ETSI TR 103 944 V1.1.1 (2023-11)

Smart Body Area Network (SmartBAN);
Technical Report on Smart Coordinator
for SmartBAN Networks

Reference
DTR/SmartBAN-0021

Keywords
air interface, wireless ad-hoc network

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Smart Body Area Network (SmartBAN).

The contents of the present document are subject to continuing work within the SmartBAN TB and may change following formal TB approval. Should the TB change the contents of the present document, it will be re-released by the TB 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 early working draft;
  - 1 presented to the TB for information;
  - 2 presented to the TB for approval;
  - 3 or greater shows the TB-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 "**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

The present document lays out an outlook of the smart coordinator, potential service flows to infrastructure, generic architecture, coexistence, cyber-security, and privacy protection.

Introduction

The present document provides information on the functionalities considered necessary and under consideration to implement the next generation of SmartBAN functionality.

1 Scope

The present document is limited to providing information about the smart coordinator operating at the link layer.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

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

[i.1] ETSI TS 103 325 (V1.1.1): "Smart Body Area Network (SmartBAN); Low Complexity Medium Access Control (MAC) for SmartBAN".

[i.2] ETSI TS 103 326 (V1.2.1): "Smart Body Area Network (SmartBAN); Enhanced Ultra-Low Power Physical Layer".

[i.3] ETSI TS 103 806 (V0.0.4): " Smart Body Area Network (SmartBAN); Hub to Hub Communication for SmartBAN Medium Access Control (MAC)".

3 Definition of terms, symbols, and abbreviations

3.1 Terms

For the purposes of 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

Void.

3.3 Abbreviations

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

ACI	Adjacent Channel Interference
AEAD	Authenticated Encryption with Additional Data
AES	Advanced Encryption Standard
AI	Artificial Intelligence

AKE	Authenticated Key Exchange
A-MPDU	Aggregate MAC Protocol Data Unit
A-MSDU	Aggregate MAC Service Data Unit
AP	Access Point
AR/VR	Augmented Reality/Virtual Reality
BCI	Brain-Computer Interface
CPU	Central Process Unit
CRC	Cyclic Redundancy Check
DoS	Denial of Service
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
EdDSA	Edwards-curve Digital Signature Algorithm
HSM	Hardware Security Module
ID	Identity
IoT	Internet of Things
IP	Internet Protocol
ISM	Industrial Scientific and Medical (frequency band)
ISS	Internal Sublayer Service
KPI	Key Performance Indicator
L2	Layer 2
L3	Layer 3
MAC	Medium Access Control
MLDE	MAC Layer Data Entity
MLME	MAC Layer Management Entity
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
OSI	Open System Interconnection
PER	Packet Error Rate
PHY	PHYsical layer
PII	Personally Identifiable Information
PKI	Public Key Infrastucture
PLDE	PHY Layer Data Entity
PLME	PHY Layer Management Entity
QoS	Quality of Service
SAP	Service Access Point
SC	Smart Coordinator
SC2SC	Smart Coordinator to Smart Coordinator
SCLC	Smart Coordinator Link Control
SDR	Software Defined Radio
SHA-3	Secure Hash 3
TSN	Time Sensitive Networking
TX	Transmitter
ZTA	Zero Trust Architecture

4 Outlook of smart coordinator

4.1 Functionalities at a glance

Future healthcare and well-being systems will extend mobile services into new vertical application domains with specific requirements for communication services and well-being services. Such new domain applications come with demanding requirements, such as high availability, high reliability, low latency, and seamless integration into infrastructure.

The technology in smart wristbands, watches, rings, patches, headbands, earplugs, chest-straps, smart clothing, shoe insoles, and in-body sensors, are collectively called wearables. Such technology is measuring ever more aspects of daily people's lives. Smartwatches collect millions of data points per day. People see themselves in ways not possible before and are finding new ways to act on what they learn. The effect on healthcare and lifestyle can be profound.

The Covid-19 pandemic accelerated the process. Wearables entered the lives of more people and took on new roles. With gyms closed, exercise shifted outdoors, and people bought them for the first time, to keep track of how much they exercised.

A parallel trend was that many consumers began to see these devices as tracking specific areas of their health. People had to be checked at home for healthcare reasons. Hospitals and nursing homes started seeing more elderly patients with smartwatches to track their health and send alerts of any problems. Wearable technology is poised to be a seamless part of clinical care, diagnosis, and, in some cases treatment. Artificial Intelligence (AI)-based apps may process the collected data from people's wearables dispensing personalized advice on what to eat or when to go for a walk or exercise. Interactive apps backed up by clinical evidence are likely to prescribe treatment.

The wearables market will split into two categories: medical-grade devices approved by respective regulatory bodies for people with chronic conditions who need tracking with greater care, and devices with fewer features and accuracy for healthy people who want to keep an eye on their metrics and be able to spot a problem early. Leading manufacturers are expected to offer increasingly specific devices for many diverse groups: children, the elderly, people with chronic diseases, and healthy people.

Fulfilling that promise is the next step for SmartBAN. It is going beyond basic radio access. Building the best way to transfer the communication flows to the infrastructure or the edge for processing and evaluation and how to coexist with current technologies such as Bluetooth and Wi-Fi. Note that the edge could be part of the infrastructure or a device at home, a vehicle, or even on the body. The controlling device is named from now on, the smart coordinator.

Healthcare and well-being data will be transformed, with 24/7 monitoring of vital and other health indicators for healthy and sick groups through numerous wearable devices.

Health monitoring will also include in-body devices that communicate with the smart coordinator, which in turn can transport the data to the infrastructure and reach hospitals and healthcare providers.

The integration of the SmartBAN network with such infrastructure, i.e. Wi-Fi™ and 6G, will be fully context-aware, and such integration will become increasingly sophisticated at predicting people's needs.

