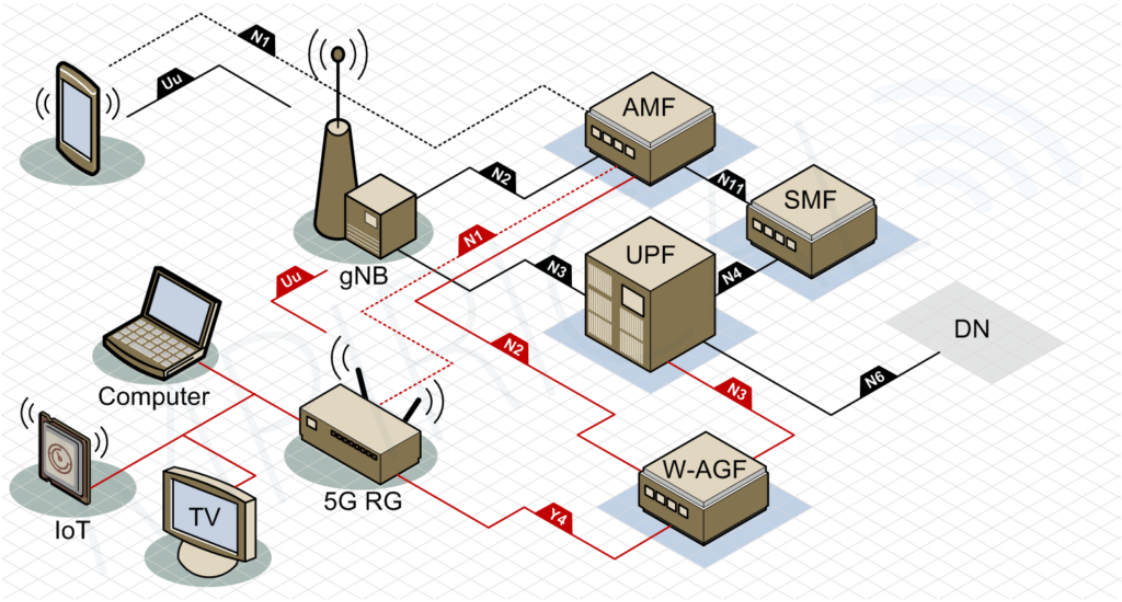


Figure 24 — Fixed wireline access: 5G Residential Gateway (5G RG)

The 5G RG provides the connection between a networked home or office to the 5GCN, and consequently to a DN such as the Internet or 5G services. The 5G RG supports a wireless interface (Uu), and a wireline interface (Y4) via the

Wireline–Access Gateway Function (W-AGF) to the 5GCN, including the N1 reference point used for NAS signalling to the AMF.

An alternative fixed endpoint has also been specified as Fixed Network Residential Gateway (FN RG). FN RG operates similarly to the 5G RG; however, it does not support the N1 (NAS) reference point. The W-AGF supports dealing with the NAS signaling on behalf of FN RG, as illustrated in Figure 25.

Using either 5G RG or FN RG, the information is sent to IoT (SmartBAN) using WLAN within the home network known as a Private 5G Network using licensed, unlicensed, or shared spectrum.

Therefore, with the introduction of wireline access in 5G, service providers will be able to offer a truly converged service over wireless and fixed broadband cable access networks.

