



Security And Interoperability in Next Generation PPDR Communication Infrastructures



Project Number: 313296

Deliverable 5.2

PPDR Security Architecture, end-to-end security, privacy mechanisms and intrusion detection approach - Intermediate

Scope	Scheduled deliverable
Lead Beneficiary	Instituto de Telecomunicações (IT)
Dissemination level	Public
Document creation date	03/Nov/2014
Document release date	15/Jan/2015
Contractual Date of Delivery	30/Nov/2014
Version	1.3
Status	Final

Abstract: Deliverable 5.2 describes the SALUS Security and Privacy Architecture between existing and next generation PPDR networks, considering possible roadmaps for the evolution of PPDR networks. It identifies the Security and Privacy Architecture components, its interfaces and interactions. This deliverable also provides details on the SALUS approach for secure handovers, secure wireless multi-hop networks, secure wireless body area networks, including location privacy, intrusion detection and physical layer security.

**This deliverable includes a RESTREIT UE Annex which contains information that was classified as security sensitive.*

AUTHORS

Name	Organisation	Email
Hugo Marques	IT	hugo.marques@av.it.pt
Jonathan Rodriguez	IT	jonathan@av.it.pt
Luís Pereira	IT	luis.pereira@av.it.pt
Konstantia Barbatsalou	ONE	tbarbatsalou@gmail.com
Bruno Sousa	ONE	bmsousa@onesource.pt
David Jelenc	UL	david.jelenc@fri.uni-lj.si
Denis Trček	UL	denis.trcek@fri.uni-lj.si
Jernej Kos	UL	jernej.kos@fri.uni-lj.si
Rick Hofstede	UTWENTE	r.j.hofstede@utwente.nl
Nuwan Weerasinghe	KU	nuwan.weerasinghe@kingston.ac.uk
Alexandros Ladas	KU	a.ladas@kingston.ac.uk
Vitaly Petrov	UBITEL	vit.petrov@gmail.com
Evgeny Kucheryavy	UBITEL	y.koucheryavy@ubitel.ru
Panagiotis Galiotos	UPAT	pgaliot@gmail.com
Dragan Olcan	UB	olcan@etf.rs
Branko Kolundzija	UB	kol@etf.rs
Aleksandra Krneta	UB	krneta@etf.rs

QUALITY ASSURANCE TEAM

Name	Organisation	Email
Manfred Blaha	PSCE	manfred.blaha@gmx.net
Jérôme Brouet	ALU-I	jerome.brouet@alcatel-lucent.com

EXECUTIVE SUMMARY

This document describes the components and interfaces for the interim SALUS Security and Privacy Architecture considering possible roadmaps for the evolution of PPDR networks. This description also includes interim solutions for security services such as security extensions for seamless mobility, end-to-end security and privacy support for interoperable PPDR communication systems, techniques for flow based intrusion detection - including forensics -, wireless sensor network security and localization privacy. Since SALUS also deals with security at the physical layer, this deliverable also describes the current achievements on propagation modelling for wireless communication channels.

This document is two-fold:

- SALUS Deliverable 5.2 (this document) [Public];
- Annex to Deliverable 5.2 (a separate document) [RESTREINT UE].

The public Deliverable 5.2 is organized as follows:

Section 1 presents the medium and long-term PPDR operating scenarios, which are grouped in three main phases/migration scenarios: phase 1 – non-mission critical cooperation with commercial LTE, phase 2 – PPDR organisations as mobile virtual network operators and phase 3 – PPDR organisations as owners of broadband (LTE) network;

Section 2 presents the SALUS Security and Privacy Architecture which identifies components, interfaces and services needed to assure integrity, confidentiality, authentication, intrusion detection and location privacy for PPDR communications over the SALUS platform;

Section 3 describes the SALUS security approaches for secure handovers between LTE and Wi-Fi networks, secure wireless body area networks, intrusion detection and security at the physical layer, which mainly focus on modelling the wireless channel in crowd environments towards a reliable communication channel;

Section 4 presents the concluding remarks and next steps.

The RESTREIN UE annex to Deliverable 5.2 contains information that has been considered security sensitive, its structure of section numbering is following the numbering of the main document and it is organized as follows:

Section 3.2 describes the SALUS approach for the secure routing for wireless multi-hop networks which will allow the rapid deployment of a secure mobile ad hoc network in scenarios where the communication infrastructure is unavailable;

Section 3.3 describes the proposed SALUS intrusion detection system architecture and the integrated mobile forensics module.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
TABLE OF CONTENTS	4
TABLE OF FIGURES	6
1 MEDIUM AND LONG-TERM PPDR OPERATING SCENARIOS.....	7
1.1 Migration roadmap: phase 1 – Non-mission critical cooperation with commercial LTE .	7
1.2 Migration roadmap: phase 2 – PPDR organizations as Full LTE Mobile Virtual Network Operators.....	8
1.3 Migration roadmap: phase 3 – PPDR organizations as owners of broadband (LTE) network.....	9
2 SALUS SECURITY AND PRIVACY ARCHITECTURE	10
2.1 Authentication and Authorization Centre (AAuC).....	15
2.1.1 Description	15
2.1.2 Security related interfaces and relation with other components	15
2.2 AAuC Proxy	17
2.2.1 Description	17
2.2.2 Security related interfaces and relation with other components	17
2.3 Mobility Management Entity (MME).....	17
2.3.1 Description	17
2.3.2 Security related interfaces and relation with other components	18
2.4 CCC Security Gateway	18
2.4.1 Description	18
2.4.2 Security related interfaces and relation with other components	18
2.5 3GPP AAA Server.....	19
2.5.1 Description	19
2.5.2 Security related interfaces and relation with other components	20
2.6 Intrusion Detection System (IDS)	20
2.6.1 Description	20
2.6.2 Security related interfaces and relation with other components	21
2.7 Message Broker	22
2.7.1 A general overview.....	22
2.7.2 Data channel.....	23
2.7.3 Control channel.....	23
2.7.4 Security related interfaces and relation with other components	24
2.8 Wi-Fi Security Gateway.....	25
2.8.1 Description	25
2.8.2 Security related interfaces and relation with other components	25
3 SALUS SECURITY APPROACHES	27
3.1 Secure handovers	27
3.1.1 Media Independent Handovers (MIH).....	27

3.1.2	Inter-technology handovers with MIH proactive authentication	32
3.2	Secure routing for wireless multi-hop networks	36
3.3	Secure wireless body area networks	36
3.3.1	Communication between PPDR terminals and the back-end applications	37
3.3.2	Communication between PPDR terminals and the body worn sensors	37
3.3.3	Location privacy	38
3.4	Intrusion Detection System approach	39
3.4.1	IDS Architecture - level 0	42
3.4.2	IDS Architecture - level 1	42
3.4.3	PPDR forensics	42
3.5	Security at physical layer: electromagnetic modelling of wireless channel for scenarios with human crowds	42
3.5.1	Brief overview of the used electromagnetic analysis	42
3.5.2	Developed methodology for efficient modeling of human crowds	42
3.5.3	Modeling example: WBAN channel in the presence of human crowds	44
3.5.4	Human crowd	46
3.5.5	Future research	47
4	CONCLUDING REMARKS	49
	BIBLIOGRAPHY	50
	ACRONYMS	53

TABLE OF FIGURES

Figure 1 – Scenario for migration roadmap: phase 1	7
Figure 2 – Scenario for migration roadmap: phase 2	8
Figure 3 – Scenario for migration roadmap: phase 3	9
Figure 4 – SALUS Security and Privacy Architecture (interim release)*	14
Figure 5 – AAuC interfaces	15
Figure 6 – AAuC Proxy interfaces	17
Figure 7 – SALUS related MME interfaces	18
Figure 8 – CCC Security GW interfaces	19
Figure 9 – SALUS related 3GPP AAA interfaces	20
Figure 10 – IDS interfaces	21
Figure 11 – Structure of the data channel message	23
Figure 12 – Structure of the control message	23
Figure 13 – Message Broker interfaces	24
Figure 14 – Wi-Fi Security Gateway interfaces	25
Figure 15 – MIH protocol frame [28].	27
Figure 16 – MIH Protocol Header (based on [29]).	27
Figure 17 – TLS message flow for a full handshake.	28
Figure 18 – MIHS PDU during TLS handshake (based on [29]).	29
Figure 19 – MIHS PDU in existence of MIH SA by TLS (based on [29]).	29
Figure 20 – Protocol Stack of service Access Authentication (with an EAP Server) [29].	30
Figure 21 – MIH Protocol Frame protected by EAP-generated SA.	31
Figure 22 – MIH protection through layer 2.	31
Figure 23 – MIH protection through IPsec.	32
Figure 24 – IPsec authentication mechanism according with network configuration.	32
Figure 25 – MIH proactive authentication architecture (example).	33
Figure 26 – Protocol Stack for MIH Supported Proactive Authentication (based on [29]).	33
Figure 27 – Unbundled media access proactive authentication.	34
Figure 28 – Bundled media access proactive authentication.	35
Figure 29 – Simplified message sequence chart for a proactive authentication signalling related to a secure handover between LTE and Wi-Fi (adapted from [29])	35
Figure 30 – An overview of the sensor-based application communication pathways.	36
Figure 31 - IDS classification methods	39
Figure 32 – Hybrid IDS Architecture	42
Figure 33 – Quadrilateral models of a human body, male and female	43
Figure 34 – Model of densely packed human crowd with each figure having different posture .	43
Figure 35 – Intensity of electric field in the vicinity of a human alone.	44
Figure 36 – Intensity of electric field with the presence of human crowd.	44
Figure 37 – Human body model with position of antennas (blue dots) and highlights (red arrows) for those antennas selected for comparison.	45
Figure 38 - Single human: comparison of s-parameters for horizontally placed antennas.	45
Figure 39 - Single human: comparison of s-parameters for vertically placed antennas.	45
Figure 40 - Model of human group with uniform spatial distribution.	46
Figure 41 - Model of human group with stochastic spatial distribution.	46
Figure 42 - Uniform crowd: comparison of s-parameters for horizontally placed antennas.	47
Figure 43 - Uniform crowd: comparison of s-parameters for vertically placed antennas.	47
Figure 44 - Stochastic crowd: comparison of s-parameters for horizontally placed antennas. ..	47
Figure 45 - Stochastic crowd: comparison of s-parameters for vertically placed antennas.	47
Figure 46 - WBAN man down situation.	48
Figure 47 - In-crowd mobile device to base station communication.	48
Figure 48 – Device-to-device wireless communication within crowd.	48

1 MEDIUM AND LONG-TERM PPDR OPERATING SCENARIOS

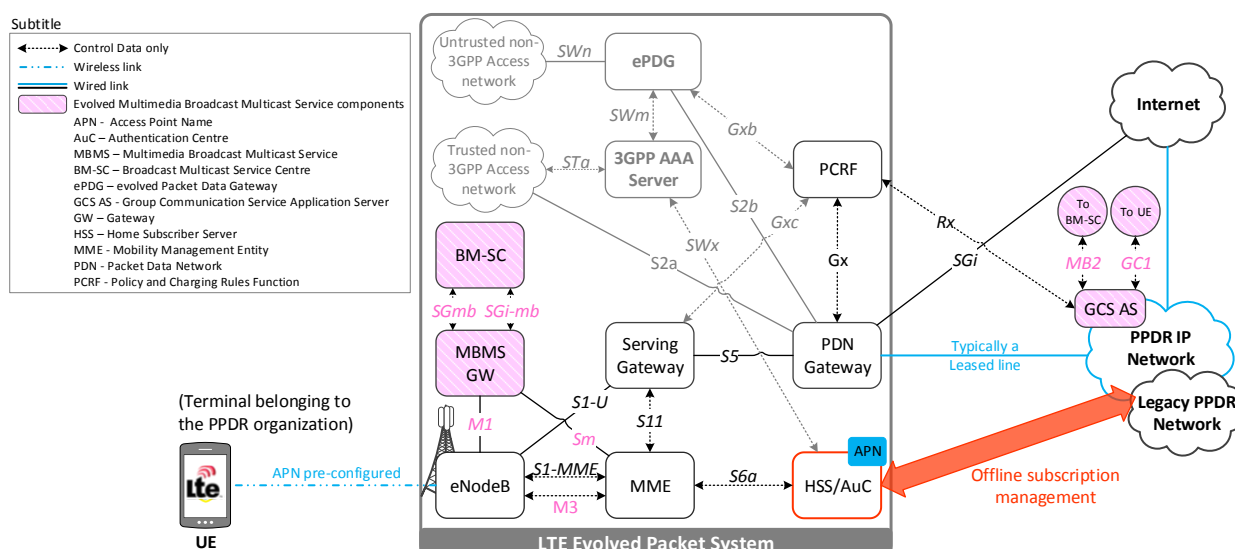
The design of the **SALUS Security and Privacy Architecture** takes into consideration that multiple phases may exist when migrating existing PPDR networks from simple cooperation with LTE commercial operators, for non-mission critical interworking, towards a full mission critical LTE owned or shared network. In fact SALUS considers the case in which current PPDR technologies and LTE coexist for a long period of time. References [1]-[9] are valuable to understand the future evolution of PPDR communications. SALUS Deliverable 4.3 (Business Analysis – Intermediate), to be released in SALUS month 18 (February 2015) provides additional details on possible migration roadmaps.

1.1 Migration roadmap: phase 1 – Non-mission critical cooperation with commercial LTE

Phase 1 considers the case where LTE connectivity is available through the use of a separate device (LTE subscription needed), mainly for high-speed data access and non-mission critical communications. All mission-critical communications are still performed using legacy PPDR systems (such as TETRA and TETRAPOL). Under this scenario PPDR organizations must have established:

- a commercial contract with the LTE operator that would specify a (dedicated) *Access Point Name* (APN) to which the LTE terminals can connect;
- a dedicated IP connectivity link (typically a leased line) from the LTE core network to the private PPDR network;
- (optionally) a dedicated Group Communication Service Application Server (GCS AS) on the private PPDR network for non-mission-critical communications;
- A separate channel for the management of the LTE subscriptions.

This concept, which already considers the enablers to support group communication services using Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access, is illustrated in Figure 1, below.



In Phase 1 it is important to note that:

- legacy PPDR networks are expected to be converted (medium term) into all-IP network at the transport level between the terrestrial components;
- a separate mobile terminal (user equipment) for LTE access is needed;

- Page 8 of 58

2 SALUS SECURITY AND PRIVACY ARCHITECTURE

The **SALUS Security and Privacy Architecture** identifies components, interfaces and services needed to assure integrity, confidentiality, authentication, intrusion detection and location privacy for PPDR communications over the SALUS platform. The overall high-level view of the (interim) SALUS Security and Privacy Architecture is depicted in Figure 4 below. Table 1 pre-identifies the majority of the components from the overall System Architecture (to be released in SALUS Deliverable 3.2 on SALUS month 21 (may 2015), which are needed to understand the SALUS Security and Privacy Architecture.

Following sub-sections will further describe, for each security component, its purpose and interfaces with other components.