Context awareness combined with new human-machine interfaces such as the Brain-Computer Interface (BCI) will make interaction with the physical and digital world much more intuitive and efficient. Dynamic digital twins in the digital world with increasing accuracy require synchronous updates of the physical world, and these will be an essential platform for augmenting human abilities.

The computing needed for these devices will not all live in the devices themselves because of their small form factor and battery power limitations. Rather, they may have to rely on locally available computing resources to complete tasks, beyond the edge. Hence, the smart coordinator will play a significant role in this endeavour.

There are problems to solve. Among others, the interface between the current specification of SmartBAN (ETSI TS 103 325 [i.1] and ETSI TS 103 326 [i.2]) and infrastructure at the link layer to minimize latency and guarantee a QoS across networks; concerns about privacy protection, data cyber-security protection, and coexistence with other wireless systems operating in the same frequency band.

The proposed smart coordinator aims to solve those issues and create one entire solution for health monitoring, prevention, and treatment.

4.2 Data traffic between the smart coordinator and the infrastructure

SmartBAN supplies the capability for remote monitoring and care. As told before, it drops the need to visit hospitals often and allows for efficient management of health monitoring for patients and physicians.

The use case suggests automated monitoring of human data. Consequently, such sensitive information should be managed securely with different authorization levels.

Regular monitoring of human data may trigger an alarm to the patient or user via an app, depending on the received information. In other cases, it may trigger authorization to access parts of the patient, like the upper body, digestive system, etc., or user information by other medical care providers.

4.3 Service flows

Most SmartBAN data needs to be transferred to support real-time traffic with a certain level of QoS. In case of emergencies, link availability and reliability are needed.

In this use case, the patient or user has wearables assumed to be connected wirelessly to infrastructure (cellular network, Wi-Fi™) via the smart coordinator. Diverse types of information are transferred to a medical centre (data measuring and policy authorization) via a service provider or network operator. The medical centre will decide the emergency contingency based on a policy to take later actions.

However, the connection may be to an app running at the edge as well. For example, based on health data monitoring, eating, sleeping habits, when it is the most proper time to exercise, and advice on how many calories in a meal to intake, among others.

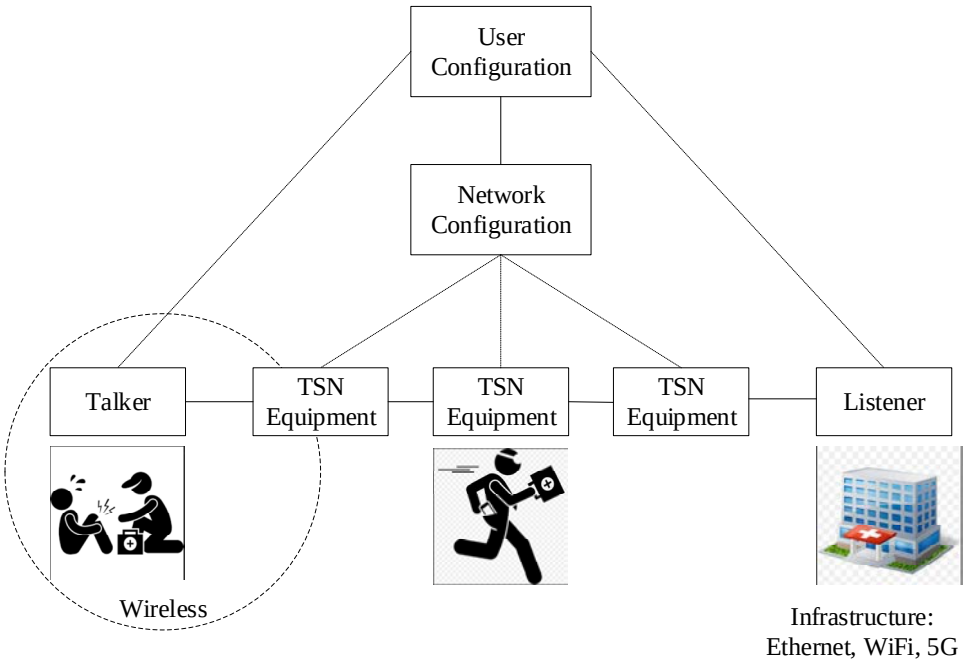


Figure 1: Service flows in SmartBAN emergency time-sensitive domain use case

In-body medical devices are implanted inside the body (if they are fixed), while some others are digestible (capsule endoscope). Such in-body devices have a small form factor, implying low power consumption and limited transmission power. Also, the information should be protected as it conveys [vital] human-body information.

SmartBAN implements power-efficient mobile access technology with battery and power-efficient connectivity. The smart coordinator will send such medical information to infrastructure while controlling reliability, QoS, cyber-security and privacy.

4.4 Smart coordinator high-level description

4.4.0 General information smart coordinator high-level description

SmartBAN complemented with the smart coordinator, enables the vertical for healthcare and well-being through mobile health monitoring and personalized delivery applications.

Such personal data, which may be medical data, is sensitive and private and requires a high degree of reliability and privacy in transporting and storing such data.

The smart coordinator will play a significant part in advancing this area of development.