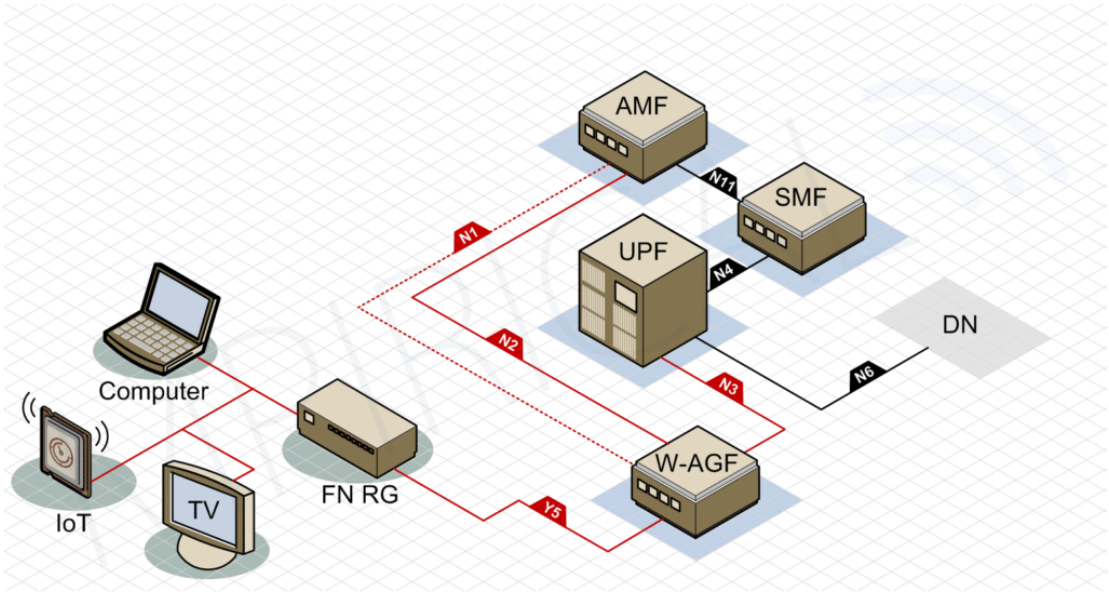


Figure 25 — Fixed wireline access: Fixed Network Residential Gateway (FN RG)

The 5G RG and FN RG facilitate the support of a non-3GPP access network. The SmartBAN coordinator envisions the 5G RG or FN RG specification for the monitoring of patients at home, hospitals, and healthcare facilities, especially for the elderly population, with the option of mobility outside the range of the 5G RG.

9.3.2 Untrusted non 3GPP access

9.3.2.1 General

The reference architecture is shown in Figure 25. The N3IWF provides a secure connection for the SmartBAN coordinator to access the 5GCN via the 5G CP and UP functions, as illustrated in Figure 25.

The N3IWF connects to the AMF via the N2 interface in the CP. For data traffic, the N3IWF connects to the UPF in the UP via the N3 interface. The SmartBAN coordinator uses the interface N1 for NAS signaling to advertise its presence, request services, and manage its connection.

After the authentication and authorization procedures, the SmartBAN coordinator accesses the 5GCN through the N3IWF The transfer of data packets between the SmartBAN coordinator and the DN over IPSec tunnels for the UP and CP. Moreover, the General Packet Radio Services Tunnelling Protocol (GTP-U) establishes a tunnel between the N3IWF and the UPF as shown in Figure x..

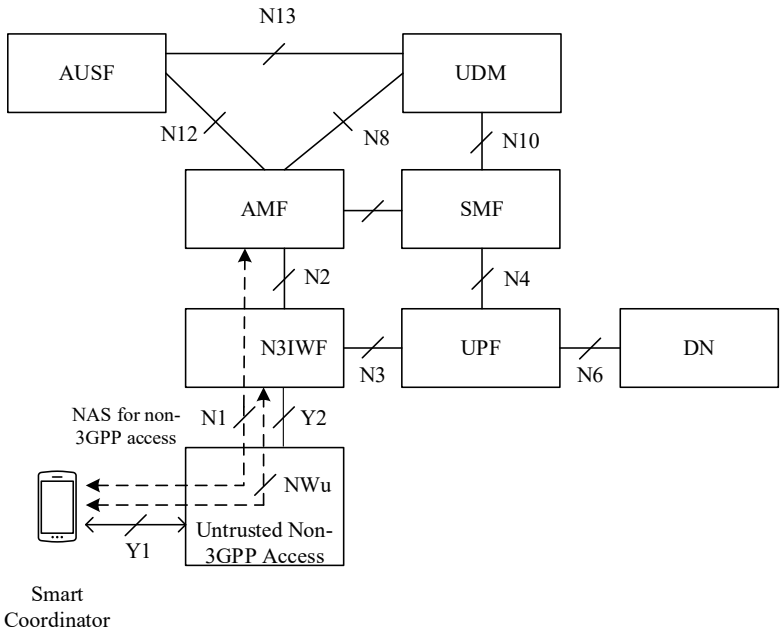


Figure 26—Architecture of SmartBAN coordinator as an untrusted non-3GPP access network.

9.3.2.2 Summary of connection protocols

A summary of the protocols and reference points involved are shown in Table 33.

Table 33 — Protocols and reference points for untrusted non-3GPP access

Component	Protocol/Interface	Role
UE ↔ N3IWF	IKEv2/IPSec	Secure tunnel setup
N3IWF ↔ AMF	N2 (NGAP over SCTP)	Authentication & session management
AMF ↔ AUSF/UDM	Nausf, Nudm (HTTP/2)	Authentication & key generation
N3IWF ↔ UPF	N3 (GTP-U over UDP)	User data forwarding

9.3.2.3 Prerequisites for Untrusted Non-3GPP Access

The following 5G CN must be in place:

- 5G Core Network with:
    - N3IWF (Non-3GPP InterWorking Function)
    - AMF (Access and Mobility Management Function)
    - AUSF (Authentication Server Function)

    - UDM (Unified Data Management)
- SmartBAN coordinator supporting 5G and EAP-based authentication.
- Untrusted Wi-Fi Access Point without special requirements.