Table 1 – SALUS System Architecture components, functionalities and interfaces (short description)

Item name	Short description
3GPP AAA Server	(LTE) Provides authentication, authorization, policy control and routing information to packet gateways. More information can be found in section 2.5.
AAuC	Authorization and Authentication Centre. The AAuC is responsible for the authentication and authorization of all PPDR devices for a specific domain. The AAuC also plays the role of Certification Authority. More information can be found in section 2.1
AAuC Proxy	Is responsible for local authentication on Wi-Fi infrastructure or ad hoc network when the connection to the AAuC is not available (also known as offline authentication). More information can be found in section 2.2.
AP	(Wi-Fi) Access Point.
BM-SC	(LTE) Broadcast Multicast Service Centre. It provides a set of functions for MBMS (see below) user services. The BM-SC authorises/keeps record of user specific MBMS multicast service activation (specific groups for which the user participates).
BS	(TETRA/TETRAPOL) Base Station.
CCC Security Gateway	The Command and Control Centre (CCC) Security Gateway operates as router/firewall and VPN end-point. It controls access to the CCC services through context based (dynamic) access control lists. It is also the end-point for all IPSec communications (tunnels) established with the CCC. More information can be found in section 2.4.
DMO	(TETRA/TETRAPOL) Direct Mode Operation. Communication between mobile radio units without using the TETRA/TETRAPOL infrastructure.
DNC	(TETRAPOL) Data Network Controller. The DNC is equipped with routing functions, laying on IP protocol over a LAN connection.
Drone Surveillance	Drones provide video and sensor data mounted on moving platforms such as micro Unmanned Aerial Vehicle (UAVs) or Unmanned Ground Vehicles (UGVs).
eNodeB	(LTE) is a logical node responsible for radio transmission / reception in one or more cells to/from the UE (also commonly called as LTE base station).

ePDG	(LTE) Evolved Packet Data Gateway.
FIGO MN	The Mobile Node of FIGO (Wi-Fi, LTE) combines multiple LTE/UMTS/HSPA radios and multiple Wi-Fi radios to provide multi-interface point-of-attachment communication – actually expanding communications coverage.
GCS AS	Group Communication Service Application Server. It is a component of the 3GPP enablers to support group communication services using EUTRAN Access. The GCS AS is responsible to transfer application signalling and for delivering application data (e.g. media data) to a group of UEs.
Gi	(TETRA) The reference point between an IP Backbone and an external IP packet data network.
Gn	(TETRA) Optional interface between SwMI and GGSN within the same TETRA network.
GGSN	(TETRA) Gateway GPRS Support Node (defined in EN 301 344).
Group Management	Entity responsible for the management of group communications (TETRA / TETRAPOL / LTE / Wi-Fi). It enrolls/unrolls users to specific groups.
HDB	(TETRA) Home DataBase. A database that comprises information about subscribers
HSS/AuC	(LTE) Home Subscriber Server/Authentication Centre is a database that contains user-related and subscriber-related information. It also provides support functions in: ▪ mobility management; ▪ call and session setup; ▪ user authentication and access authorization.
IDS	Intrusion Detection System. The IDS is placed in all networks within the SALUS Security Architecture and features a collection of sub-components that are used for performing intrusion detection. More information can be found in sections 2.6, 3.4. and in the (Restraint UE) Annex to D5.2.
KMC	(TETRAPOL) Key Management Center. It manages the TETRAPOL system security keys.
LTE Dispatcher	Manages the communication of and with LTE User Equipment for PPDR operations in the field.
MBMS	(LTE) Multimedia Broadcast Multicast Service. MBMS is a Single Frequency Network (SFN) service in which the same data is transmitted from a single source entity to multiple recipients via one or more eNodeB using MBMS bearers. Together with the GCS AS and the BM-SC (see above) it enables group communications in E-UTRAN
Message Broker	It aids in communication between PPDR terminals and the back-end applications located within the CCC. Its main task is to route messages that carry body worn sensor readings of PPDR personnel to the back-end applications. More information can be found in section 2.7.
MIH IS	Media Independent Handover Information Services. Provides information to assist handover decisions.
MME	(LTE) Mobility Management Entity. Is the key control-node for the LTE

	access-network. The main security feature is ciphering, integrity and replay protection of NAS signalling.
MN	(Wi-Fi) Mobile Node.
Mobile GCS	Mobile Ground Control Station (GCS). It works as an ergonomic user interface and as a data integration hub between multiple sensors and the CCC, by providing a comprehensive situation picture in complex environments. Through the GCS an operator can control UAVs/UGVs.
Mobile VMS	Mobile Video Management System. This VMS works in a PPDR (command) vehicle and it stores and displays video streams collected from in-vehicle video cameras and/or wearable cameras connected through Wi-Fi to the in-car network. The mobile VMS also uploads the video streams to the VMS running on the CCC.
Mobility Management	The entity that enables seamless connection from the different mobile access methods of the PPDR networks (LTE, TETRA/TETRAPOL, WiFi) to the PPDR core network and external networks to the PPDR network. It includes Mobile Access Gateways (MAGs), Local Mobility Anchor (LMA), a mobility Control Center, Proxy Mobile IP (v4/v6) and a Media Aware Proxy (MAP). More information on the supported mobility functionalities can be found in SALUS Deliverable 6.1 [11].
MS	(TETRA/TETRAPOL) Mobile Station.
MSA	The Media Specific Authenticator (MSA) is an authentication module that runs on the AAuC specific for inter-technology handover operations.
NMS	Network Management System. It allows supervising individual components of the PPDR communication network, within a larger network management framework. It mainly assists with network device discovery, network device monitoring, network performance analysis while also providing intelligent notifications. More information on the NMS can be found in SALUS D6.1 [11].
OMC	(TETRAPOL) Operation and Maintenance Centre.
PCRF	(LTE) Policy and Charging Rules Function – is the entity responsible to determine in real-time the policy rules.
PDN Gateway	(LTE) Packet Data Network Gateway is the point of interconnection between the EPC (Evolved Packet Core) and the external IP networks. The PDN Gateway also performs various functions such as IP address / IP prefix allocation or policy control and charging.
R0	(TETRA) The reference point at the TETRA Air Interface for IP packet data.
ROH LDS	Rohill Line Dispatch Station. It manages the communication of and with TETRA MS for PPDR operations in the field.
SALUS Relay	Routes IP sessions between TETRA and TETRAPOL IP gateways as well as with LTE user equipment.
SALUS TIG	SALUS TETRA-to-IP Gateway. It uses the TETRA Peripheral Equipment Interface (PEI) as specified in the ETSI EN 300 392-5 standard. Amongst others, it allows an external application to control and monitor MS activity, including group selection, call setup, talking party identification, and priority control and monitoring. The information is transferred as asynchronous serial data using the RS-232 standard with a typical bitrate

	of 9.600 bps
SALUS TpIG	SALUS TETRAPOL-to-IP Gateway. Similar to the SALUS TIP, although the PEI interface is not applicable here. In this case, transmitter control and receiver indication is still possible, but the information on talking party, priority control and monitoring, etc. is currently not supported.
Serving Gateway	(LTE) is the point of interconnection between the radio-side and the Evolved Packet Core (EPC). As its name indicates, this gateway serves the UE by routing the incoming and outgoing IP packets. It is the anchor point for the intra-LTE mobility (i.e. in case of handover between eNodeBs) and between LTE and other 3GPP accesses.
Situation Awareness	(Concept) Multi-display arrangement that provides multiple layers of information (object type, positioning, sensor related data, functionality, etc.).
TETRAPOL Dispatcher	Manages the communication of and with TETRAPOL MS for PPDR operations in the field.
TIG	(TETRA) TETRA IP Gateway.
TNG	(TETRA) TETRA Node Gateway.
UE	(LTE) User Equipment.
VMS (CCC)	Video Management System running at the CCC. It stores and displays video streams collected from multiple mobile VMSs. The CCC VMS can also perform remote configuration for the mobile VMSs.
VDB	(TETRA) Visitor Data Base. A database that comprises temporary information about (visiting) subscribers.
Wi-Fi Security Gateway	The Wi-Fi Security Gateway operates as router/firewall, VPN end-point, local IDS and AAuC Proxy. More information can be found on section 2.8.

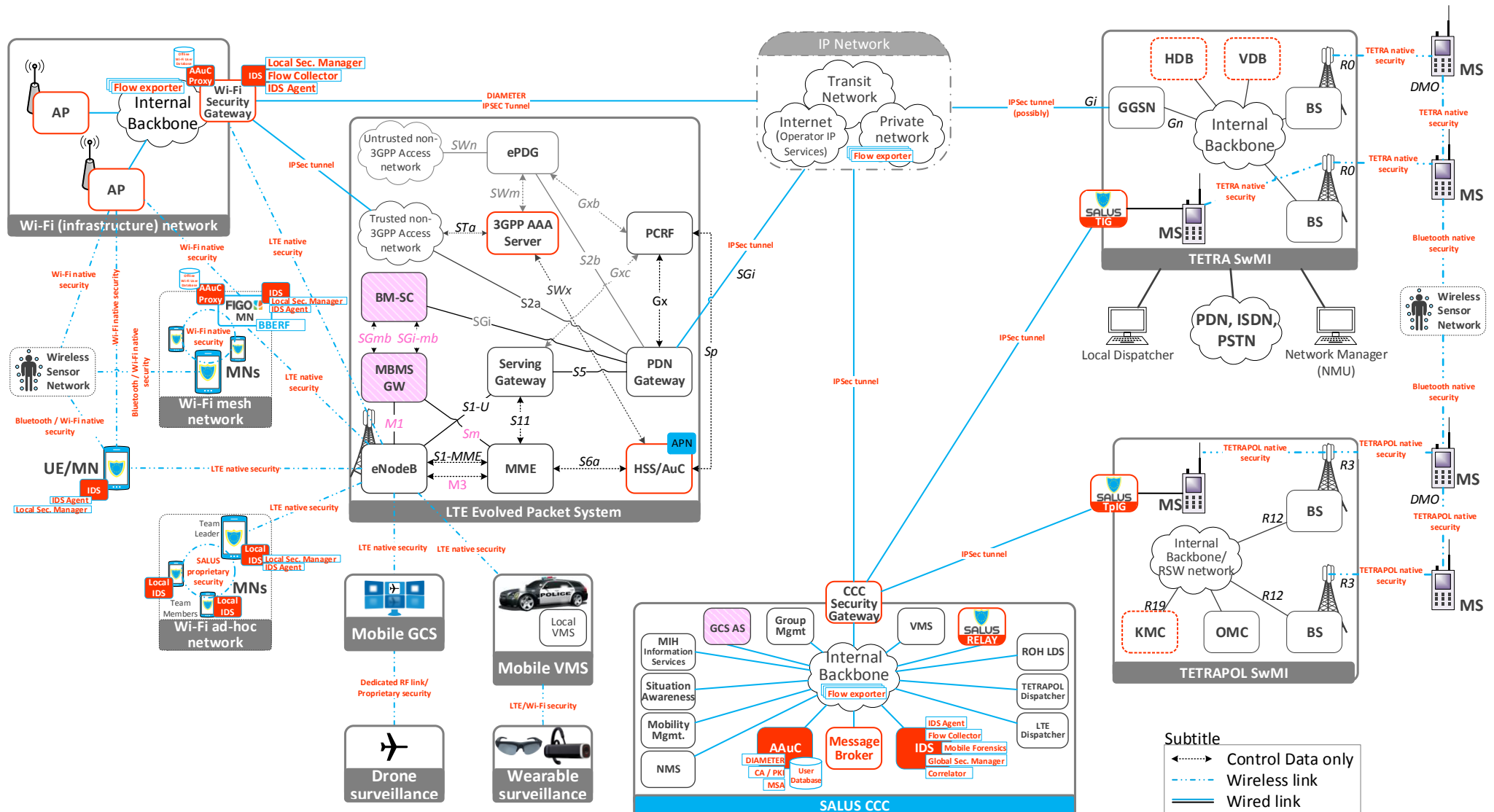


Figure 4 – SALUS Security and Privacy Architecture (interim release)*

*Orange colour depicts security related components/interfaces

The following subsections provide a description of the architecture security components. The description includes its purpose, to which other components (from the System Architecture) it relates, the purpose of that relation and its interfaces towards each of those components.

2.1 Authentication and Authorization Centre (AAuC)

2.1.1 Description

The AAuC is the component responsible for the authentication and authorization of all PPDR devices for a specific domain. At migration roadmap phase 1, the AAuC will only be used for Wi-Fi device authentication and authorization. In subsequent migration roadmap phases (2 and 3) the AAuC will be extended to be the single authentication and authorization centre for the multiple PPDR communication technologies (LTE, TETRA and TETRAPOL and WiFi). The AAuC will hence incorporate similar functions as of the LTE *Home Subscriber Server* (HSS). Transport of authentication and authorization information is done by using the DIAMETER protocol.

The AAuC also implements the functionalities of a Public Key Infrastructure (PKI), allowing LTE UE's, Wi-Fi devices and other network components to request digital certificates and certificate revocation lists.

2.1.2 Security related interfaces and relation with other components

Interaction with the AAuC is done through the interfaces depicted in Figure 5 below.

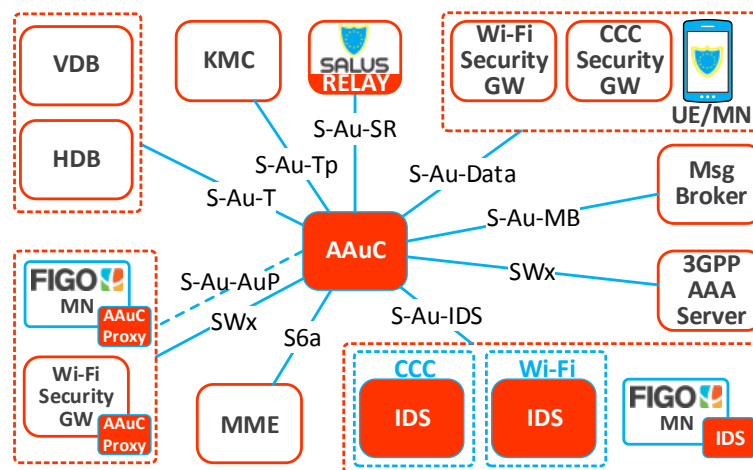


Figure 5 – AAuC interfaces

The purpose of each interface and correspondent interaction is described in Table 2 below.

Table 2 – AauC interactions and services

AAuC interacts with	Interface to use	Purpose of interaction
MME	S6a	It enables transfer of subscription and authentication data for authenticating/authorizing LTE user access to the evolved system (AAA interface) between MME and the AAuC, similar to what is defined in [13]. In migration roadmap phase 2, the AAuC will fulfil the roles of external HSS, as depicted in Figure 2. SALUS also intends the AAuC to use this interface to request the MME to disconnect of a specific device when it is tagged by the IDS as a threat.