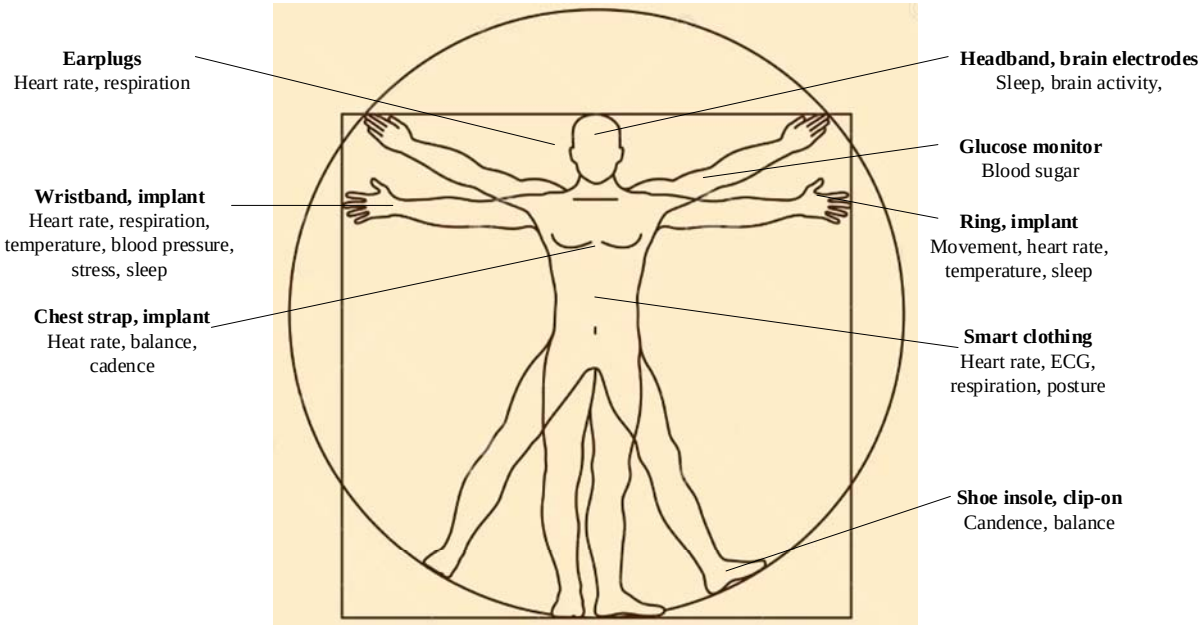


Figure 2: Wearables in SmartBAN

4.4.1 KPIs

Key Performance Indicators (KPIs) for reliability include but are not limited to, packet delivery ratio, end-to-end latency, traffic priority, QoS, security level, and resilience to interference.

Figure 3: SmartBAN connection to infrastructure

The smart coordinator targets low-latency applications with high reliability. The main techniques introduced in SmartBAN to achieve these performance targets are short MAC frames and fast channel access.

4.4.2 New technologies

In addition, the smart coordinator may employ new techniques:

- The SmartBAN service may be dynamically split between execution in the edge or as part of the smart coordinator.
- The SmartBAN radio interface may be implemented in the Software Defined Radio (SDR) platform, which can be used to implement the MAC interface in software as well. Hence, beyond the extension of the traditional connectivity architecture into a variety of SmartBAN subnetworks, it is expected advances in slicing and virtualization between the smart coordinator and infrastructure. Slices can be highly specialized, potentially with separate software stacks in each slice for different functional treatments of the communication flows into modular micro-services that can be flexibly composed into slice-specific implementations as shown in Figure 4.

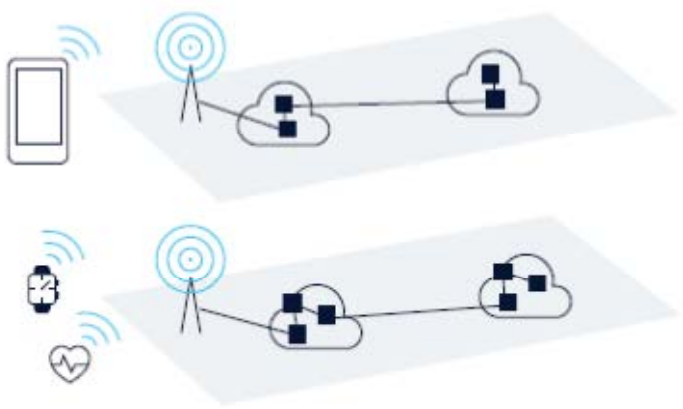


Figure 4: Slide virtualization concept

For example, one slice may specialize in gaming or social network service, incorporating specific optimizations. Similarly, low-throughput Internet of Things (IoT) slices can incorporate functions allowing connectionless access, while other slices are based on a traditional access approach:

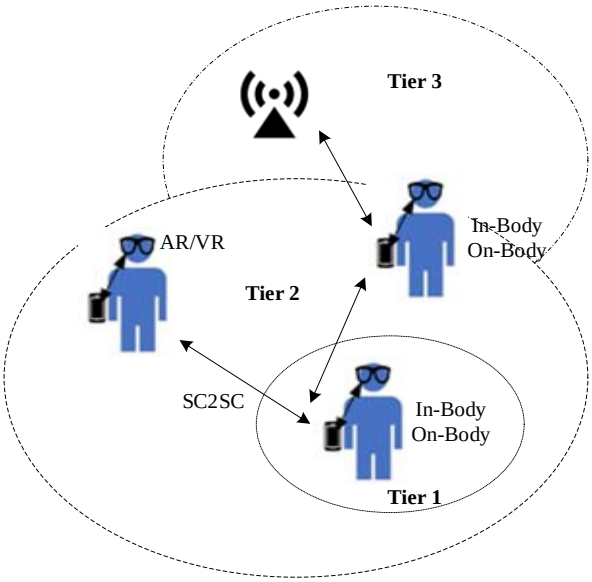
- The smart coordinator is used as a bridge to connect to the infrastructure. Also, it may employ new architecture techniques, such as Time-Sensitive Networking (TSN), to support dependable QoS across networks.
- Hence, the SC offers support for other communication interfaces at L2. In the case of Bluetooth, a study case will be evaluated at the application layer because it is an isolated ad hoc piconet.

The smart coordinator may interact with suitable infrastructure via a bridge at the link layer to facilitate the setup, operation, and maintenance of deterministic traffic and latency. For example, a TSN domain.

4.5 SmartBAN generic architecture

Figure 7 shows the generic architecture of SmartBAN. Three tiers form the SmartBAN configuration. A person with wearables forms Tier 1 following the SmartBAN configuration as specified by ETSI TS 103 325 [i.1] and ETSI TS 103 326 [i.2]. A set of persons with a SmartBAN form Tier 2, where the recent introduction of hub-to-hub functionality assists coexistence among SmartBANs, is currently under development [i.3].