9.3.2.4 Steps Connection Process

Step 1: UE Connects to Untrusted Wi-Fi

- The UE associates with an untrusted Wi-Fi network (e.g., a public hotspot).
- The Wi-Fi network provides Internet access but no direct 5G integration.

Step 2: UE Discovers N3IWF

- The UE must know the IP address/FQDN of the N3IWF (pre-configured or via DNS query).
- The UE initiates an IKEv2/IPSec tunnel setup with the N3IWF.

Step 3: IKEv2/IPSec Tunnel Establishment

- IKEv2 Phase 1 (Authentication)
    - UE and N3IWF exchange security parameters.
    - The UE authenticates the N3IWF using a certificate (if configured).
- IKEv2 Phase 2 (EAP Authentication for UE)
    - The N3IWF acts as a relay between UE and 5GCN.
    - The UE runs EAP-AKA' (Extensible Authentication Protocol for 5G).
    - The N3IWF forwards EAP messages to the AMF/AUSF in the 5GCN.

Step 4: 5G Authentication (EAP-AKA')

- AUSF/UDM verifies the UE's credentials (SUPI/SUCI).
- If successful, the 5G Core generates security keys:
    - K_seaf (from AUSF) → Used for session security.
    - K_amf → Sent to AMF.
    - K_n3iwf → Sent to N3IWF for IPSec encryption.

Step 5: IPSec Security Association (SA) Setup

- After authentication, the N3IWF and UE establish a secure IPSec tunnel.
- All user traffic between UE and 5GCN is encrypted via this tunnel.

Step 6: Registration with 5G Core (AMF)

- The UE sends a Registration Request to the AMF via the N3IWF.
- The AMF validates the UE's subscription and establishes a 5G session.
- The SMF (Session Management Function) assigns a PDU Session (similar to a bearer in LTE).

Step 7: Data Transmission over Untrusted Wi-Fi

- All user traffic now flows securely through the IPSec tunnel to the N3IWF.
- The N3IWF forwards traffic to the UPF (User Plane Function) in the 5GCN.
- The UE can now access 5G services (e.g., IMS, Internet) securely.

9.3.2.5 Protocol description from SmartBAN coordinator to 5GCN via N3IWF

9.3.2.5.1 General

The protocol breakdown traces the IKEv2/EAP-AKA' handshake and IPSec tunnel establishment between the SmartBAN coordinator and 5G Core via the N3IWF .

9.3.2.5.2 Initial connection set up

A: SmartBAN coordinator connects to an untrusted non-3GPP access network in L2

The untrusted non-3GPP access network is assumed to be a Wi-Fi AP over reference point Y1 using WPA2/3 Enterprise security. The connectivity follows the IEEE Std 802.11.

Note: WPA2/3 is independent of 5G authentication.

B: SmartBAN coordinator discovers N3IWF in L3

The N3IWF IP address may be pre-configured in the SmartBAN coordinator. Otherwise, it makes a DNS query for the N3IWF IP address.

SmartBAN coordinator: Query("_n3iwf._5gc.<operator-domain>") → DNS server.

DNS Server: Response (N3IWF IP) → SmartBAN coordinator.

9.3.2.5.3 SmartBAN coordinator establishes IPSec Tunnels with IKEv2

Phase 1: IKE_SA_INIT (Key Exchange)

1. SmartBAN coordinator → N3IWF:

```
IKE_SA_INIT Request {
        HDR (Initiator SPI, Version)
        SAi1 (Proposed IKEv2 Algorithms: AES-GCM, SHA-256, DH Group 19/20)
        KEi (Public Key for DH Exchange)
        Ni (Nonce)
}
```

Now both derive IKE_SA keys (SK_e, SK_a, SK_d).

2. N3IWF → SmartBAN coordinator:

IKE_SA_INIT Response {
HDR (Responder SPI)
SAr1 (Chosen Algorithms)
KEr (N3IWF's Public Key)
Nr (Nonce)
}

Now both derive IKE_SA keys (SK_e, SK_a, SK_d).

Phase 2: IKE_AUTH + EAP-AKA' (Authentication)

3. SmartBAN coordinator → **N3IWF**:

IKE_AUTH Request {
HDR (Encrypted with `SK_e`)
SK {IDi (UE Identity, e.g., SUPI/SUCI)}
SK {AUTH (UE's Signature over Message 1/2)}
SK {SAi2 (Proposed IPSec Algorithms)}
SK {TSi/TSr (Traffic Selectors)}
SK {EAP-Response/Identity (SUPI/SUCI)}
}

4. N3IWF → AMF/AUSF:

Forwards EAP-Identity via reference point N2 (NGAP) to AMF.