UE/MN	S-Au-Data	It is a secure data channel that Security Gateways, UEs (LTE) or MNs (Wi-Fi) use to request digital certificates or certificate revocation lists. These certificates can then later be used for protecting other PPDR communications, for IPsec authentication.
SALUS Relay	S-Au-SR	<i>This interface is yet to be defined. Its purpose is to provide security related profiles for the involved communication parties. Its description will be included in SALUS Deliverable 5.3 (PPDR Security Architecture, end-to-end security, privacy mechanisms and intrusion detection approach – Final).</i>
IDS	S-Au-IDS	This interface enables the IDS to inform the AAuC on a detected intrusion. Based on the threat severity level, the AAuC may initiate the procedures to disconnect/limit the device's/user's activities and capabilities by requesting such action to be taken by the CCC Security Gateway, the MME or the AAuC Proxy. If the intrusion comes from an internal user, the IDS will first attempt to disable the terminal through internal mechanisms (e.g. through the local IDS agent running on the device), potentially followed by disabling it within the network, e.g., by blocking MAC addresses or disabling interfaces.
Message Broker	S-Au-MB	This interface allows the Message Broker to obtain information regarding various authorization policies about forwarding sensor and other messages that are exchanged – via the Message Broker – between PPDR terminals and the back-end applications.
VDB & HDB	S-Au-T	It enables transfer of subscription and authentication data for authenticating/authorizing TETRA local and roaming devices on the AAuC. <i>This is a tentative implementation – it may not be supported in the final security architecture implementation if a simpler approach is found.</i>
KMC	S-Au-Tp	It enables transfer of subscription and authentication data for authenticating/authorizing TETRAPOL local and roaming devices on the AAuC. <i>This is a tentative implementation – it may not be supported in the final security architecture implementation if a simpler approach is found.</i>
FIGO MN AAuC Proxy & Wi-Fi Security GW AAuC Proxy	S-Au-AuP	This is a synchronization interface. It allows synchronizing the AAuC Proxy user database with a specific Wi-Fi user database domain in the AAuC. Such synchronization will allow the AAuC Proxy to locally authenticate the Wi-Fi users when a backbone connection to the AAuC is not available (offline operation). This interface is also used to request the AAuC Proxy to disconnect a specific device when it is tagged by the IDS as a threat.
	SWx	Transport of authentication and connection related data. Similar behaviour as the standardized LTE SWx interface [12]. Typically triggered by the AAuC Proxy to request authentication for a new mobile node who wants to join the Wi-Fi PPDR network. Both the AAuC Proxy and the AAuC use DIAMETER protocol to transport the authentication related data. The AAuC Proxy acts as an authenticator and the AAuC as an authentication server in the IEEE 802.1x nomenclature.
3GPP AAA Server	SWx	Transport of authentication, subscription and PDN connection related data. This corresponds to the behaviour of the standardized LTE SWx interface, as described in [12].

2.2 AAuC Proxy

2.2.1 Description

The AAuC Proxy is the component responsible for local authentication on Wi-Fi infrastructure or ad hoc network when the connection to the AAuC is not available (also known as offline authentication). It supports the same authentication mechanisms as the AAuC, hence the AAuC Proxy's user database is synchronized with a specific Wi-Fi user database domain in the AAuC. Under normal conditions the AAuC Proxy forwards all authentication and authorization requests to the AAuC. If operating in infrastructure mode, authentication and authorization responses from the AAuC are relayed to the Access Point (AP), if operating in ad hoc mode, the AAuC Proxy acts as an authenticator in IEEE 802.1x nomenclature.

2.2.2 Security related interfaces and relation with other components

The AAuC Proxy has two interfaces as depicted in Figure 6 below.

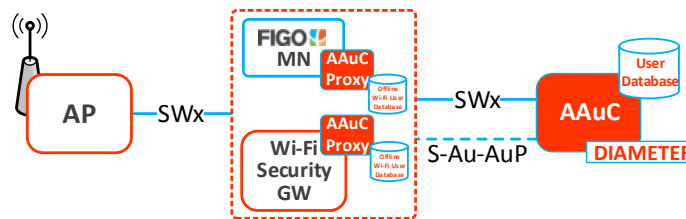


Figure 6 – AAuC Proxy interfaces

The purpose of each interface and correspondent interaction is described in Table 3 below.

Table 3 – AAuC Proxy interactions and services

AAuC Proxy interacts with	Interface to use	Purpose of interaction
AAuC	S-Au-AuP	{Same as described in Table 2} This is a synchronization interface. It allows synchronizing the AAuC Proxy user database with a specific Wi-Fi user database domain in the AAuC. Such synchronization will allow the AAuC Proxy to locally authenticate the Wi-Fi users when a backbone connection to the AAuC is not available (offline operation). This interface is also used to request the AAuC Proxy to disconnect a specific device when it is tagged by the IDS as a threat.
	SWx	{Same as described in Table 2} Transport of authentication and connection related data. Similar behaviour as the standardized LTE SWx interface [12]. Typically triggered by the AAuC Proxy to request authentication for a new mobile node who wants to join the Wi-Fi PPDR network. Both the AAuC Proxy and the AAuC use DIAMETER protocol to transport the authentication related data. The AAuC Proxy acts as an authenticator and the AAuC as an authentication server in the IEEE 802.1x nomenclature.
AP	SWx	It enables the AP to treat the AAuC Proxy as an authentication server. Its operation is similar to the SWx as described in Table 2.

2.3 Mobility Management Entity (MME)

2.3.1 Description

The MME is not a security exclusive component, being also responsible for UEs' mobility management. Its operation is defined in 3GPP TS 23.401[13]. From the security point of view it

basically sits between the UE and the HSS (in LTE the UE has no direct connection with the HSS). For LTE enabled PPDR devices, the MME is responsible to derive (in conjunction with the UE) the keys for integrity and confidentiality protection of the signalling. The MME also provides the eNodeB which serves as the UE point-of-attachment (PoA) with the KeNB, a master key used by the eNodeB to protect the air interface with this specific UE - as explained in SALUS D5.1 [14], section 1.7.

In SALUS migration roadmap phase 2 (see Figure 2), the MME interacts with an external HSS, which in this case is the AAuC. In phase 3 the AAuC and the HSS operate as a single entity.

2.3.2 Security related interfaces and relation with other components

The AAuC Proxy has two interfaces as depicted in Figure 7 below.

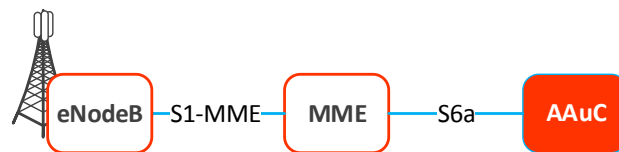


Figure 7 – SALUS related MME interfaces

The purpose of each interface and correspondent interaction is described in Table 4 below.

Table 4 – MME interactions and services

MME interacts with	Interface to use	Purpose of interaction
AAuC	S6a	{Same as described in Table 2} It enables transfer of subscription and authentication data for authenticating/authorizing LTE user access to the evolved system (AAA interface) between MME and the AAuC, similar to what is defined in [13]. In migration roadmap phase 2, the AAuC will fulfil the roles of external HSS, as depicted in Figure 2. SALUS also intends the AAuC to use this interface to request the MME to disconnect of a specific device when it is tagged by the IDS as a threat.
eNodeB	S1-MME	It enables the eNodeB to forward UEs' <i>Attach Request</i> messages to the MME – these are normally contained in a S1-MME control message. Upon receiving this control message, the MME triggers the authentication procedure with the UE, through the eNodeB. The S1-MME interface is specified in [13].

2.4 CCC Security Gateway

2.4.1 Description

The Command and Control Center (CCC) Security Gateway operates as router/firewall and VPN end-point. It controls access to the CCC services through context based (dynamic) access control lists. It is also the end-point for all IPsec communications (tunnels) established with the CCC.

2.4.2 Security related interfaces and relation with other components

The CCC Security Gateway has three interfaces as depicted in Figure 8 below.

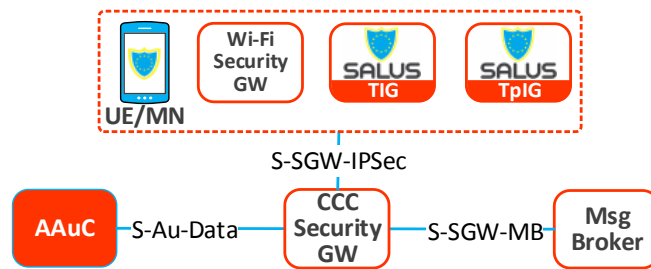


Figure 8 – CCC Security GW interfaces

The purpose of each interface and correspondent interaction is described in Table 5 below.

Table 5 – CCC Security GW interactions and services

CCC Security Gateway interacts with	Interface to use	Purpose of interaction
AAuC	S-Au-Data	{Same as described in Table 2} It is a secure data channel that Security Gateways, UEs (LTE) or MNs (Wi-Fi) use to request digital certificates or certificate revocation lists. These certificates can then later be used for protecting other PPDR communications, for IPsec authentication.
UE/MN & Wi-Fi Security Gateway & SALUS TIG & SALUS TpiG	S-SGW-IPSEC	It enables the establishment of IPsec tunnels between CCC Security Gateway and: - the Wi-Fi Security Gateway; - the UE/MN; - The SALUS TIG; - The SALUS TpiG. This approach optimizes the number of IPsec security associations to be supported by each entity, since a single IPsec tunnel can be established with the CCC Security Gateway to protect traffic from multiple applications or devices. This approach can also optimize the number of IPsec security associations needed to protect the traffic related with other Wi-Fi components, such as the traffic between the AAuC proxy and the AAuC, amongst others.
Msg. Broker	S-SGW-MB	It enables the Message Broker to query the CCC Security Gateway for active IPsec sessions for a specific MN/UE, allowing it to authenticate messages.

2.5 3GPP AAA Server

2.5.1 Description

The 3GPP Authentication, Authorization and Accounting (AAA) server is used by LTE network providers to perform authentication and authorization to users who access the LTE core through a non 3GPP access network (typically Wi-Fi), as depicted in Figure 4. There is an intrinsic relation between the 3GPP AAA server and the HSS since the HSS contains a subscriber and authentication credential database required for the 3GPP subscribers to access the WLAN interworking service.

In migration roadmap phases 2 and 3, the 3GPP AAA Server must contain an interface to the AAuC, as depicted in Figure 2 and Figure 3.

2.5.2 Security related interfaces and relation with other components

For the scope of the SALUS Security and Privacy Architecture, the 3GPP AAA Server interfaces depicted in Figure 9 are relevant.

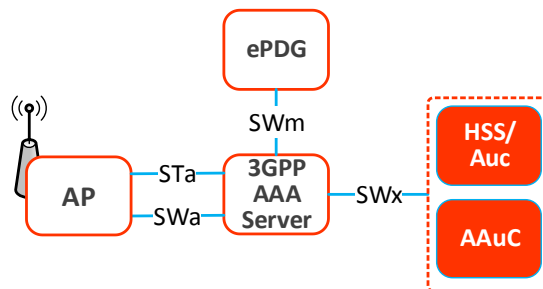


Figure 9 – SALUS related 3GPP AAA interfaces

The purpose of each interface and correspondent interaction is described in Table 6 below.

Table 6 – 3GPP AAA Server and services

3GPP AAA Server interacts with	Interface to use	Purpose of interaction
AP	STa	This corresponds to the standardized LTE STa interface [12]. It is used when the Wi-Fi network is considered a trusted non-3GPP IP network. It enables the AP to connect with the 3GPP AAA Server and transports access authentication, authorization and charging-related information in a secure manner.
AP	SWa	This corresponds to the standardized LTE SWa interface [12]. It is used when the Wi-Fi network is considered an untrusted non-3GPP IP network. It enables the AP to connect with the 3GPP AAA Server and transports access authentication, authorization and charging-related information in a secure manner.
ePDG	SWm	This corresponds to the standardized LTE SWm interface [12]. It is used for Authentication, Authorization, and Accounting (AAA) interactions between the ePDG and the 3GPP AAA Server. In this case the ePDG fulfils either the role of Mobile Access Gateway (MAG) or the role of Local Mobility Anchor (LMA) in a Proxy Mobile IPv6 (PMIPv6) Domain.
HSS/AuC & AAuC	SWx	<i>{Same as described in Table 2}</i> Transport of authentication, subscription and PDN connection related data. This corresponds to the behaviour of the standardized LTE SWx interface, as described in [12].

2.6 Intrusion Detection System (IDS)

2.6.1 Description

The IDS component is implemented in all networks within the SALUS Security Architecture and features a collection of sub-components that are used for performing intrusion detection. All IDS blocks feature at least an IDS agent, responsible for performing the detection of intrusions, and a Security Manager that takes care of receiving incident reports by one or more agents within its working domain (e.g., the Wi-Fi network and the internal backbone). All the local Security

Managers automatically send their incident reports to the global Security Manager that is present within the CCC.

2.6.2 Security related interfaces and relation with other components

The IDS interfaces are depicted in Figure 10 below.

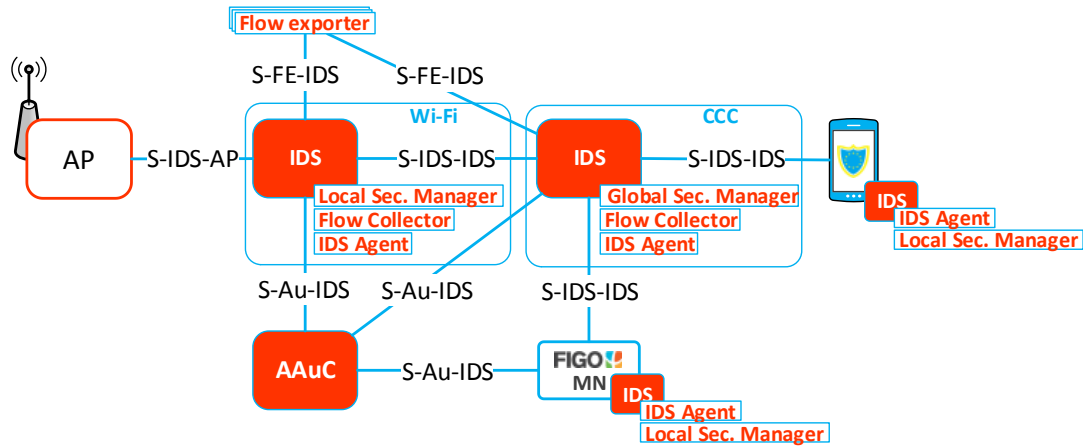


Figure 10 – IDS interfaces

The purpose of each interface and correspondent interaction is described in Table 7 below.

Table 7 – IDS interactions and services

IDS Security Manager interacts with	Interface to use	Purpose of interaction
AAuC	S-Au-IDS	<i>{Same as described in Table 2}</i> This interface enables the IDS to inform the AAuC on a detected intrusion. Based on the threat severity level, the AAuC may initiate the procedures to disconnect/limit the device's/user's activities and capabilities by requesting such action to be taken by the CCC Security Gateway, the MME or the AAuC Proxy. If the intrusion comes from an internal user, the IDS will first attempt to disable the terminal through internal mechanisms (e.g. through the local IDS agent running on the device), potentially followed by disabling it within the network, e.g., by blocking MAC addresses or disabling interfaces.
AP	S-IDS-AP	This interface enables the (Wi-Fi) IDS to request the AP to disassociate a specific MN.
(Wi-Fi) IDS & (FIGO MN) IDS	S-FE-IDS	This interface is used by enabled routers (or dedicated probes) to export traffic flow characteristics to flow collectors using NetFlow/IPFIX. This data is then further analysed by the IDS agent and incidents are shared with the Local/Global Security Manager. In addition, the interface is used by the IDSs to instruct the packet forwarding device running the flow exporter to block or reroute certain traffic, if necessary.
(Wi-Fi) IDS & (FIGO MN) IDS	S-IDS-IDS	The Local Security Managers share the reported incidents with the Global Security Manager (part of the CCC), such that there is one

MN) IDS		entity in the network that has a complete overview of all incidents. This will allow for taking preventive measures against attackers in a domain where the attacker was not active yet (e.g., malware present on handhelds may be blocked in the core network preventively, even before the core network's IDS has detected the malware by itself).
---------	--	--

2.7 Message Broker

The Message Broker is a network element that aids in communication between terminals that are carried by the PPDR personnel including body-worn sensors, and the computer programs, usually (but not necessarily) located within the CCC, called back-end applications. The most common use case of the Message Broker is to route messages that carry body worn sensor readings of PPDR personnel to the back-end applications. First, PPDR UE act as local data collectors, and then, at given intervals (push approach) or on demand (pull approach), send readings – via the Message Broker – to the back-end apps that process, visualise or store them. Note, however, that the direction in which messages flow is not fixed and the Message Broker can also be used to send any type of messages from one UE to another or between back-end applications, or from back-end application to the UEs. Because of this, we will denote PPDR UEs and back-end applications with the term “entities”.