Bridging SmartBANs to infrastructure, i.e. 5G, 6G, Wi-Fi™, or TSN domain forms Tier 3, as shown in Figure 5. The smart coordinator will specify the functionalities for operation in Tier 2 and Tier 3.



NOTE: SC-to-SC (SC2SC), Augmented Reality/Virtual Reality (AR/VR).

Figure 5: SmartBAN configurations

The SmartBAN hub and the smart coordinator are functionally two separate layer entities. As such, the smart coordinator may be implemented in the protocol stack as the Smart Coordinator Link Control (SCLC) layer and part of the link layer (see clause 4.6) or as a separate bridge device for legacy SmartBAN devices, as shown in Figure 6 and Figure 7, respectively.

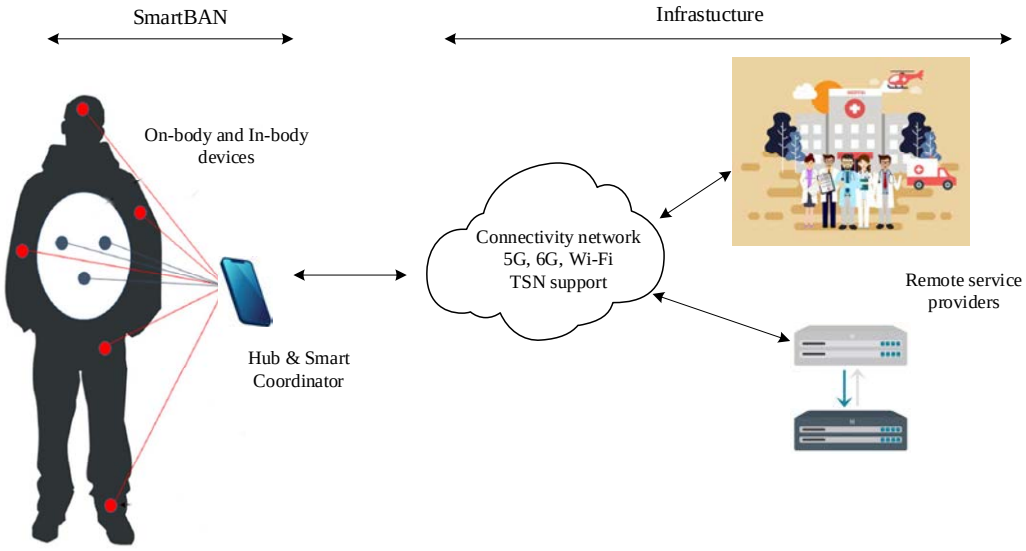


Figure 6: Smart coordinator concept in a SmartBAN generic service architecture

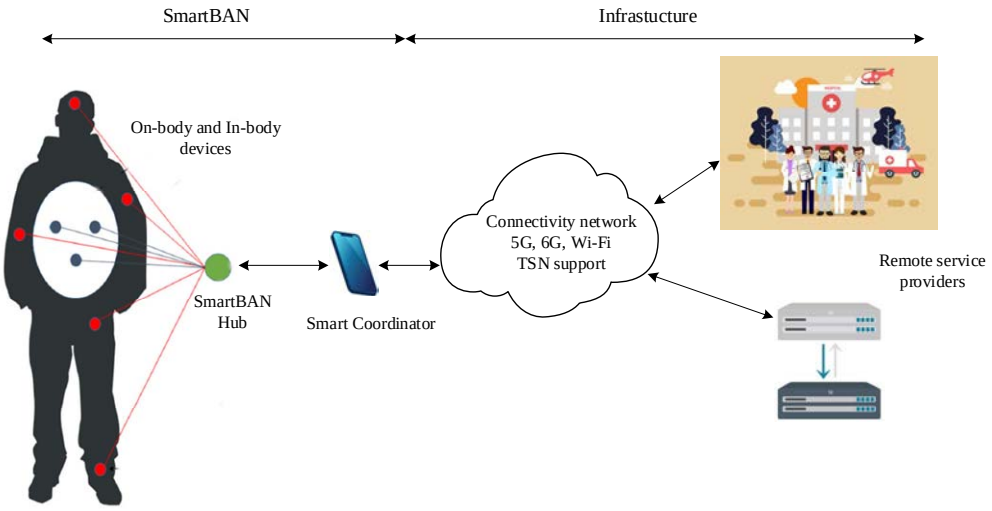


Figure 7: Smart coordinator concept in legacy mode

4.6 Reference model

Figure 8 illustrates the user plane and control plane protocol stack for the smart coordinator. The Smart Coordinator Link Control (SCLC) layer operates in the link layer (L2), offering support for the network layer and bridge operation to infrastructure via the convergence interface.

For other acronyms, see clause 3.3.