AMF fetches authentication vectors from AUSF/UDM.

5. N3IWF → SmartBAN coordinator :

IKE_AUTH Response {
HDR (Encrypted)
SK {EAP-Request/AKA'-Challenge (RAND, AUTN)}
}

6. SmartBAN coordinator → N3IWF:

IKE_AUTH Request {
HDR (Encrypted)
SK {EAP-Response/AKA'-Challenge (RES)}
}

The SmartBAN coordinator validates AUTN and computes RES using K (from USIM).

7. N3IWF → AMF/AUSF:

Verifies RES with AUSF. If valid, **5G keys** (K_amf, K_n3iwf) are generated.

8. N3IWF → UE:

IKE_AUTH Response {
HDR (Encrypted)
SK {EAP-Success}
SK {AUTH (N3IWF's Signature)}
SK {SAr2 (IPSec SA Parameters)}
SK {TSi/TSr}
}

IPSec Child SA is now established.

9.3.2.5.4 IPSec Child SA Activation

Encapsulating Security Payload (ESP). A security association is created with AES-GCM-256 for encryption and SHA-256 for integrity.

SmartBAN coordinator ↔ N3IWF: ESP packets (SPI, Seq, Encrypted Payload)

9.3.2.5.5 5G Registration & PDU Session Setup

N2/N1 Signaling (via N3IWF):

1. **UE → N3IWF → AMF**:

   5G Registration Request{ (NAS over IPSec)

   SUCI/5G-GUTI

   Requested NSSAI

   }

2. **AMF ↔ AUSF/UDM**:

   Secondary authentication (if needed).

3. **AMF → SMF**:

   PDU Session Create Request {

   DN (e.g., "internet")

   QoS Profile

}

4. **SMF ↔ UPF**:

   Sets up **N4 (PFCP)** session and **N3 (GTP-U)** tunnel.

5. **SmartBAN coordinator ↔ UPF**:

   User data flows over:

   SmartBAN coordinator → Wi-Fi AP → IPSec → N3IWF → GTP-U → UPF → Internet

9.3.2.6 Summary of security

1. **Link layer (L2)**: Protected by WPA2/WPA3 (independent of 5G).
2. **Network layer (L3)**:
   - **IKEv2**: Mutual authentication (EAP-AKA' + PKI).
   - **ESP**: AES-256 encryption for user data.
3. **5G Core**:
   - Keys generation (K_n3iwf) protect N3IWF-AMF link.
   - UPF enforces QoS and firewall rules.

9.3.3 Trusted non-3GPP access network

9.3.3.1 General

The trusted non-3GPP access network (TNAN) is formed by the Trusted non-3GPP Access Point (TNAP) and the Trusted non-3GPP Gateway Function (TNGF) that provide a trusted connection to the 5GCN, as shown in Figure 26. The trusted access means that the Mobile Network Operator (MNO) of a 5G Core Network controls the operation and management of the TNAN.

Compared to untrusted non-3GPP access, in trusted non-3GPP access, security is enabled on the non-3GPP access layers, rather than as part of an encrypted IPsec tunnel. Nonetheless, the 3GPP 5G specifications mandate the establishment of an IPsec tunnel, but without encryption enabled. This allows the implementation of the same protocol stack, regardless of whether access is trusted or untrusted.

The SmarttBAN coordinator over the TNAN is registered, authenticated, and authorized throughout the 5GCN. The SmartBAN coordinator establishes a secure connection to the TNGF over the NWt interface. After the establishment of IPSec with the TNGF, the SmartBAN coordinator uses a TCP connection for transporting NAS messages in the CP. Furthermore, the SmartBAN coordinator establishes a child IPSec tunnel to transfer UP data.

9.3.3.2 Wireless access with TNGF

The TNAN is split into two parts, the Trusted Non-3GPP Access Point Function (TNAP) and the Trusted Non-3GPP Gateway Function (TNGF), as shown in Figure 26. Ta represents the interface between the trusted Access Point and the TNGF, within the 5GCN.