This following section provides a high-level overview of the Message Broker and its security mechanisms that ensure the protection of the exchanged messages.

2.7.1 A general overview

The problem that is addressed by the Message Broker is the establishment of connection and the exchange of messages between a dynamic number of UEs and back-end applications. In this context, three issues need to be resolved:

- Device and application discovery. A mechanism enabling entities to learn the presence and addresses of each other is needed; UE/MNs, in particular, may change their network addresses and if the communication is to be asynchronous and bi-directional, this requires a discovery and (preferably) simple addressing mechanism.
- Unified message transportation mechanism. A unified approach to transfer messages in all directions is needed; otherwise every entity would need to provide its own mechanisms for sending and receiving messages which does not scale.
- Unified security approach. Similarly, a unified approach to secure messages is needed; otherwise every entity would need to provide its own security solutions.

The Message Broker addresses these problems by acting as an application level router. It operates on a well-known network address and accepts connections from terminals and back-end applications. Once connections have been established, the Message Broker acts as an intermediary that receives messages from one entity and forwards them to another.

An important aspect of the Message Broker is its addressing mechanism – a mechanism by which PPDR UE and applications address each other. While all entities will have IP addresses, they will not address each other by IP addresses, but rather by the entities' *identities*. An identity is simply a unique identifier that represents a single PPDR UE or a back-end application. The mapping between identities and the IP addresses is an inherently internal matter of the Message Broker; it is dynamically constructed at runtime. The concept of identities allows entities to address each other independently of the assigned IP addresses. While the procedure to create identities has not been completely defined, the general approach will be based on deriving the identity of a device from its security credentials. For instance, a hash of a device's public key seems to be a good candidate, because it is derived from the credentials that are issued by the PPDR organizations and it produces unique identities (at least with sufficient probability).

The Message Broker provides two communication channels: a data channel and a control channel. The data channel carries data messages: messages that contain sensor readings or similar type of *business logic* content. The control channel, analogously, carries control messages: messages that contain instructions, for instance, for changing settings on terminals and similar. While the data channel would usually flow from terminals to back-end applications and the control channel from back-end applications to terminals, these directions are not fixed: any entity can send any message – via the Message Broker – to any other.

2.7.2 Data channel

In the data channel, messages are distributed in a publish-subscribe pattern. Before each message is sent out, the sender tags it with a *topic*. Topic is simply a label that describes the originator and the content of the message. For instance, if a PPDR terminal is sending status updates, then such messages – containing location coordinates and the information about the well-being of the PPDR personnel – are tagged with *identity#status_update* topic. The idea is that a single topic describes the whole stream of messages; for instance all status updates of a given PPDR operative. The topic thus contains two pieces of information: the identity of the sender, and the tag of the content. The figure below demonstrates the structure of the data messages.



Figure 11 –Structure of the data channel message

The topic encodes the identity of the sender and the tag of content that is carried in the payload of the message. While the size and the format of the topic are fixed, the size, content and the format of the payload are application specific.

Entities can be configured to receive messages from a given topic. Once the user subscribes the entity, the Message Broker will forward all messages tagged with that topic to it. The data channel thus offers an application layer multicast mechanism: a single message sent by one entity will get replicated by the Message Broker and sent to all interested, that is subscribed, receivers.

2.7.3 Control channel

The control channel is used for sending and receiving control messages. These messages will mainly flow from back-end applications to the PPDR terminals and will be used for changing various configuration settings on the terminals but, as with the data channel, the message exchange direction is not fixed and a control message may be sent from any entity to any other.

The main difference between the data channel and the control channel is in the number of intended recipients and in the way how the recipients are addressed. While the publish-subscribe pattern of the data channel can send a message from a single publisher to many subscribers, the control channel can only transfer a single message from a single sender to a single recipient (support for multiple recipients of the same control information which may help in scaling up the Message Broker equipment are yet to be considered). And while the recipients in the data channel are addressed implicitly – the topic of the message and the set of active subscriptions determines the set of recipients – here the sender needs to determine the recipient explicitly; a control message has to include the identity of the recipient. Control messages may thus be simple asynchronous and self-contained notification messages or they may represent request and response messages in the remote procedure call protocol. The figure that represents the content of the control messages is given below.



Figure 12 – Structure of the control message

The identity of the sender, the identity of the recipient, the type of the message and its unique identification number are of fixed length and format, while the size, the contents and the format of the payload are application specific.

2.7.4 Security related interfaces and relation with other components

On the data channel, the Message Broker must ensure that publishers are allowed to send messages and the subscribers are allowed to receive them. Such rules or policies depend on the topic; for a given topic, each publisher needs to be allowed to send messages and each subscriber needs to be allowed to receive them. When sending messages on the control channel, the Message Broker must ensure that this sender is allowed to send that particular control message to this specific recipient. To perform these types of authorization checks, the Message Broker needs to interface the AAuC server as depicted in Figure 13. Communication between each PPDR terminal and the Message Broker is first protected by technology specific (layer 2) mechanisms and later by IPsec (at layer 3) (tunnel ending at the CCC gateway). IPsec uses encryption algorithms, digital signatures, key exchange algorithms, and hashing functions which, when the correct algorithms are chosen, provide strong authentication, integrity and encryption mechanisms. Because the IPsec session is not established between the PPDR terminal and the Message Broker, but between PPDR terminal and the CCC Security gateway, the Message Broker cannot guarantee that the received message (on any channel) was actually sent by the entity that is listed as sender. In general, any node that can set a valid IPsec session, and thus send messages to the Message Broker, can set the contents of the messages – including the identity of the sender – to an arbitrary value. Thus to prevent sending messages with spoofed sender identities, the Message Broker will query – upon creating a new connection with a UE – the CCC Security gateway to obtain information about the established IPsec session. Based on this information, the Message Broker will be able to determine the authenticity of the sender field.

The Message Broker interfaces are depicted in Figure 13 below.

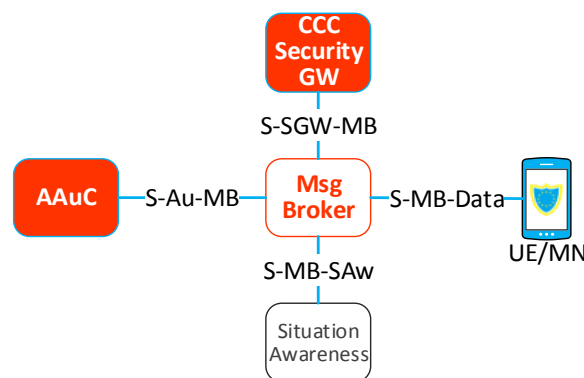


Figure 13 – Message Broker interfaces

The purpose of each interface and correspondent interaction is described in Table 8 below.

Table 8 – Message Broker interactions and services

Message Broker interacts with	Interface to use	Purpose of interaction
AAuC	S-Au-MB	{Same as defined in Table 2} This interface allows the Message Broker to obtain information regarding various authorization policies about forwarding sensor and other messages that are exchanged – via the Message Broker – between PPDR terminals and the back-end applications.

UE/MN	S-MB-Data	This interface enables MNs to send data to the Message Broker. Note, however, that this interface is conceptual; the actual messages will pass through CCC security GW when going from UE/MN to MB.
Situation Awareness	S-MB-SAw	This interface enables the Message Broker to send data to various back-end applications (the situation awareness is provided as an example).
CCC Security GW	S-SGW-MB	{Same as defined in Table 5} It enables the Message Broker to query the CCC Security Gateway for active IPsec sessions for a specific MN/UE, allowing it to authenticate messages

2.8 Wi-Fi Security Gateway

2.8.1 Description

The Wi-Fi Security Gateway operates as router/firewall, VPN end-point, local IDS and AAuC Proxy. As a router/firewall and VPN end point it routes and protects, using IPsec tunnels, communications between the SALUS Wi-Fi domain and the SALUS CCC. It can also block communications per AAuC request. As IDS it collects flows from the flow exporters (other routers in the Wi-Fi backbone infrastructure) and uses the IDS agent to constantly search for intrusions (based on decisions from the Local Security Manager). As an AAuC Proxy, the Wi-Fi Security Gateway can also act as an authentication server when connection to the AAuC (CCC) is lost. In such cases offline authentication is possible at the AAuC.

2.8.2 Security related interfaces and relation with other components

The Wi-Fi Security Gateway interfaces are depicted in Figure 14 below.

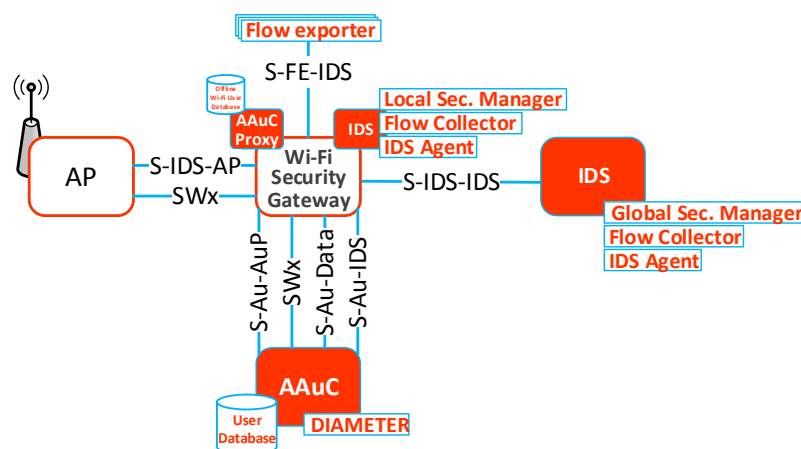


Figure 14 – Wi-Fi Security Gateway interfaces

The purpose of each interface and correspondent interaction is described in Table 9 below.

Table 9 – Wi-Fi Security Gateway interactions and services

Wi-Fi Sec. GW interacts with	Interface to use	Purpose of interaction
AAuC	S-Au-AuP	{Same as defined in Table 2} This is a synchronization interface. It allows synchronizing the AAuC Proxy user database with a specific Wi-Fi user database domain in the AAuC. Such synchronization will allow the AAuC Proxy to locally authenticate the Wi-Fi users when a backbone connection

		to the AAuC is not available (offline operation). This interface is also used to request the AAuC Proxy to disconnect a specific device when it is tagged by the IDS as a threat.
	S-Au-Data	<i>{Same as defined in Table 2}</i> It is a secure data channel that Security Gateways, UEs (LTE) or MNs (Wi-Fi) use to request digital certificates or certificate revocation lists. These certificates can then later be used for protecting other PPDR communications, for IPsec authentication
	S-Au-IDS	<i>{Same as defined in Table 2}</i> This interface enables the IDS to inform the AAuC on a detected intrusion. Based on the threat severity level, the AAuC may initiate the procedures to disconnect/limit the device's/user's activities and capabilities by requesting such action to be taken by the CCC Security Gateway, the MME or the AAuC Proxy. If the intrusion comes from an internal user, the IDS will first attempt to disable the terminal through internal mechanisms (e.g. through the local IDS agent running on the device), potentially followed by disabling it within the network, e.g., by blocking MAC addresses or disabling interfaces.
	SWx	<i>{Same as defined in Table 2}</i>
Flow Exporter	S-FE-IDS	<i>{Same as defined in Table 7}</i> This interface is used by enabled routers (or dedicated probes) to export traffic flow characteristics to flow collectors using NetFlow/IPFIX. This data is then further analysed by the IDS agent and incidents are shared with the Local/Global Security Manager. In addition, the interface is used by the IDSs to instruct the packet forwarding device running the flow exporter to block or reroute certain traffic, if necessary
AP	S-IDS-AP	<i>{Same as defined in Table 7}</i> This interface enables the (Wi-Fi) IDS to request the AP to disassociate a specific MN.
(CCC) IDS	S-IDS-IDS	<i>{Same as defined in Table 7}</i> The Local Security Managers share the reported incidents with the Global Security Manager (part of the CCC), such that there is one entity in the network that has a complete overview of all incidents. This will allow for taking preventive measures against attackers in a domain where the attacker was not active yet (e.g., malware present on handhelds may be blocked in the core network preventively, even before the core network's IDS has detected the malware by itself).

3 SALUS SECURITY APPROACHES

3.1 Secure handovers

This section describes the security features to protect signalling messages during the handover procedures between different technologies – for the scope of this deliverable, handovers between LTE to and from Wi-Fi are considered. This section complements section 5.3 of SALUS Deliverable 6.1 [11].

3.1.1 Media Independent Handovers (MIH)

The Media Independent Handovers (MIH) are standardized in IEEE 802.21-2008 [28]. Its objective is to standardize handovers between different technologies (e.g. IEEE 802.11, LTE, at layer 2). The security related with IEEE 802.21 is described in another document, standard IEEE 802.21a-2012 [29]. This section mainly presents the MIH security features, as described in the IEEE 802.21a standard [29], that are relevant for the SALUS Use Cases (an overview of MIH is provided in Section 5.3 of SALUS Deliverable 6.1 [11]). The following subsections describe the features/mechanisms that can be used within MIH to perform a secure handover between different technologies.

3.1.1.1 MIH protocol frame and protocol header

The following figures are extracted from SALUS D6.1 [11]) and serve for reference only.

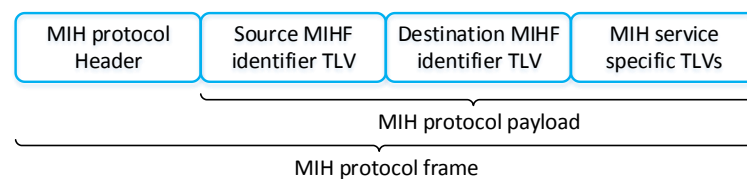


Figure 15 – MIH protocol frame [28].

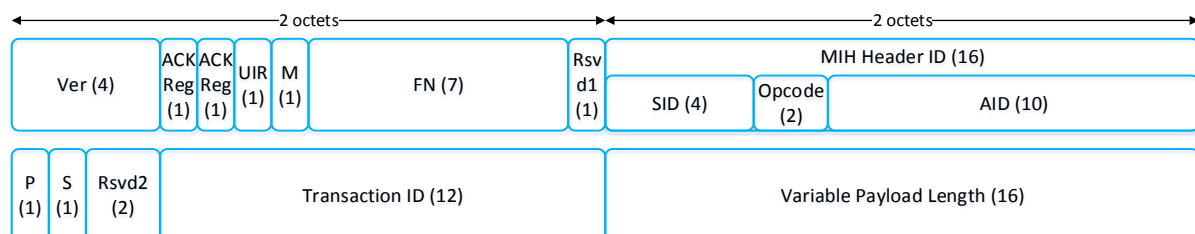


Figure 16 – MIH Protocol Header (based on [29]).