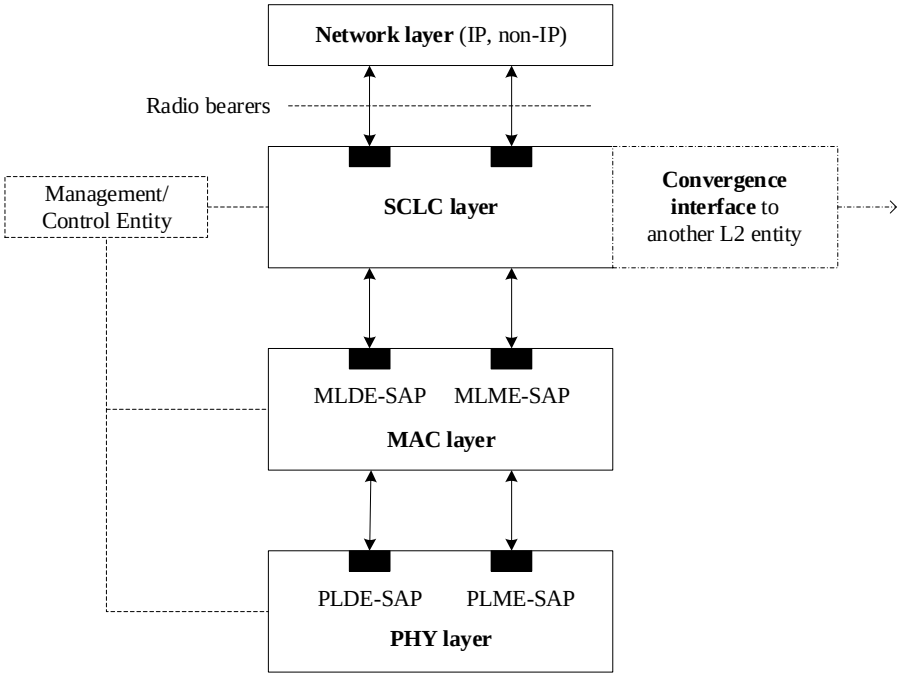


Figure 8: Reference model for smart coordinator protocol stack

4.7 Control management

Mechanisms to control and manage the resources required to set up an environment with several SmartBANs currently under study.

- Resource allocation management.
- Admission control and cyber-security.
- Spectrum sharing and interference management.
- Link monitoring.

The smart coordinator enables control and optimization of SmartBAN elements and resources at the edge, as shown in Figure 9.

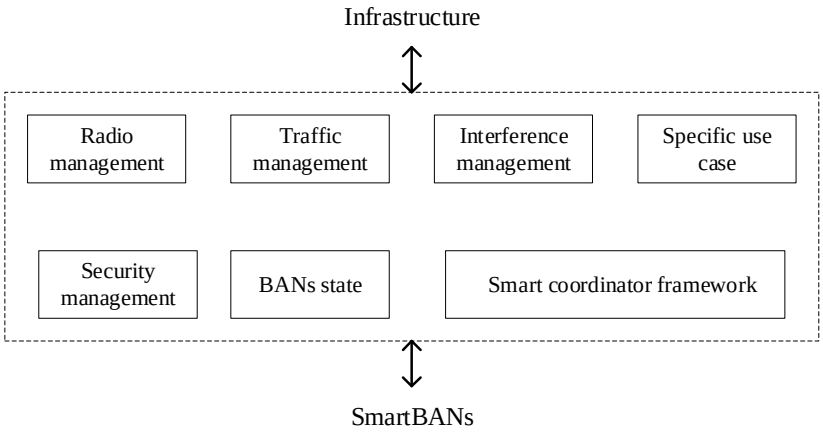


Figure 9: Supported services at the edge

4.8 Coexistence

Unwanted emissions define interference from coordinated or uncoordinated sources operating in the 2,4 GHz ISM band.

In the context of non-intentional interference, such interference induced on a single receiver is due to the transmission from multiple radio interfaces using the same frequency band. Hence, a sub-division is as follows:

Uncoordinated interference: when such radio interferences operate independently of each other. For example, radio interfaces from other SmartBAN ad hoc networks within range and other wireless systems using the same frequency band.

Coordinated interference: when there is a managed spectrum. Adjacent Channel Interference (ACI), or out-of-band emissions, is the interference induced between radio interfaces using adjacent frequency bands. ACI is part of intra-interference, and a spectral mask should have been specified to mitigate its effect.

A subject of further study is a dynamic frequency management system via smart coordinators.

Intentional interference, better known as jamming, and ACI are out of scope:

- The smart coordinator may support the functionality to control the transmit power to minimize interference to other systems and power consumption.
- The smart coordinator may support the functionality to mitigate interference from other wireless systems operating in the ISM band.
- In the case of a smart coordinator operating in coordination with other smart coordinators, such configuration may support the functionality to control and mitigate interference, as indicated above.

5 Cyber-security and privacy protection

5.1 Introduction

Securing the communication and control links in SmartBAN is challenging as wearables have limited computing capacity and power consumption. Moreover, it runs in an ad hoc manner with limited access to infrastructure. Hence, the security protocol should work in a distributed manner with limited access to a Public Key Infrastructure (PKI) for digital certificate management.

As applications with wearables become more ubiquitous, which likely incorporate access to infrastructure, the integration of security provisions is of paramount importance. Indeed, by combining SmartBAN with cloud services via the cellular network or Wi-Fi, the possibility of cyber-attacks increases with every unsecured communication link. Cyber criminals would have more incentives to perform cyber-attacks.

Moreover, a malicious hacker may do considerable damage by taking control of a sensitive actuator like an insulin pump or manipulating or simply overhearing the health indicators sent to a remote service provider.

Data protection includes modern cyber-security for the confidentiality of data, integrity of data, and authentication of all different entities. Key management includes the generation of cryptographic keys based on elliptic-curve cryptography and physical-layer security, and Authenticated Key Exchange (AKE) based on a zero-knowledge procedure.

Encryption and decryption are based on Authenticated Encryption with Associated Data (AEAD) with stream or block cipher.

Privacy protection: payload data at the link layer is protected with strong encryption. Hence, user data and IP addresses are protected. It supplies an important level of privacy protection. However, MAC addresses and metadata in the MAC header may be used to track users. The present document recommends the randomization of MAC addresses. Note that still the payload data decrypted at the link layer and delivered to higher layers requires protections at the application layer. That is out of the scope of the SmartBAN specifications.

5.2 Threat model

The smart coordinator considers cyber-attacks against the cyber-security protocol described below. However, it does not consider tampering with the wearables' hardware. The smart coordinator assumes the implementation of a Hardware Security Module (HSM) for storing cryptographic information and performing cryptographic functions.

An attacker can be active or passive. An active attacker can generate packets or SmartBAN signals and so able to change or alter SmartBAN messages or impersonate an end-user. A passive attacker eavesdrops on the communication session. In practice, the location of a passive attacker is unknown, and its presence is undetected.