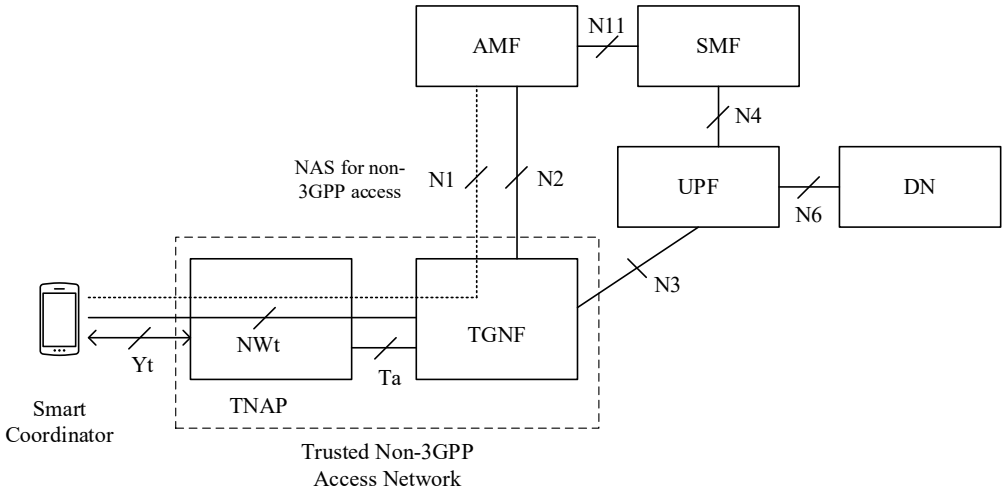


Figure 27 — Not roaming trusted non-3GPP access network

9.3.3.2 Protocol description from SmartBAN coordinator to 5GCN via TNGF

9.3.2.5.1 General

The protocol breakdown traces the session establishment between the SmartBAN coordinator and 5GCN via the TNGF.

9.3.2.5.2 Initial connection set up

A: SmartBAN coordinator connects to a trusted non-3GPP access network in L2

The untrusted non-3GPP access network is assumed to be a Wi-Fi AP over reference point Y1 using WPA2/3 Enterprise security. The connectivity follows the IEEE Std 802.11 secure association.

9.3.2.5.3 EAPOL-Start (Trigger EAP-AKA')

Protocol: 802.1X/EAP over L2 (EAPOL)

SmartBAN coordinator → AP: EAPOL-Start

AP → SmartBAN coordinator: EAP-Request/Identity

SmartBAN coordinator → AP: EAP-Response/Identity (SUPI/SUCI)

NOTE: The Subscription Concealed Identifier (SUCI) contains the encrypted Subscription Permanent Identifier (SUPI) using the Elliptic Curve Integrated Encryption Scheme (ECIES).

9.3.2.5.4 RADIUS Authentication (AP ↔ 5GCN)

Protocol: RADIUS (UDP port 1812)

1. AP → AAA Server:

RADIUS Access-Request {

EAP-Response/Identity (SUCI)

Called-Station-ID (AP MAC)

}

2. AAA Server → AUSF (via STa/SWx interface):

Conversion to 5G Authentication and Key Agreement (AKA) authentication vectors.

3. AAA Server → AP:

RADIUS Access-Challenge {

EAP-Request/AKA'-Challenge (RAND, AUTN)

}

4. EAP-AKA' Challenge (UE ↔ AP)

AP → UE: EAP-Request/AKA'-Challenge (RAND, AUTN)

SmartBAN coordinator → AP: EAP-Response/AKA'-Challenge (RES)

SmartBAN coordinator verifies the Authentication Token (AUTN) using the Universal Subscriber Identity Module (USIM) and computes RES/CK/IK.

In 5G authentication, RES, CK, and IK are components of the Authentication Vector (AV), which is used to secure communication between the User Equipment and the 5GCN.

RES (Response): The UE calculates this response value based on the RAND (Random Number) and the AUSF's authentication token (AUTN) or challenge.

CK (Cipher Key): This key encrypts communication between the UE and the 5GCN. It's derived from the AV and secures both NAS (Non-Access Stratum) signaling and data traffic.

IK (Integrity Key): This key ensures the integrity of the communication, meaning it verifies that the data hasn't been tampered with. It's also derived from the AV and is used to protect NAS messages.

9.3.2.5.5 5G Key Derivation

Protocol: 5G AKA

1. AUSF/UDM:

- Generates K_ausf → K_seaf → K_amf
- Derives K_tngf for TNGF

2. RADIUS Accept:

AAA → AP: RADIUS Access-Accept

- EAP-Success
- Master Session Key (MSK) (for WPA3 key hierarchy)

9.3.2.5.6 TNGF Registration

Protocol: NGAP (SCTP) over N2 interface.

Signaling Protocol for 5G SA: Next Generation Application Protocol (NGAP) on the N2 interface between the trusted non-3GPP access network and the AMF. NGAP is transferred over the Stream Control Transmission Protocol (SCTP) as part of IP network signaling.