3.1.1.2 MIH security features

The MIH protocol can provide the most important security services:

- Confidentiality: cyphering the MIH service specific TLVs field;
- Integrity protection: using message integrity code field in MIH protocol frame;
- Authentication: by the usage of authentication mechanisms provided by TLS, EAP or IPsec based protocols.

MIH messages can be protected in two different ways:

- Protection at transport protocols: the MIH PDUs can be protected by the transport protocols at two different layers:
 - Layer 2: the protection at this layer can be provided by TKIP and CCMP;
 - Layer 3: in this layer the MIH PDUs may be protected by IPsec;
- Protection at MIH Layer: the MIH PDUs can be protected by MIH specific protection mechanisms at MIH layer.

Note: for the purpose of the SALUS project the protection through IPsec shall be the preferred method. This document currently provides an overview of all methods since the implementation of IPsec is mandatory. The support for IPv6 is mandatory in newer devices and the implementation of MIHF only is supported in the new devices, hence IPsec shall be used to protect MIHF messages. In cases where IPv6 is not supported by one or both devices, then one of the other methods may be chosen.

Protection through MIH Layer

The MIH PDUs can be protected by MIH specific protection mechanisms at MIH layer. This way the protection of MIH messages does not depend on the transport protocols. Standard IEEE 802.21a [29] specifies two mechanisms for a Mobile Node and a Point of Service to negotiate protection mechanisms and establish MIH security associations:

- Extensible Authentication Protocol (EAP) or Extensible Re-authentication Protocol (ERP): may be used where MIH service authentication is needed.
- Transport Layer Security (TLS) or Datagram TLS (DTLS): may be used for establishing the an MIH SA where MIH service access authentication is not required;

A brief description on each protection mechanism is given below.

Protection through TLS (or DTLS)

In the scenarios where MIH service access authentication is not required then a Transport Layer Security (TLS) based authentication can be used to establish the MIH SAs. When the MIH protocol transport is reliable, Transport Layer Security Version 1.2 (TLS) specified in IETF RFC 5246 [30], is used [29]. Otherwise, Datagram Transport Layer Security Version 1.2 (DTLS) specified in IETF RFC 6347 [31] is used [29]. The message flow between two MIHF in order to establish a TLS handshake is depicted in Figure 17.

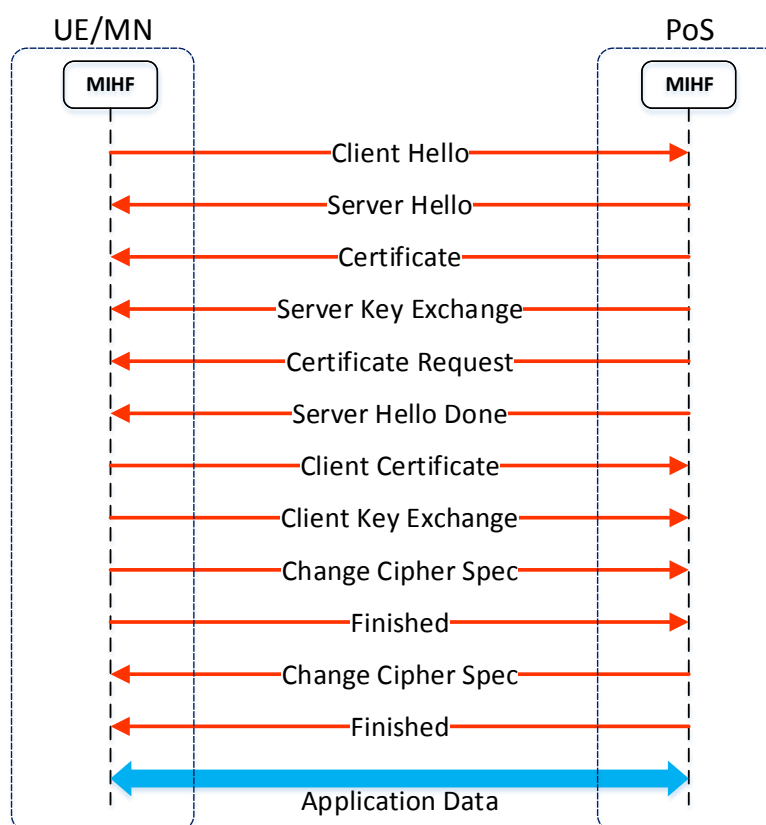


Figure 17 – TLS message flow for a full handshake.

The following considerations apply for the presented message flow:

- Both the UE/MN and PoS support the TLS protocol to establish the MIH SAs;
- Authentication is based on digital certificates;
- Both UE/MN and PoS have digital certificates signed by a trusted Certification Authority (CA);
- Mutual authentication is performed.

Note: TLS supports for other authentication mechanisms (besides the digital certificates approach presented here), and mutual authentication is not mandatory on TLS. A complete description on each message and authentication mechanisms used with TLS can be found in [30].

The TLS messages are exchanged inside the MIH protocol as depicted in Figure 18.

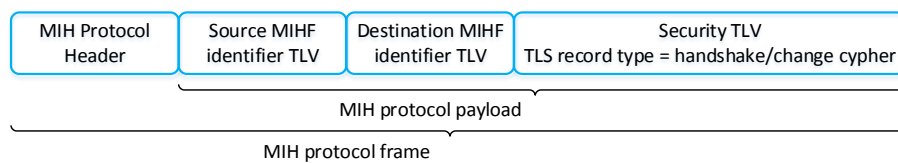


Figure 18 – MIHS PDU during TLS handshake (based on [29]).

After the MIH SA is established, the MIH service specific TLVs are protected by TLS. The TLS record type is inserted in the MIH frame as depicted in Figure 19 below and the message is sent to destination with the “S” bit in the MIH Protocol Header set to “1”. A Security Association Identifier (SAID TLV) is also added to the frame.

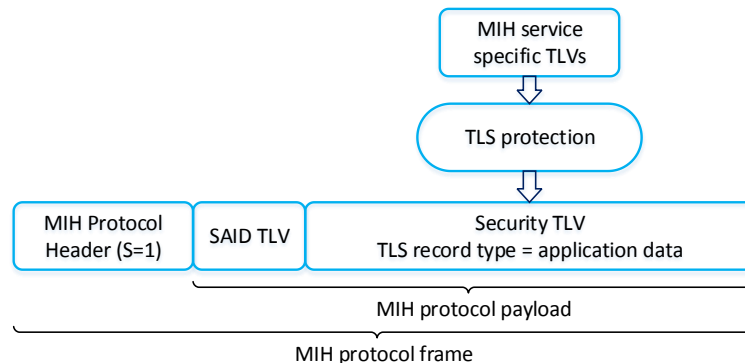


Figure 19 – MIHS PDU in existence of MIH SA by TLS (based on [29]).

Note: when a security association exists and the “S” bit is set to “1”, the MIH frame may not have the Source and Destination identifiers [29].

Protection through EAP (or ERP)

In those scenarios where MIH service authentication is needed and an authentication server is available, the Extensible Authentication Protocol (EAP) based protocol may be used. The EAP protocol is specified in IETF RFC 3748 [33].

After a successful authentication, the MN and the Point-of-Service (PoS) share the same Master Session Key (MSK) that can be derived by the procedures described in IETF RFC 3748 [33]. Based on MSK the MN and the PoS can derive the remaining keys:

- 128 bit Media Independent Authentication Key (MIAC)
- Media Independent Encryption Key (MIEK)
- Media Independent Integrity Key (MIIC)

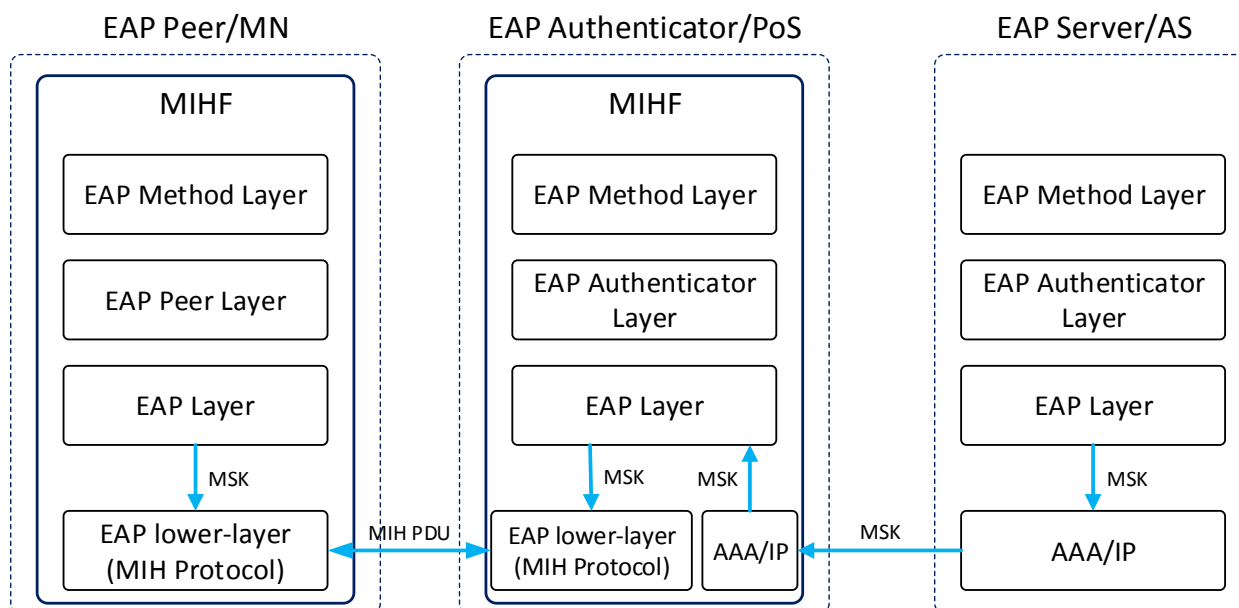


Figure 20 – Protocol Stack of service Access Authentication (with an EAP Server) [29].

The procedures to derive the keys are described in section 9.2.2 of IEEE 802.21a [29].

Table 10 specifies the key derivation functions, encryption algorithms and integrity algorithms that can be used when an MIH SA is established through EAP method.

Table 10 – IEEE 802.21a cryptographic algorithms [29]

Encryption algorithm	Description
AES_CBC	AES CBC mode
NULL	No encryption is applied
Integrity algorithm	Description
HMAC_SHA1_96	HMAC-SHA1 with 96 bits MAC
AES_CMAC	AES CMAC mode with 128 bits MAC
Authenticated encryption	Description
AES_CCM	AES-CCM mode
PRF used for key derivation function	Description
PRF_CMAC_AES	AES CMAC as PRF in counter mode
PRF_HMAC_SHA1	HMAC-SHA1 as PRF in counter mode
PRF_HMAC_SHA256	HMAC-SHA256 as PRF in counter mode

The cipher suites and key lengths are defined in Table 11.

Table 11 – Cypher suites [29].

Code	Encryption algorithm	Integrity algorithm	MSK length (L)
0b00000010	AES_CBC	HMAC_SHA1_96	384
0b00000100	NULL	HMAC_SHA1_96	256
0b00000101	NULL	AES_CMAC	256
0b00000110	AES_CCM		256

Depending on the selected cypher suite, the MIH Protocol Frame protected by EAP-generated SA can be seen in Figure 21 as well as the protected and unprotected parts of the message.

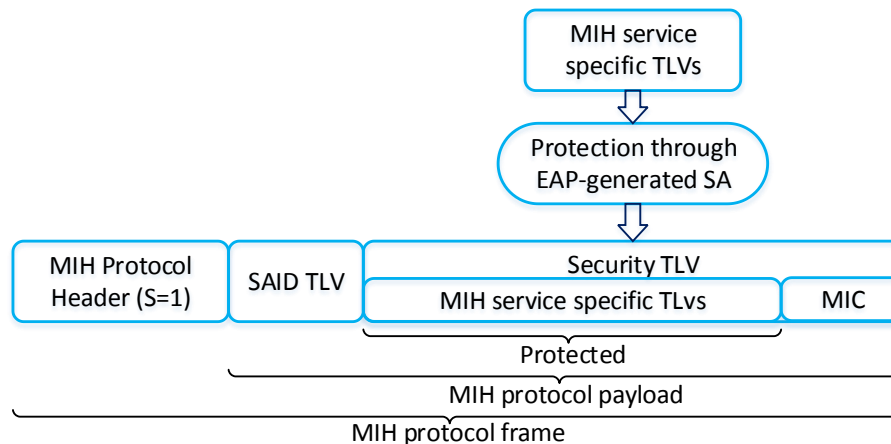


Figure 21 – MIH Protocol Frame protected by EAP-generated SA.

For the purpose of authentication and confidentiality of PPDR communications, SALUS will use AES_CCM cypher suite, following NIST recommendation SP 800-38C [32].

Protection through layer 2

When the MIH PDUs are exchanged between two devices that talk each other at layer 2, the MIH messages can be transported also at layer 2. In such cases, the protection may be provided through the layer 2 protocol such as TKIP and CCMP specified in IEEE Standard 802.11 [34].

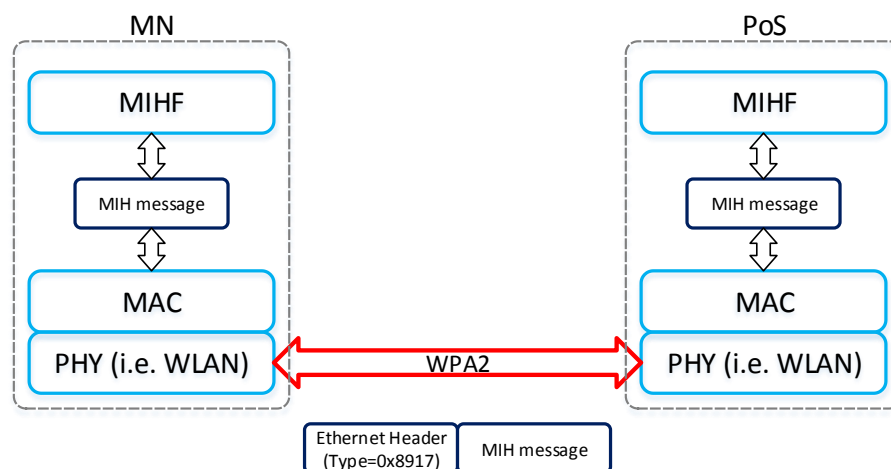


Figure 22 – MIH protection through layer 2.

Protection through IPsec

MIH messages may be protected by IPsec when they are transported over IPv4. If the MIH messages are transported over IPv6 then the protection by IPsec is mandatory [29]. The protocol stack and MIH message encapsulation is shown in Figure 23.

- When IPsec is applied between the MN and the PoS the MIH specific protection can be avoided.
- The protection through IPsec can provide end-to-end protection in all scenarios contrary to the protection through layer 2 presented above.