Attacks considered in the present document include but are not limited to:

- The integrity of messages: an attacker may alter information in the SmartBAN messages to affect the behaviour of wearables or applications relying on such messages.
- Leakage of confidential information: disclosure of user ID, location, health data, and in general, Personally Identifiable Information (PII) for tracking purposes.
- Denial of Service (DoS): an attacker may want to bring down a SmartBAN network. DoS may include channel jamming or injection of spoof packets or signals to block genuine data traffic.
- Impersonation: an attacker pretends to be a legitimate user by using a false identity.
- Combination of multiple attacks. For instance, if an attacker jams a SmartBAN network, the attacker may try to inject false information.

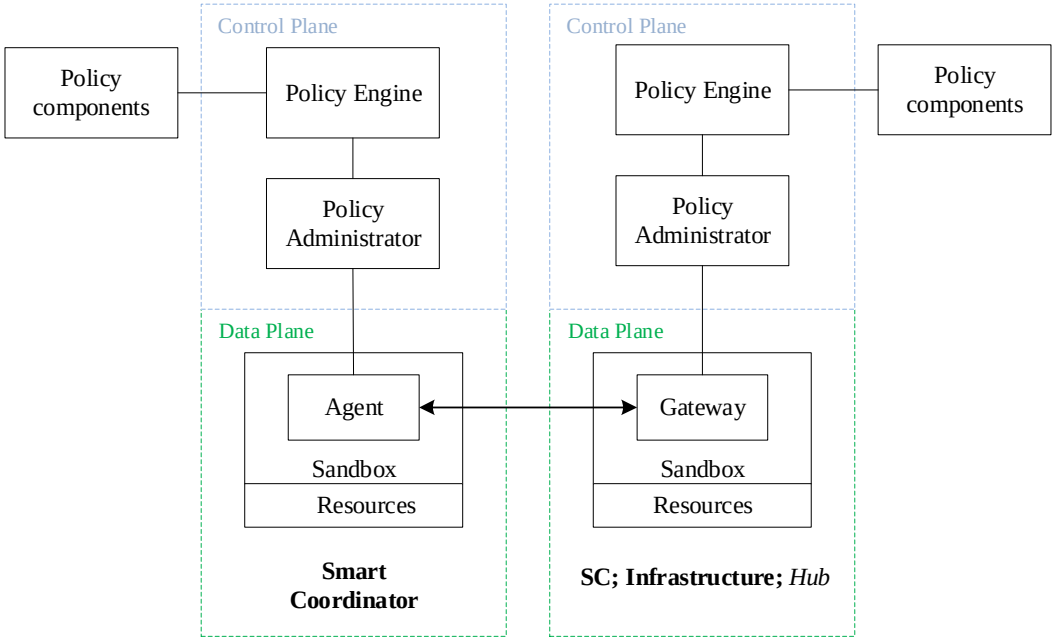
5.3 Security and trust model

5.3.0 General information security and trust model

The security protocol prevents the threats listed above, except for physical threats such as jamming, as follows:

- Mutual entity authentication: Data origin authentication for sender and receiver.
- Mutual explicit key agreement authentication. It is the property obtained when the sender and receiver have the assurance that only the other party knows the negotiated shared key.
- Confidentiality: Encryption with a stream or block cipher protects data information.
- Perfect forward secrecy and future secrecy. The effect of refreshing keys mitigates a compromised key in such a way that past messages (from the time of detection of a compromised key) and future messages (from the time instant of detection of a compromised key) cannot be decrypted.
- Verification of data integrity: Authenticated Encryption with Additional Data (AEAD) protects against data tampering giving assurance of the legitimacy of messages.
- DoS protection: MAC packet filtering supports protection against DoS attacks. When authentication of packets fails, the MAC layer discards them. However, if the attacker has legitimate cryptographic credentials and the certificate is still valid, other mechanisms of DoS control will be required. Those are out of the scope. Also, protection against channel jamming is out of scope.
- Anonymity: The security protocol runs in the L2 of the SmartBAN. Hence, it encrypts the user's information, offering privacy protection against unauthorized observers.
- Distributed control: The security protocol is self-contained in the L2 of the SmartBAN, meaning access to infrastructure is not mandatory. The smart coordinator runs the required key management. Access to a PKI would be desirable for digital certificate management, but it is not a requirement.
- Real-time constraints: The security overhead follows latency constraints.

Authorization policies are based on the Zero-Trust Architecture (ZTA). A subject, asset, or workload is verified by reliable authentication and authorization (access rules) to grant access to resources such as sensors, actuators, hubs, or smart coordinators while minimizing end-to-end latency.



NOTE: Support of a hub is under consideration. Resources are SmartBAN applications, sensors, and actuators.

Figure 10: Zero-trust architecture for Smart Coordinator interacting with other SC or infrastructure

The zero-trust model aims for protection for a wide range of issues related to trustworthiness, cyber-security, and privacy within the context of SmartBAN.

It supports regulatory aspects, i.e. European privacy laws, and addresses cyber-security and privacy issues exposed on social media. Hence, derived from societal concerns and regulatory frameworks, trustworthiness is a necessary area of development for the success and broad market adoption of SmartBAN applications and being an enabler of Health Informatics as described in the Introduction.

Consequently, to mitigate undesirable outcomes or incorrect insights, the zero-trust model leverages proven approaches from other technologies dealing with predictive outcomes, namely the use of a risk-based approach. A risk management framework is required to balance performance and risk mitigation.

Such balance is a form of quality model that encompasses functional safety, objectives, and approaches for SmartBAN applications, and transparency taxonomy of SmartBAN applications.

5.3.1 SmartBAN ontology

The taxonomy formalizes the hierarchical relationships among concepts and specifies the term to be used to refer to each. It prescribes structure and terminology. The taxonomy of SmartBAN will be based on the semantic ontology specified in ETSI TS 103 378 [i.4]. The semantic ontology identifies and distinguishes concepts and their relationship to SmartBAN services.

5.4 Low-power radio interface

SmartBAN applications depend on the deployment of low-power technologies that make use of constrained wireless networks such as SmartBAN.