TNGF → AMF: Initial SmartBAN coordinator message

- 5G NAS Registration Request
- SmartBAN coordinator Location (Tusted non-3GPP access network ID)

AMF → TNGF: Authentication Request

TNGF → SmartBAN coordinator: EAP-Request/AKA'-Notification

SmartBAN coordinator → TNGF: EAP-Response/AKA'-Notification

TNGF → AMF: Authentication Response

9.3.2.5.7 PDU Session Establishment

Protocol: GTPv2 (N11/N4)

The GPRS Tunnelling Protocol version 2 separates data traffic into different communication flows.

1. SMF Selection:

   AMF → SMF: Nsmf_PDUSession_CreateSMContext

2. UPF Setup:

   SMF → UPF: PFCP Session Establishment

- FAR (Forwarding Rules)
- QER (QoS Policies)

9.3.2.5.8 User Plane Activation

Protocol: GTP-U

The GPRS Tunnelling Protocol User Plane (GTP-U) with UDP port 2152.

SmartBAN coordinator → AP → TNGF → UPF → Internet

NOTE: The security protocols are WPA3 and GTP-U without additional IPSec overhead.

9.3.2.6 Wireless access with TWIF

Mobile UE devices that do not support 5G capabilities (e.g., NAS protocol for N1 and NR-Uu) but have 3GPP credentials: Universal Subscriber Identity Module (USIM) or Embedded Universal Integrated Circuit Card (eUICC) to access the 5GCN via a trusted non-3GPP access network, as shown in Figure 27.

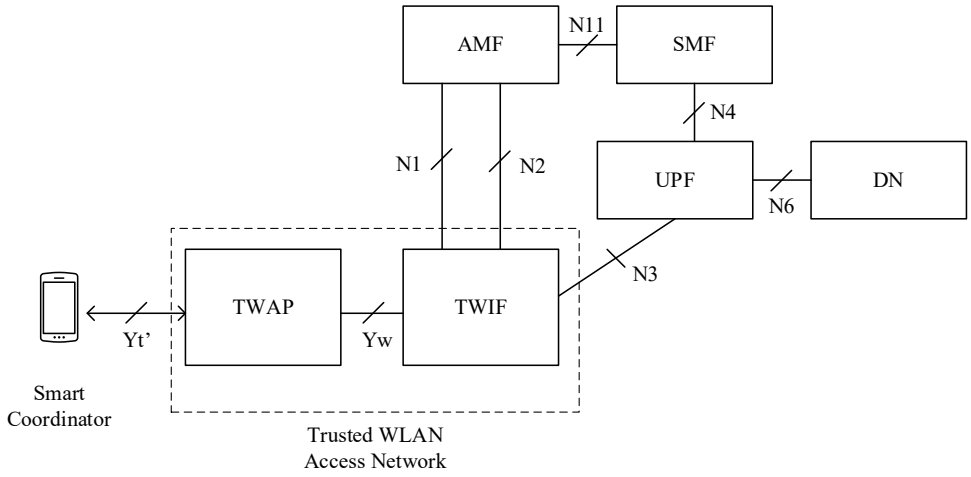


Figure 28— Non-roaming trusted WLAN access network

The SmartBAN coordinator, as a non-3GPP device that does not support 5GCN NAS signalling, is referred to as “Non-5G-Capable over WLAN”, or N5CW device.

Even though a N5CW device does not support the N1 reference point, it may be capable of operating on a 5GCN with the introduction of a dedicated gateway function. The role of the TNGF is therefore replaced by the Trusted WLAN Interworking Function (TWIF), with the main difference that TWIF terminates the N1 NAS interface and is seen as a RAN regarding the Core Network.

A trusted WLAN access network is a particular type of Trusted Non-3GPP Access Network (TNAN) that supports a WLAN access technology, e.g., IEEE Std 802.11, and supports a TWIF function. The 5GCN registration is performed by the TWIF function on behalf of the N5CW device.

The TWIF provides interworking functionality that enables N5CW devices to access a 5GCN. The TWIF supports the following functions:

- Terminates the N1, N2, and N3 interfaces.
- Implements the AMF selection procedure.
- Implements the NAS protocol stack and exchanges NAS messages with the AMF on behalf of the N5CW device.
- On the user plane, it relays protocol data units (PDUs) between the Yw interface and the N3 interface.

The Yt' and Yw reference points are outside the scope of the 3GPP specifications. The Yt' reference point transports WLAN messages, while the Yw reference point:

- Shall be able to transport authentication messages between the TNAP and the TWIF for enabling authentication of an N5CW device;
- Shall allow the N5CW device to request and receive IP configuration from the TWIF.
- Shall support the transport of user-plane traffic for the N5CW device.
- The N1, N2, and N3 reference points are the same reference points defined in clause 4.2.7 of TS 23.501.
  NOTE: N1, N2, N3 define interfaces in L3.