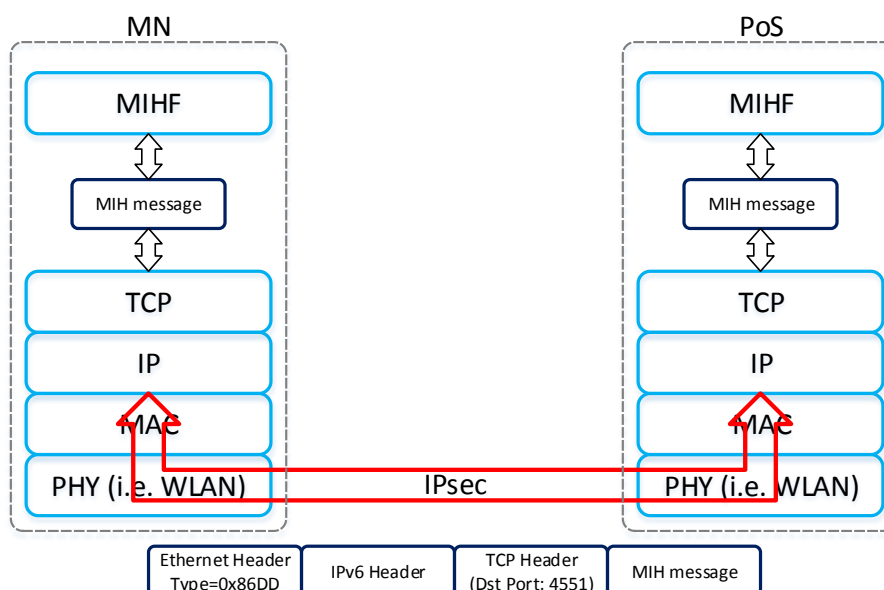


Figure 23 – MIH protection through IPsec.

Three protocols (IKEv1, IKEv2 and MOBIKE) can be used in order to establish IPsec SAs, although for the purpose of the SALUS project and regarding the security specifications for PMR networks only the IKEv2 and MOBIKE protocols are recommended¹. The use of Internet Key Exchange Version 2 (IKEv2) (specified in IETF RFC 7296 [35]) or IKEv2 Mobility and Multihoming Protocol (MOBIKE) (specified in IETF RFC 4555 [36]) will depend if the IPv6 address of the devices remains static or is dynamic. The use of MOBIKE or IKEv2 can be defined according with the following image, Figure 24.

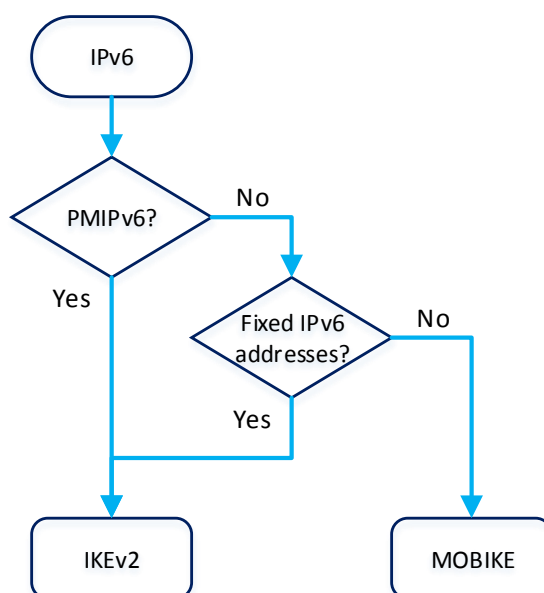


Figure 24 – IPsec authentication mechanism according with network configuration.

3.1.2 Inter-technology handovers with MIH proactive authentication

When a UE/MN moves between different PoAs it may need to authenticate to the target network before it starts sending data. The authentication and key establishment between the UE/MN and the target network causes delay (packet loss may also occur during this phase), which

¹ IKEv1 suffers from specific implementation guidelines ambiguities and is more prone to denial-of-service attacks than IKEv2. It also does not include standard mobility support.

interferes in ongoing communications. The MIH specification uses proactive authentications to improve the handover latency. Two mechanisms were specified to assist these procedures:

- **Unbundled media access proactive authentication:** the UE/MN conducts an authentication with the targeted network through a specific media, where the authenticator is a Media Specific Authenticator (MSA), as depicted in Figure 25 below;
- **Bundled media access proactive authentication:** at the end of MIH service access authentication the UE/MN and the PoS also establish a key(s) for a target PoA(s). The key(s) are distributed to the PoA(s) so that when a handover to one of the PoAs happens, the UE/MN can seamlessly establish a protected link with the chosen target PoA [29].

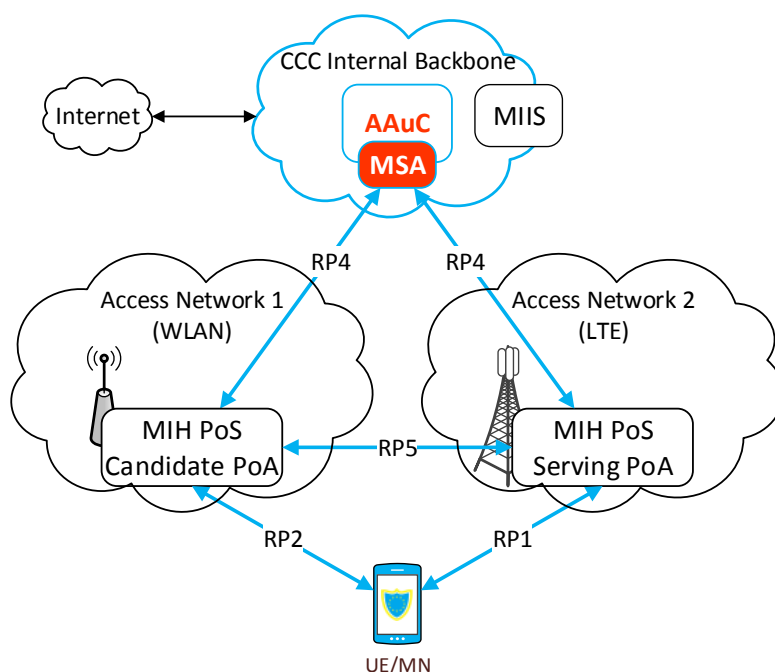


Figure 25 – MIH proactive authentication architecture (example).

The MSA, in Figure 25, is the component responsible for the handover authentication procedures to both PoAs (Serving PoA and Candidate PoA).

3.1.2.1 Unbundled media specific proactive authentication

In an *Unbundled media access proactive authentication*, the PoS passes authentication messages between the mobile node and the MSA, as depicted in Figure 26 below.

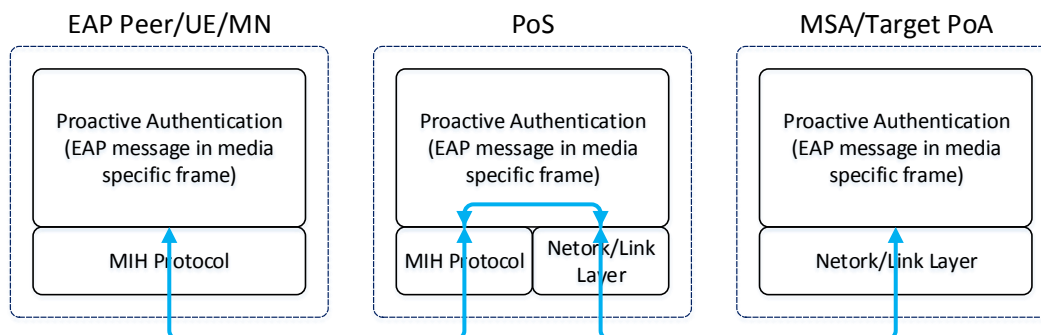


Figure 26 – Protocol Stack for MIH Supported Proactive Authentication (based on [29]).

Procedures in a media specific proactive authentication

The following steps apply when a MIH assisted media specific proactive authentication occurs:

- **PoS and candidate media specific authenticator discovery:** UE/MN searches for PoS and MSA addresses;
- **Proactive authentication through EAP or ERP:** after the UE/MN knows the PoS and MSA addresses it initiates the EAP or ERP authentication with the MSA. The PoS in this case acts only as an intermediate between the UE/MN and the MSA, the UE/MN is the EAP peer and the MSA acts as an EAP authenticator.
- **Media specific association handshake:** When the UE/MN decides to handover to a candidate network, the UE/MN and the PoA instead of performing a complete authentication, perform a media specific association based on the keying material derived by the proactive authentication. For example, the media specific handshake could be a 4-way handshake as in an IEEE 802.11 network [34]. A media specific handshake may further derive media specific session keys to protect the communication between the MN and the PoA once it is attached to it [29].

Figure 27 illustrates the three main steps described above for an unbundled media access proactive authentication.

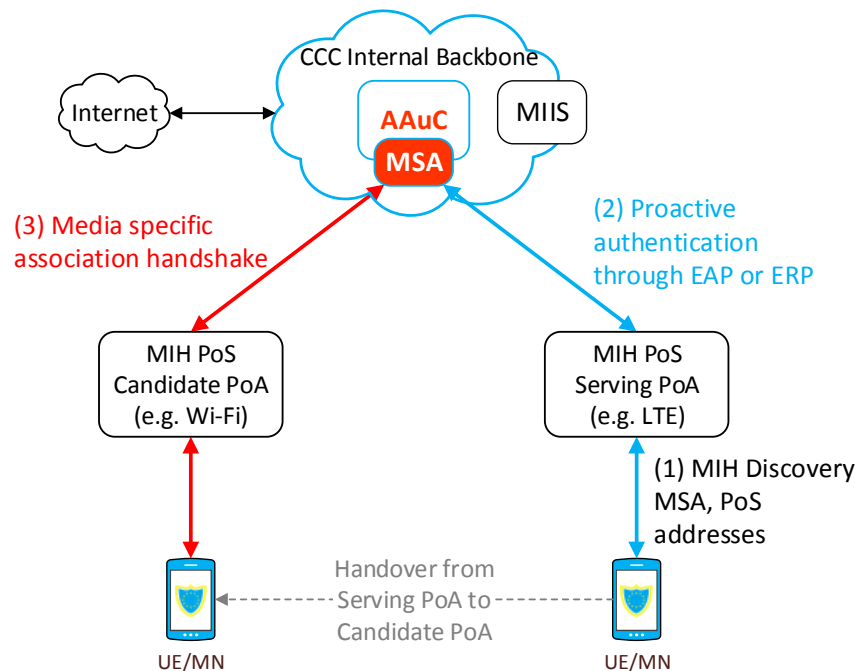


Figure 27 – Unbundled media access proactive authentication.

In this scenario, when the UE/MN performs handover to the candidate PoA, it will be authenticated by the MSA using already pre-computed security parameters.

3.1.2.2 Bundled media access proactive authentication

With *Bundled media access proactive authentication* it is intended that at the end of a successful service access authentication, a PoS will derive not only keys for the MIH message protection but also a key called *Media Specific Root Key (MSRK)*. This key will be further used to derive other key(s) called *Media Specific Pairwise Master Keys (MSPMKs)* to be used by a target PoA or PoAs [29]. When the UE/MN performs the handover to the Candidate PoA, the MSPMK is already installed on it and the authentication procedure can be done much faster and with a few number of messages exchanged. In this scenario the PoS can act as an authentication server where the UE/MN will be authenticated. This procedure is depicted in Figure 28.

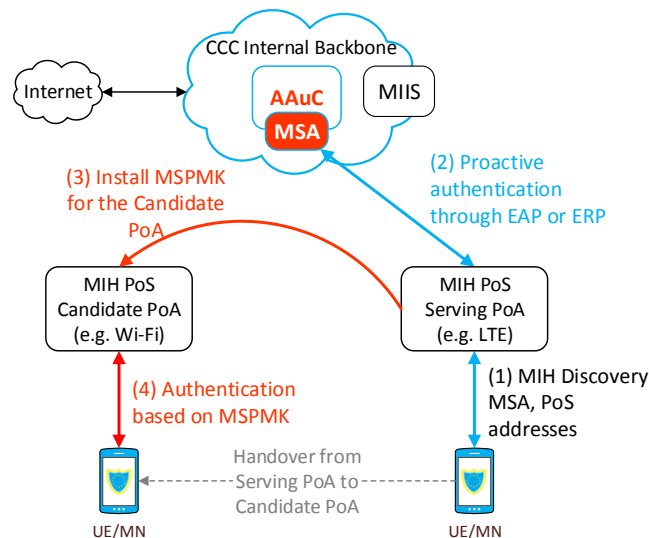


Figure 28 – Bundled media access proactive authentication.

Media specific key distribution

There are several ways a PoS can use to distribute the MSPMKs keys to the PoAs:

- Push key distribution: a PoS uses the MIH protocol to push a key into a target PoA;
- Reactive pull key distribution: a reactive pull key distribution is performed after the UE/MN moves to the target PoA and does not consider the usage of MIHF. This mechanism is out of scope of IEEE standard 802.21a [29] and depends on the technology used in the target PoA.
- Optimized proactive pull key distribution: this mechanism allows the UE/MN to perform a media-specific authentication proactively with a target PoA, without being directly connected to the wireless link of the target PoA by means of sending link-layer frames through the PoS to the target PoA [29].

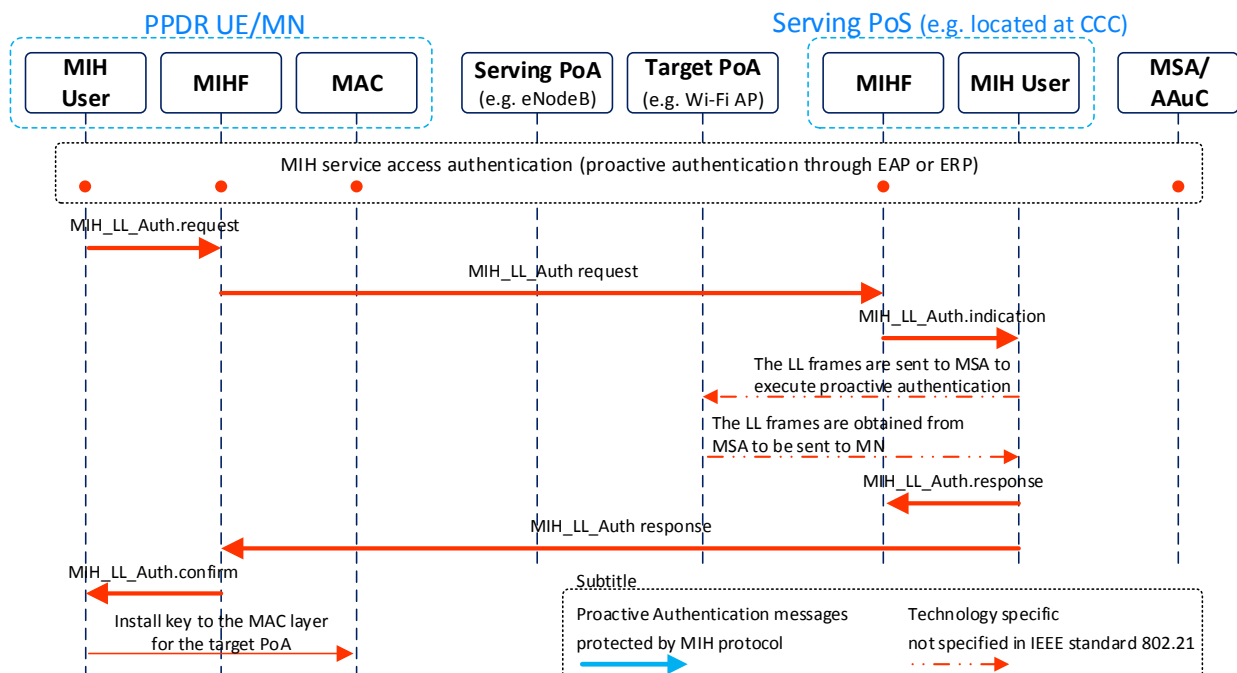


Figure 29 – Simplified message sequence chart for a proactive authentication signalling related to a secure handover between LTE and Wi-Fi (adapted from [29])

Figure 29 shows a simplified message sequence chart for proactive authentication when a PPDR UE/MN performs a seamless and secure handover between LTE and Wi-Fi.