Power consumption in constrained wireless networks is limited. Moreover, transmitting, receiving, and listening use more energy than the energy required for signal processing. The radio interface is a more limiting factor than CPU power due to bandwidth, latency, duty-cycle, and overall energy consumption.

SmartBAN operates in the unlicensed spectrum that is not characterized by fixed-sized frames. The effects of large messages may have a significant impact on time and energy consumption.

SmartBAN is characterized by small frame sizes with low or moderate transmission data rates. Devices are designed with low power consumption so that battery-powered devices can be deployed with inexpensive batteries for years.

Large payload sizes may lead to unacceptable completion times due to fragmentation into many frames and long waiting times between frames in case of retransmissions. Consequently, in SmartBAN networks, the signal processing energy consumption is typically almost negligible compared to the energy consumption for the radio interfaces (transmitting, receiving, and listening) and for sensor measurement.

Hence, the principal factor to reduce power consumption is to transmit bytes or frames as low as possible. Keeping the number of bytes or frames low is also essential for low latency and efficient use of the radio spectrum to support a large number of devices operating in the ad hoc network.

5.5 Cryptography in SmartBAN

The power consumption for symmetric cryptography is negligible in devices using radio interfaces, as the power consumption is several orders of magnitudes lower than the power for transmission, receiving, and listening. Such symmetric cryptography elements include: the block cipher Advanced Encryption Standard (AES), Secure Hash Algorithm (SHA-3), stream cipher, and other cryptographic primitives. However, the increased processing in terms of time and energy consumption, may be a concern for large key sizes.

On the other hand, the power consumption for asymmetric cryptography such as Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) or Edwards-curve Digital Signature Algorithm (EdDSA) is typically within the same order of magnitude as actively transmitting or receiving a message.

Consequently, the most crucial factor for power consumption and battery lifetime in SmartBAN is the size of the messages and the number of message exchanges required for a secure handshake during association or session key refreshment.

A direct consequence is the use of Elliptic Curve Cryptography (ECC) as it is proven to be robust against theoretical and practical attacks, has a fast implementation, and produces small key sizes as compared to other techniques for medium or elevated levels of security.

Another consequence is the design of a lightweight Authenticated Key Exchange (AKE) protocol with as small messages as possible.

5.6 Authenticated Key Exchange protocol with one Diffie Hellman key exchange combined with digital signature and proof of knowledge of discrete logarithm

The trust model is based on the verification of a digital certificate with a trusted authority repository, deployed in a Public Key Infrastructure (PKI).

Hence, it requires connectivity to such repository. To speed up the procedure, devices do not verify constantly such digital certificates. In other scenarios, such connectivity is not available. Hence, the protocol has two ways to verify authentication: when there is connectivity to a Trusted authority, and when such connectivity is not available or used.

When devices establish association, the selected cipher suite may use the same or different Elliptic Curve (EC) parameters than in the digital certificate.

After a successful Authenticated Key Exchange (AKE), Alice and Bob will share the same symmetric session key, and both will generate long-term keys, whose valid period will depend on the authorization policies. The protocol provides authentication via a Trusted authority, whose digital certificate may be mandated for vendors, or via a zero-knowledge proof.

NOTE: The AKE protocol does not require the knowledge of the digital certificates of the opposite party beforehand.

After a successful run of the protocol, both parties are authenticated and share the same symmetric key for the encryption and decryption of messages at the link layer. The AKE protocol employs state-the-art security primitives for a block or stream cipher with authenticated data mode, nonces, key derivation function, digital signature, and zero knowledge.

5.7 Ratchet-based key refreshing

The following protocol will refresh either the symmetric session key, long-term keys, or both. It assumes a successful run of the AKE protocol such that Alice and Bob share the same symmetric session key, and both have generated long-term keys. Hence, if the communication session suffers interruptions, there is no need to establish a secure channel again. Moreover, in case of a key is compromised, the protocol mitigates the attack by supporting perfect forward secrecy and future secrecy.

6 Smart coordinator data plane architecture

6.1 Smart coordinator data service

6.1.0 General information smart coordinator data service

The smart coordinator data plane architecture is shown in Figure 11 for transmission.

6.1.1 Higher layers

6.1.1.0 General information higher layers

Concerning the OSI model as reference, higher layers mean the entities above the link layer (L2), including the network layer (L3).

6.1.1.1 Infrastructure Security Access Entity & L3

From Figure 11, the Smart Coordinator may be linked to infrastructure via a bridge or to an application in a smart device (smartphone, tablet) worn by a person. Hence, information data to be transmitted is coming from infrastructure or an application within a SmartBAN network (top blocks of Figure 11). In case there is an information flow from infrastructure (connectivity to the Internet via 5G/6G or Wi-Fi), there is a Security Access Entity that grants the Smart Coordinator access to the cellular network (edge or core network) or the Internet via a Wi-Fi Access Point (AP) in L2.

6.1.1.2 L3 Protocol discriminator

The next block in Figure 11 is the first operation in L2 over the information data coming from applications either relying on SmartBAN's PHY and MAC or from infrastructure. L3 provides the information data encapsulated into the MAC frame payload known as MAC Service Data Unit (MSDU). The MAC layer adds a MAC header and MAC footer to form the MAC frame known as MAC Protocol Data Unit (MPDU).

The L3 Protocol discriminator identifies the network layer protocol that encapsulates MSDUs via an Ethertype value in the MAC header. Such protocol discriminator will be used at the receiving side to multiplex MSDU's payload to the corresponding network protocol.

6.1.1.3 Bridge convergence function

The bridge convergence function provides an instance of the Internal Sublayer Service (ISS) (to be specified) to upper layers, connecting the Smart coordinator through an instance of the MAC Service Access Point (MAC-SAP) (to be specified). The bridge convergence function is an interface to exchange MSDUs between a bridge and the SmartBAN MAC. The Smart Coordinator may provide link metrics for the use of external path selection protocols such as spanning tree protocol.