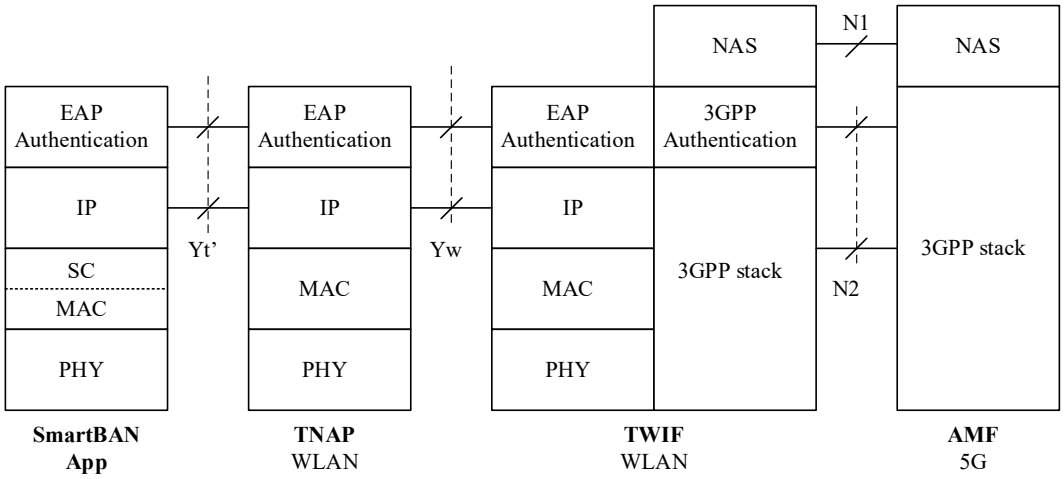


Figure 29 — SmartBAN application protocol stack in a Trusted non-3GPP access network.

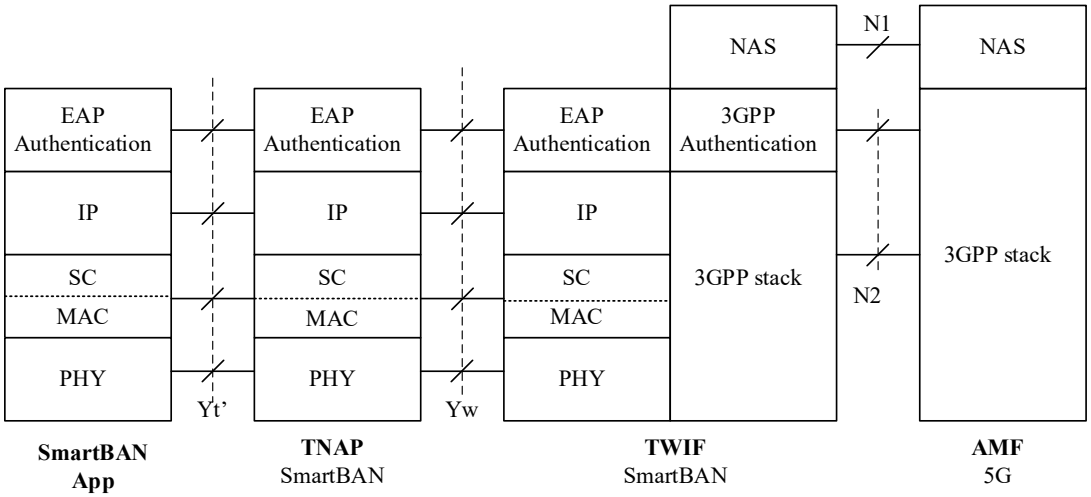


Figure 29 — Concept of SmartBAN application protocol stack as part of a Trusted Wireless non-3GPP access network.

9.3.2.7 Protocol description from SmartBAN coordinator to 5GCN via TWIF

9.3.2.7.1 General

Wireless access with TWIF is a particular case of TNGF. Hence, the protocol description is similar to 9.3.2.6. The connection process involves several layers:

- Association with the TWIF (e.g., WPA3 Enterprise) in L2.
- EAP authentication (L2 and L3), EAP-AKA' for SIM-based devices or EAP-TLS for certificate-based devices (non-SIM but still with 3GPP credentials).
- Interaction with the 5GCN (L3 and above).

The TWIF interacts with the 5GCN using NGAP (Next-Generation Application Protocol) over SCTP for signaling. The user plane uses GTP-U (GPRS Tunneling Protocol User Plane) over UDP. There's also RADIUS involved between the WLAN AP and the AAA server, which ties into the 5G authentication via AUSF/UDM.