3.2 Secure routing for wireless multi-hop networks

The information on this subsection has been considered security sensitive and it has been moved to D5.2 RESTREINT UE Annex, which is a separated document (SALUS_D5.2-Annex_v1.3.docx)

3.3 Secure wireless body area networks

A body area network (BAN), also referred to as a wireless body area network (WBAN), is a (wireless) network of wearable computing devices, normally consisting in data sensors, a processor unit, a transceiver and a battery. Existing and future WBANs play an important role in all three SALUS Use Cases, providing sensor data (biometric signals, location, environment perception, intrusion detection, etc.) to PPDR network. Nevertheless, they are still vulnerable and need to be secure. This section describes the sensor approach in SALUS and how data will be protected, regarding location privacy and security.

The SALUS platform shall feature several sensors in order to improve situational awareness for the deployed PPDR personnel and to provide additional information to the command and control centre. Such sensors will either be attached to the body of PPDR operatives or embedded in terminals that they carry. There are numerous sensor-based applications, but as an example we name two such solutions: man-down detection software that detects whether a PPDR user falls to the ground, and the remote monitoring of PPDR personnel biometric readings, such as their stress and fatigue levels (or simply their heart beat rate).

In general, sensor-based applications operate in the following manner: body worn sensors sense environment and send readings to the terminal of the PPDR personnel. In this regard the terminal serves as local hubs that later relays collected reading to the back-end applications. Actually, the terminals do not interface with the back-end applications directly, but send these messages with the help of the Message Broker (for a more detailed description of the Message Broker see section 2.7).

To secure such systems, two independent communication pathways need to be secured: the communication between the PPDR terminal and the back-end application and the communication between the PPDR terminal and the body worn sensors. Furthermore, there is a particular type of sensor-based applications where sensors are not attached to the body of PPDR users – indoor-localization services. The security of such systems is thus described separately.

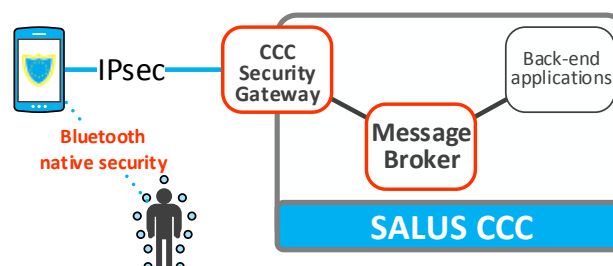


Figure 30 – An overview of the sensor-based application communication pathways.

Two pathways need to be secured: the communication between the PPDR terminal and the back-end applications and the communication between the PPDR terminal and (body-worn) sensors.

3.3.1 Communication between PPDR terminals and the back-end applications

Following what has been described in section 2.7.4, PPDR UE serve as local hubs that collect sensor readings and then – either on demand or periodically – forward them to the back-end applications. Messages carrying these readings may traverse several untrusted networks therefore they require proper security.

However, since PPDR terminals communicate with the back-end applications with the help of the Message Broker, all required security mechanisms are already in place: if the terminal is to send a message to the Message Broker, it has to establish a valid IPsec session with the CCC Security GW. Once such session is established, the entire communication between the terminal and the CCC Security GW is secured.

3.3.2 Communication between PPDR terminals and the body worn sensors

In some cases the wireless body area networks operate in environments with open access (e.g., hospital staff or fire brigades), which facilitate attacks. This makes the data prone to being eavesdropped, modified, or injected. The threats to such sensor networks were already analysed in SALUS Deliverable 5.1 [14].

Most of the sensors used in WBAN communicate through short-range networks (IEEE 802.15 Bluetooth), medium range networks (IEEE 802.15.4 Low Rate WPAN) and long-range networks (IEEE 802.11 WLAN), as it will be presented in the upcoming SALUS Deliverable 3.2 – “Enterprise and System Architecture - Intermediate”. Nonetheless, sensors can also rely on other type of technologies, for instance, they can be wired to PPDR terminals or other devices that communicate by Wi-Fi and/or LTE networks interfaces.

For most of body sensors the main communication mode is the short-range networks (IEEE 802.15 Bluetooth), because of the energy savings. The Bluetooth security mechanisms, presented in D5.1, are based on the following techniques:

- Pairing: that requires both/all the devices to use a certain PIN code as a shared secret to authenticate the establishment of the encryption key.
- Secure Simple Pairing (SSP): introduced in Bluetooth v2.1, that improves the pairing experience for Bluetooth devices, while increasing the use and strength of security.
- Advanced Encryption Standard (AES): introduced in Bluetooth v4.0, that is used as the encryption algorithm for data transfer.

For the sensors that use medium range networks (IEEE 802.15.4 Low Rate WPAN), as described in D5.1 [14], the security mechanisms are provided by the IEEE 802.15.4 standard. The supported security features of this standard meet the security requirements of PPDR applications. In this sense, the first level of security is assured by securing the sensors and the support infrastructure according to the security practices of IEEE 802.15.4 standard. As an example, there is no need to share the security keys.

Regarding the sensors that use long-range networks (IEEE 802.11), as described in D5.1 [14], the main security mechanism are defined in IEEE 802.11ah standard. This standard is an amendment to the IEEE 802.11-2007 (with some features of IEEE 802.11-2012 and modified PHY and MAC layers). From a security point of view, the standard has the same efficiency than the IEEE 802.11-2012 protocol, with security features taken directly from IEEE 802.11i.

Even though the security mechanisms presented in D5.1 [14] support security, privacy and end-to-end security for sensor networks, applications that manage sensors (e.g. frequency of data collection) should also be secured. Such applications are requested to support the following features:

- Resiliency– dealing with problems of limitation of power resources, computational complexity, aggregation, distribution processing.

- Privacy – dealing with secure data cloaking, secure communication channel and definition of privacy policies.
- Authentication and node localization – dealing with communication attacks, attacks against privacy, sensor node targeted attacks, power consumption attacks, policy attacks and cryptology attacks on key management.

3.3.3 Location privacy

As stated in D2.3 [15], localization is one of the services used by PPDR forces in all three use cases. Moreover, the exact positioning of units on the field is extremely important for coordination of their activities or/and emergency rescue from the danger if needed. However, the exact position of the selected unit is claimed being sensitive information due to huge benefits an attacker can obtain by eavesdropping and, especially, manipulating it. In particular, five types of attacks are considered:

1. Attacker eavesdrops the exact location of PPDR forces in a selected region and uses this information for crime planning (e.g. the robbery can be performed when all the units are far away from the location).
2. Attacker interrupts the communication between the unit and CCC/squad leader and modifies the sent localisation data from the selected unit to other units/Command and Control Centre (e.g. creating fake positions of units or destroying the unit locations on the map).
3. Attacker interrupts the communication and modifies the data sent from the localization nodes to the unit (e.g. to persuade the unit, it is in the wrong location).
4. Attacker jams the communication between localization nodes and the unit to disable the positioning feature.
5. Attacker jams the communication between the unit and the squad leader/CCC to disable the unit sharing its location with others.

With respect to the listed attacks, the concept of location privacy is defined as follows: Location privacy is a feature of location data to be written or modified only by the trusted entity that participate in the localization procedure.

To face these challenges, several enhancements to existing localization algorithms and protocols has to be introduced. First of all, the unit to localization nodes channel has to be designed in a way that prevents easy jamming. Existing cellular-based (LTE, A-GPS) and satellite-based (GPS, Galileo [GALILEO PRS]) already have sufficient protection from jamming and are hardly to be modified. Thus, similar level of protection has to be provided for sensor-based localisation services for indoor-positioning. This feature is to be provided by using the sufficient transmission power level on localization sensor nodes and reliable wireless channel for unit to localization node interaction - Wi-Fi or Bluetooth Low Energy (BT LE). Second, both localization node to unit and unit to squad leader/CCC communication channels have to be integrated into the jamming detection system. Once first signs of a possible jamming attack are noticed, the unit, CCC and squad leader have to get a report.

Third, the communication channels between localization nodes and units have to be protected from both eavesdropping and active attacks. As such, the proper encryption and authentication mechanisms are required. Again, existing cellular-based and satellite-based systems already have both features. Therefore, the similar level of confidentiality and integrity has to be provided for sensor-based systems. Due to huge importance of the localization, the usage of data sent from trusted nodes (with valid digital signature) exclusively is proposed. Before sending any localization data, sensor should pre-pend node's ID to the data, sign them with a valid signature and then encrypt the signature, the ID and the data chunk with a strong cipher. The key management is proposed to be done via pre-sharing of encryption keys and digital signatures to all the sensors and unit localization devices.

Finally, the localization data sent from the unit to the squad leader/CCC and localization data of other units downloaded to (collaborating) units from the squad leader/CCC has to be protected the same way as the data received by the unit from the localization nodes. Thus, the usage of existing secured wireless channel is proposed. The communication data channel between units and squad leader/CCC is protected from both eavesdropping and active attacks. As such, this channel is proposed to be used for all the localization data exchange as well.

3.4 Intrusion Detection System approach

Currently, there are two major categories in which an IDS can be classified, Host-based (HIDS) or Network-based (NIDS). Both types of IDSs can be either signature-based or anomaly-based:

- Signature-based: uses definitions of malicious behaviour for identifying such behaviour in a traffic stream.
- Anomaly-based: uses a model of benign behaviour for identifying malicious deviations/anomalies. As such, it is able to identify previously unidentified attacks (commonly referred to as 'zero-day' attacks).

However, there exist deeper classification of signature and anomaly-based detection, according to the methods used in each category and their traits. A more detailed overview is provided in figure Figure 31. According to static detection, the software of interest is directly analysed using the source code or if not available, the corresponding binary file by means of reverse-engineering [17]. Despite the fact of being the cheapest solution in terms of computational resources, static analysis is limited by the capability of code analysers and can only deal with applications, which use a small number of permissions and Application Program Interfaces (APIs) [18]. Moreover, various obfuscation methods have been implemented so as to bypass static analysis. In dynamic analysis on the other hand, the behaviour of the software is examined while it is executed by the OS on the host device [19] or in an isolated environment, such as a virtual machine or emulator [20]. Despite its advantages, dynamic analysis also faces some issues, one of which is related to the difficulty of creating an environment with the exact conditions that a malware application needs in order to be activated and big false-positive detection rate. Moreover, there is a factor of uncertainty concerning the time needed for a complete observation of malware behaviour [21]. Thus, both detection method categories are significant when aiming to implement a complete intrusion detection solution.

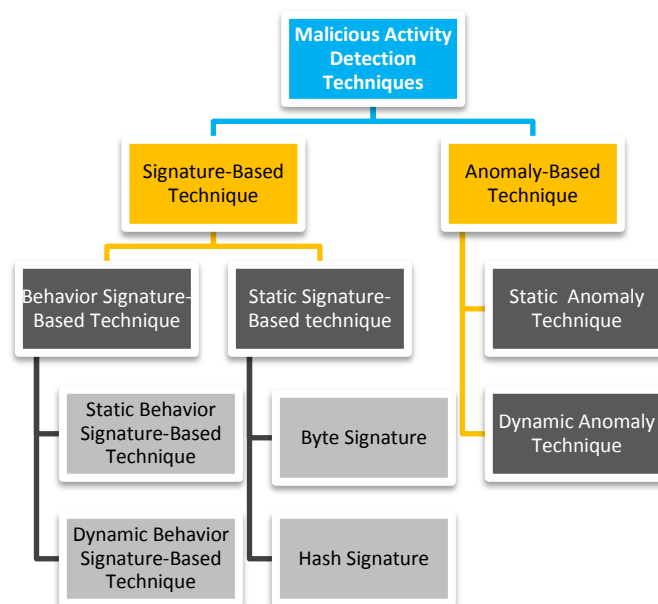


Figure 31 - IDS classification methods

HIDS and NIDS both have their own advantages and drawbacks, which are going to be further discussed in the remainder of this section. A HIDS is installed in the machine to monitor its behaviour in real-time. One of its features is to “consult its log analysis files or data from the audit agents and thus detect and assess changes in the file system, user access control, behaviour of system processes, and use of resources among others” [22]. Many of HIDSs have adopted the feature of file system hashing. The most significant files are hashed and their corresponding values are stored in a database. If changes to the hashes occur, after comparison to the equivalent values in the database, the HIDS alerts for potentially malicious activity. The particular technique applies successfully to cases such as: detection of rootkit installation, inclusion of new users, or setting changes. The major advantages and drawbacks of a HIDS [26] are presented below.

Advantages:

- Keeps track of user activity and correspondent interactions with applications and commands. Facilitates the association of potentially malicious actions to the responsible users.
- Collects real-time data related to the ongoing attacks.
- Provides exclusivity to the collection of data related only to the attacks occurring to the host system, without the need of capturing the whole network traffic.
- Does not have dependencies in order to access the host system.
- Does not require additional hardware.

Disadvantages:

- Requires simultaneous or centralized control over multiple hosts.
- Is highly dependent to the operating system of the host.
- Is vulnerable to attacks that lead to deletion and corruption of data, due to the fact that it, itself is a part of the host.
- It is likely to become correlated with attack data and extra performance data correlation analysis on data to be demanded from all involved network hosts.
- The performance of the host monitoring process can be negatively influenced by very extensive data analysis.

The basic function of a NIDS is to track traffic from different network hosts and the network where it resides in. NIDS can generally rely on either of two types of network traffic: packets and flows. There are different approaches concerning a NIDS architecture, but the main components that can be found in approximately all versions are: (i) a data collector; (ii) a manager and; (iii) a communication module responsible for transfer of data and results of the analysis. The role of the data collector is to capture and edit data as well as to analyse network traffic. Data are normalized and acquiring a form compatible to the standard anomaly profiles. The manager contains a classification mechanism that is responsible for categorizing an action/event to normal or potentially dangerous. A classification manager can be generally specialized in two types of detection, based on signature recognition or anomalous behaviour. In anomaly-based detection, the manager “captures network packets, analyses their headers, and compares them with known statistical patterns or signatures” [22]. On the other hand, signature-based detection, either static or dynamic detects sequences of bytes or hexadecimals that create identical signatures to the ones of known malicious software. Below, advantages and disadvantages [26], [27] deriving from the use of a NIDS are presented.