6.1.1.4 Infrastructure Controlled & Uncontrolled access filtering

Access to infrastructure is granted after an exchange of specific messages related to the security entity protocol. Those messages are exchanged using the Uncontrolled Port (U). On the other hand, all data traffic passes through the Controlled Port (C). The Controlled/Uncontrolled access filtering discards any received MSDU if the Controlled Port is not enabled and if the MSDU does not represent an infrastructure security access frame. Note that once the Controlled Port is enabled, the instance of the ISS to upper layers in the Bridge Convergence Function connects the Smart Coordinator with an instance of the MAC-SAP.

6.1.1.5 TX MSDU rate limiting.

MAC layer should perform rate limiting to enforce the resource utilization limit.

6.1.1.6 TX Aggregation A-MSDU

Frame aggregation increases throughput by sending multiple MSDUs in a single transmission. It reduces overhead, as multiple MAC frames can be sent with a single PHY frame.

6.1.1.7 Sequence number assignment

Every MSDU gets a sequence number assignment to avoid replay attacks.

6.1.1.8 TX Fragmentation

Fragmentation is used to improve the performance in terms of PER in situations where there is significant interference, noise, or long distances between nodes. It does this by dividing larger frames into smaller fragments, which increases the probability of successful data transfer. However, fragmentation increases overhead and latency and thus decreases throughput and channel utilization.

6.1.1.9 MPDU number assignment

Every MPDU gets a sequence number assignment to avoid replay attacks.

6.1.1.10 MPDU Payload Encryption

According to the security suite, the Smart coordinator applies authenticated encryption to the MPDU payload (MSDU).

6.1.1.11 Append MPDU Header & CRC

The MAC later adds a MAC header and MAC footer or Cyclic Redundancy Check (CRC) to the encrypted MPDU payload to form a MAC frame.

6.1.1.12 TX Aggregation A-MPDU

Multiple MPDUs are bundled together to create an aggregate MPDU (a-MPDU) to be transmitted in a single PHY frame. The Smart coordinator may support more than one SmartBAN. Hence, one scenario is the potential aggregation of MPDUs from different SmartBANs to be transmitted by a single PHY frame by the Smart Coordinator's radio interface.

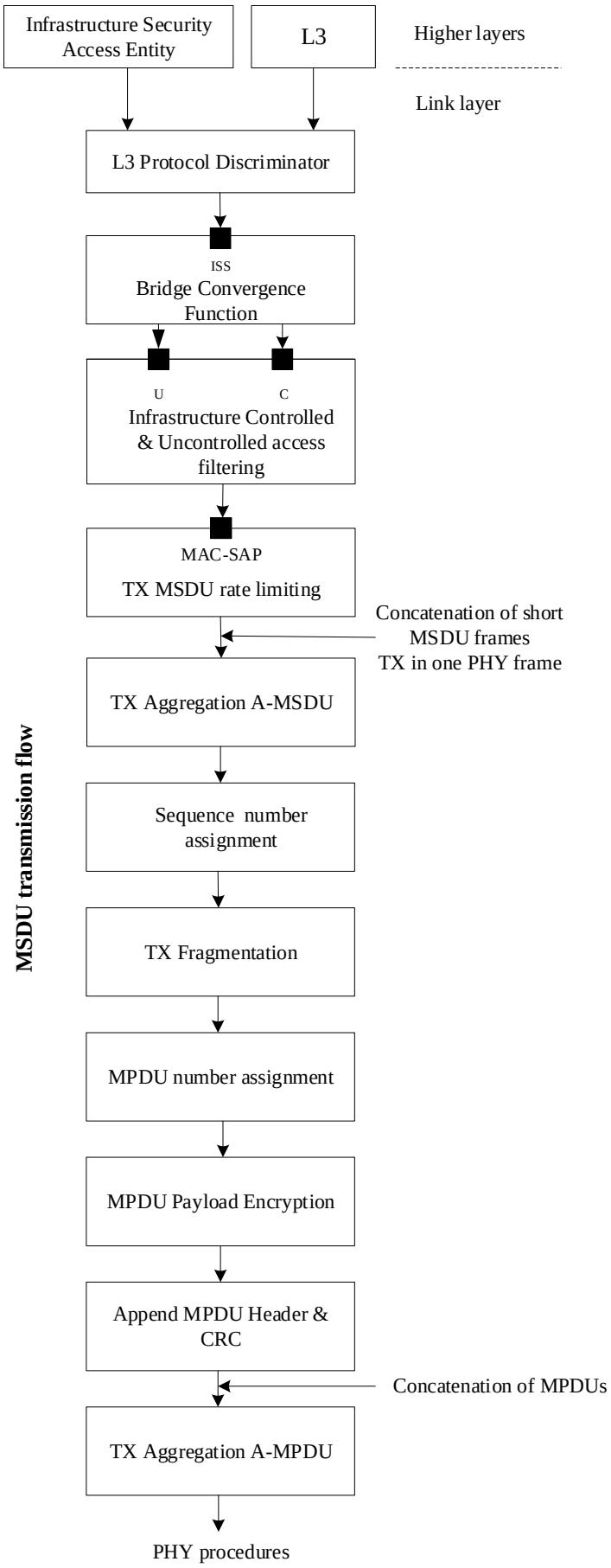


Figure 11: Smart coordinator data plane architecture: transmission flow from the top

Annex A (informative): Change history

Date	Version	Notes
21/12/2022	0.0.1	Release of an early draft
01/06/2023	0.0.2	Update on early draft
21/08/2023	1.1.0	Release of final draft for public inquiry
10/10/2023	1.1.1	Editorial review

Annex B (informative): Bibliography

ETSI TR 103 621: "Guide to Cyber Security for Consumer Internet of Things".

ETSI TR 103 719: "Guide to Identity-Based Cryptography".

ETSI TS 103 645: "CYBER; Cyber Security for Consumer Internet of Things".

History

Document history		
V1.1.1	November 2023	Publication