9.3.2.7.2 TWAP (L2)

Protocol: IEEE Std 802.11 (WPA3-Enterprise)

- **Purpose**: Secures the wireless link between the SmartBAN coordinator and the trusted Wi-Fi AP.
- **Security features**:
  - **AES-256-GCMP**: Encryption and integrity protection for data frames.
  - **802.1X**: Port-based authentication framework.
  - **EAP-AKA'/EAP-TLS**: Used for device authentication (integrated with 5GC).
- **Frames**:
  - **Authentication/Association**: Establishes L2 connectivity.
  - **EAPOL (EAP over WLAN)**: Encapsulates EAP messages for 802.1X authentication.

9.3.2.7.3 Authentication Protocols

A. Extensible Authentication Protocol (EAP)

- **Role**: Authenticates the device to the 5G Core.
- **Types**:
    1. **EAP-AKA'** (for SIM-based devices with Remote SIM Provisioning (RSP) Compatible with eSIM or eUICC cards):
        - **Mechanism**: Uses SIM credentials (SUPI/SUCI) and 5G authentication vectors (RAND, AUTN, XRES*).
        - **Phases**:
            - **Identity Exchange**: Device sends SUCI.
            - **Challenge-Response**: 5GC validates RES using USIM-derived keys.
    2. **EAP-TLS** (for certificate-based devices):
        - **Mechanism**: Uses X.509 certificates validated by the 5GC PKI.
        - **Phases**:
            - **TLS Handshake**: Mutual authentication (device ↔ AAA server).

B. RADIUS

- **Role**: Relays EAP messages between the Wi-Fi AP and the 5GC.
- **Protocol**: **UDP Port 1812/1813** (authentication/accounting).
- **Key RADIUS Attributes**:
    - User-Name: SUCI or certificate identifier.
    - EAP-Message: Encapsulates EAP-AKA'/TLS payloads.
    - Called-Stataion-ID: MAC address of the Wi-Fi AP.

9.3.2.7.4 5G Core Signaling (Control Plane)

A. NGAP (Next-Generation Application Protocol)

- **Role**: Manages registration, authentication, and session setup between TNGF and AMF.
- **Transport**: **SCTP** (Stream Control Transmission Protocol, Port 38412).
- **Key Messages**:

- **InitialUEMessage**: Registration request from TNGF to AMF.
- **Authentication Request/Response**: Exchanges RAND, AUTN, and RES.
- **Security Mode Command**: Activates integrity/ciphering for NAS signaling.

- **Parameters**:
  - **5G-S-TMSI**: Temporary device identifier.
  - **Allowed NSSAI**: Network slice selection info.

B. HTTP/2 (N11 Interface)

- **Role**: Used by AMF to communicate with SMF for session management.
- **Key Service-Based Interfaces (SBIs)**:
  - **Nsmf_PDUSession_CreateSMContext**: Triggers PDU session setup.

9.3.2.7.5 User Plane Protocols

A. GTP-U (GPRS Tunneling Protocol User Plane)

- **Role**: Encapsulates user data between TNGF and UPF.
- **Transport**: **UDP Port 2152**.
- **Key Fields**:
  - **TEID (Tunnel Endpoint ID)**: Identifies the PDU session.
  - **QFI (QoS Flow Identifier)**: Marks traffic priority (e.g., 5QI values).
- **Data Flow**:

```
Device → Wi-Fi AP → TNGF → UPF → Internet
       [WPA3]      [GTP-U]
```

B. PFCP (Packet Forwarding Control Protocol)

- **Role**: Configures UPF rules (e.g., QoS, routing) via SMF.
- **Transport**: **UDP Port 8805**.
- **Key Messages**:
  - **Session Establishment Request/Response**: Creates GTP-U tunnels.
  - **FAR (Forwarding Action Rule)**: Defines traffic routing (e.g., N6 interface to the Internet).

Annex A (normative): Management Information Base (MIB)

Table 34 — Management Information Base (MIB)

Object	Default value; (Range)	Description / Reference
SupportedDataRatesTX SYNTAX Integer32 UNITS Mb/s ACCESS read_only STATUS Current	1; (1, 2, 3)	
QoSOptionImplemented SYNTAX TruthValue ACCESS read-only STATUS current DESCRIPTION "When true, this attribute indicates that the device supports QoS. The capability is disabled, otherwise."	Truth	

Annex (informative): Bibliography

-

Annex (informative): Change History

Date	Version	Information about changes
<Month year>	<#>	<Changes made are listed in this cell>