Advantages:

- Passive network monitoring causes no disturbance in the network traffic.
- Enables on-the-spot adoption of countermeasures, since detection occurs in real-time.
- There are no dependencies on operating systems of the network entities.

- With the correct configurations, it can be invisible to exterior entities whereas with a HIDS, leaving some activity traces in the operating system is inevitable. In
- Infrastructural requirements are very small when flow-based monitoring is performed, since most high-end packet forwarding devices are shipped with flow export capabilities.

Disadvantages:

- There may be requirements for complex protocols related to some of its applications.
- There is a risk of applications being restricted, especially in networks that consist of many fragments (i.e. networks with switches). More precisely, a network switch may limit traffic monitoring for a specific host only to the part that is addressed to it. As a partial solution, some switches provide support for a monitoring and scanning port.
- Infrastructural requirements are relatively high when packet-based monitoring is performed, due to the stringent processing and storage requirements when handling large amounts of traffic.

Packet forwarding devices, such as routers, switches and firewalls, with support for flow export technologies like NetFlow and IPFIX are nowadays widely deployed in any larger network, ranging from small business to backbone networks. As such, the flow data exported by these devices is often already collected and flow-based intrusion detection systems (IDSes) can be deployed at minimal cost. Three major components can be identified in a typical flow monitoring setup [23]:

1. Flow exporter – Aggregates individual packets into flows and once a flow is considered to have terminated, a flow is exported to a flow collector.
2. Flow collector – Responsible for reception, storage and analysis of flow data from one or more flow exporters, and sometimes even pre-processing in the form of anonymization or data profiling.
3. Analysis application – Reads or receives flow data from the flow collector and performs some sort of analysis, such as intrusion detection.

The design and implementation of flow export technologies, protocols, hardware and software poses limitations to the timeliness of flow-based intrusion detection. This is because of the timeout-based manner in which flows are expiring within a flow exporter and the delays incurred within a flow collector due to preliminary processing. Still, performing intrusion detection within the analysis application has advantages in terms of data correlation, since data from various observation points is available. Both IDS types have their own advantages and disadvantages. However, in order to maximize the strengths of both HIDS and NIDS, the implementation of hybrid IDSs started becoming adopted. One of their important characteristics is the centralized management of the infrastructure. More precisely, “the IDS can locate sensors in various network segments and other host-based IDSs used in machines. The management centre can control the rules or instructions for both IDS types, thus forming a hybrid IDS” [24]. In fact, an architecture for multi-layered, i.e., hybrid intrusion detection has been recently proposed [25] by SALUS. Moreover, a complete level of end-to-end security preservation is provided, since specifications of HIDS and NIDS are different and a combination of both is effective against a bigger set of attack types.

A hybrid IDS overcomes the restrictions that are caused due to limited host resources (especially when referring to mobile terminals) in case of HIDS and lack of centralized connectivity in case of NIDS equivalently. Lastly, the implementation of a hybrid IDS does not have additional infrastructure requirements, since the HIDS part is independent and does not create conflicts with the existing NIDS. This fact is depicted in Figure 32, where the architecture of a hybrid IDS is presented.

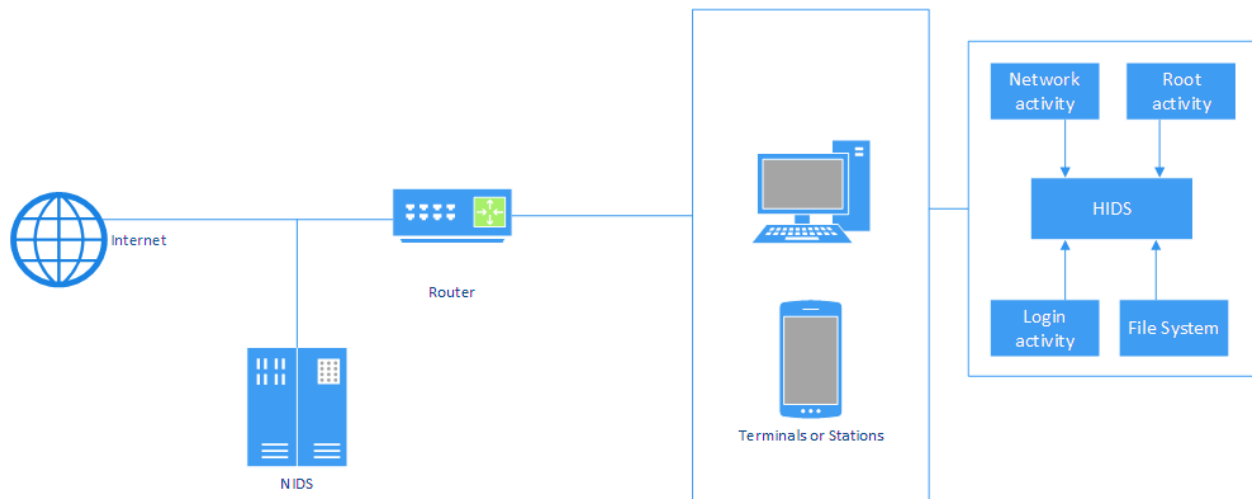


Figure 32 – Hybrid IDS Architecture

3.4.1 IDS Architecture - level 0

The information on this subsection has been considered security sensitive and it has been moved to D5.2 RESTREINT UE Annex, which is a separated document (SALUS_D5.2-Annex_v1.3.docx)

3.4.2 IDS Architecture - level 1

The information on this subsection has been considered security sensitive and it has been moved to D5.2 RESTREINT UE Annex, which is a separated document (SALUS_D5.2-Annex_v1.3.docx)

3.4.3 PPDR forensics

The information on this subsection has been considered security sensitive and it has been moved to D5.2 RESTREINT UE Annex, which is a separated document (SALUS_D5.2-Annex_v1.3.docx)

3.5 Security at physical layer: electromagnetic modelling of wireless channel for scenarios with human crowds

This section summarizes an approach for electromagnetic (EM) modelling of human bodies in crowds. The primary objective of these analyses is to calculate the wireless channel parameters under such scenarios and to better characterize the signal propagation characteristics for an increased resilient/secure communications. The approach uses distributed surface loadings with method of moments based on surface integral-equation formulation. It significantly reduces the computer resources needed for the electromagnetic analysis while keeping the final results accurate enough for the engineering purposes.

3.5.1 Brief overview of the used electromagnetic analysis

For EM analysis we use Method of Moments (MoM) based on Surface Integral-Equation formulation (SIE) [37][38], with higher order basis function for the surface current approximation and Galerkin testing, encapsulated in WIPL-D² code [39][40]. Nonetheless, the proposed approach for human body modeling can be used with any MoM-SIE code.

3.5.2 Developed methodology for efficient modeling of human crowds

The first step in modeling EM fields in the presence of human crowds is geometrical modeling of humans, with possibility to create various postures.

² WIPL-D is a software tool for high-frequency simulations of arbitrary electromagnetic structures.
url: <http://www.wipl-d.com/>

3.5.2.1 Generating geometry of human bodies

The starting geometry of humans is prepared in the open-source MakeHuman software [41], using low polygon approximation for the surface of the human body. The geometry of the model is further tailored with the open-source software Blender [42], primarily by removing the unnecessary details for EM analysis, while keeping the topology of the model unchanged. The final geometry is imported into WIPL-D, by translating the geometry description into WIPL-D native format using a custom-made code. It is worth noting that WIPL-D, MakeHuman and Blender software all use quadrilateral mesh for the model description, which is most efficient from the perspective of electromagnetic analysis (WIPL-D) and from the perspective of topology and geometry modifications for postures (MakeHuman and Blender).

For the illustration of the approach we use models as shown in Figure 33 and Figure 34. The model of a single human consists of approximately 1600 quadrilaterals and the model of a group consists of approximately 8100 quadrilaterals. In all models used, the human body is treated as a completely closed surface.

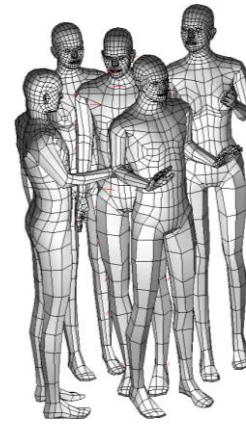
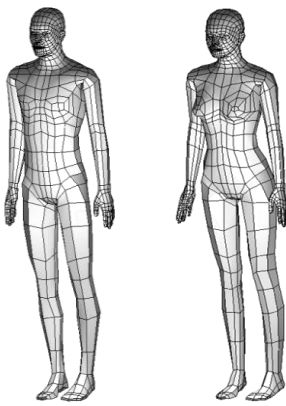


Figure 33 – Quadrilateral models of a human body, male and female

Figure 34 – Model of densely packed human crowd with each figure having different posture

3.5.2.2 Electromagnetic parameters of human body

Two approaches are used for the electromagnetic analysis, for the purpose of comparison of results and the analysis efficiency:

- the interior of the body model is filled with homogeneous lossy dielectric with complex permittivity being the average of complex permittivity of human tissue and;
- the distributed loadings are placed on the surface of the bodies, while keeping a vacuum everywhere.

The human model with dielectric has the advantage that it is closer to the real situation, but the downside of it is that it needs significantly more computer resources for the numerical EM analysis. The complex permittivity of the dielectric, as a function of frequency f , follows [43] and is calculated as:

$$\underline{\varepsilon}_r(f) = \varepsilon_{r\infty} + \sum_{k=1}^2 \frac{\Delta\varepsilon_k}{1 + (j2\pi f\tau_k)^{1-\alpha_k}} + \frac{\sigma}{j2\pi f\varepsilon_0}, \quad (1)$$

where $\varepsilon_{r\infty} = 4.0$, $\Delta\varepsilon_1 = 32.0$, $\tau_1 = 7.32 \text{ ps}$, $\alpha_1 = 0.0$, $\Delta\varepsilon_2 = 1100$, $\tau_2 = 32.48 \text{ ns}$, $\alpha_2 = 0.2$, $\sigma = 200 \mu\text{S/m}$, ε_0 is the permittivity of a vacuum, and $j = \sqrt{-1}$.

The human model with distributed loadings at the body surface has the advantage over the dielectric model as it needs significantly less computer resources. The downside of it is that the

distributed loading must be heuristically found, for example by comparison of results obtained from the dielectric model and from the model with loadings distributed on the surface.

3.5.3 Modeling example: WBAN channel in the presence of human crowds

WBANs have a significant role in a variety of applications such as rescue scenarios, medical purposes, amongst others. They are perceived as a building block of sensor networks within the SALUS project. Numerical EM modeling of WBAN channel parameters poses a challenge in cases when there are densely packed humans around or in the near vicinity of the WBAN bearer. Such situations can arise in public events of various kinds, like those described in the SALUS Use Cases.

3.5.3.1 Electromagnetic analysis setup

The EM analyses are performed in the frequency range from 2.36 GHz to 2.485 GHz, as this is the highest³ frequency range allocated for WBAN in the IEEE 802.15.6 standard [44].

3.5.3.2 Illustration of EM field for a single human and crowd

We place four human bodies around the original model, as it is shown in Figure 34. The positions of surrounding body models are chosen so that the spatial density of humans resembles the density in crowded places estimated to be 3 persons/m² [45].

The intensity of the electric field in the vicinity of a human body in a free-space is shown in Figure 35, and with densely packed crowd is shown in Figure 36. From the presented results one can observe a visible change in electromagnetic near-field distribution. This field change can lead to changes in the parameters of the wireless communication channel between antennas in the WBAN.

3.5.3.3 Single human

Further, the comparison of magnitude of the calculated scattering (s) parameters obtained by using dielectric model and the model with distributed loadings at the body surface is shown in Figure 37. The dielectric model leads to the numerical analysis with 21518 unknown coefficients for the surface current approximation, while the model with distributed loadings needs only 10.538 unknown coefficients.

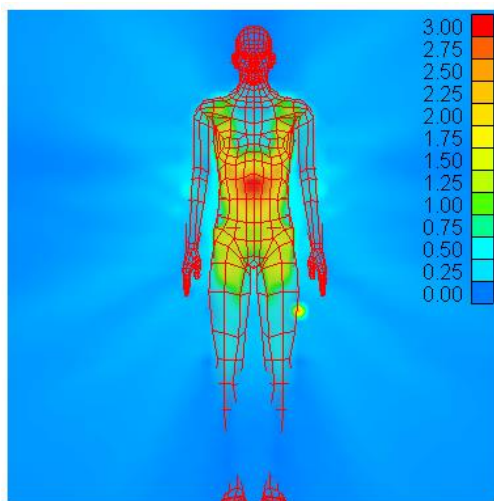


Figure 35 – Intensity of electric field in the vicinity of a human alone.

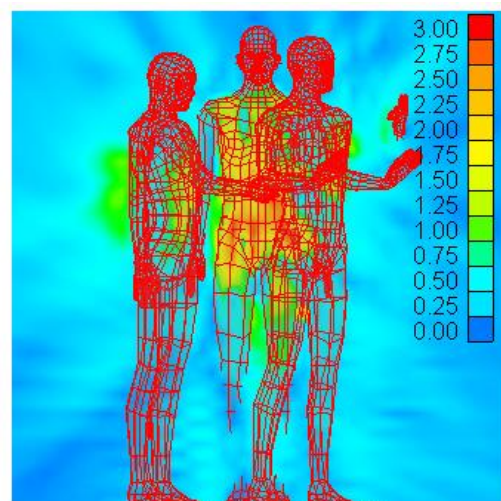


Figure 36 – Intensity of electric field with the presence of human crowd.

³ From the 3D EM simulation point-of-view, when a full wave analysis is used, like in the case of a Method of Moment applied to Surface Integral Equations, the most critical simulations regarding resources (memory and CPU required) are at the highest frequency. Namely, the number of unknown coefficients is directly proportional to the surface area in lambda squared.

In this case, thirty antennas were positioned at the vicinity of the human body, close to the spots commonly used in WBAN, like foot, knee, hip, tummy, chest, ear, hand, elbow, etc. The antennas ordinal numbers are shown in blue color in Figure 37. The antennas are placed either horizontally (i.e. parallel to the feet of the model) or vertically (i.e., parallel to the human spinal cord). From the 30 antennas in total, 6 with characteristic positions (identified with red arrows) were chosen for the comparison that follows.

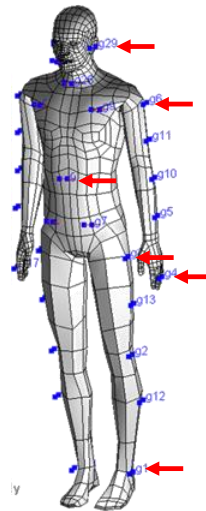


Figure 37 – Human body model with position of antennas (blue dots) and highlights (red arrows) for those antennas selected for comparison.

This EM structure was numerically analyzed as an EM system with 30 ports, with each antenna acting as a port. The analysis was done by exciting one port at a time while the other ports are shunted with $50\ \Omega$ terminations. The objective of the analysis is to calculate the scattering (s) parameters. The distributed loading used for the analysis was estimated to be $Z_s = (100 - j20)\ \Omega$. The penetration depth (i.e., EM skin effect) is in this case around 1 cm. The comparison of s-parameters calculated for a single human with dielectric model and the model with distributed loadings is shown in Figure 38 for horizontally placed antennas and in Figure 39 for vertically placed antennas.

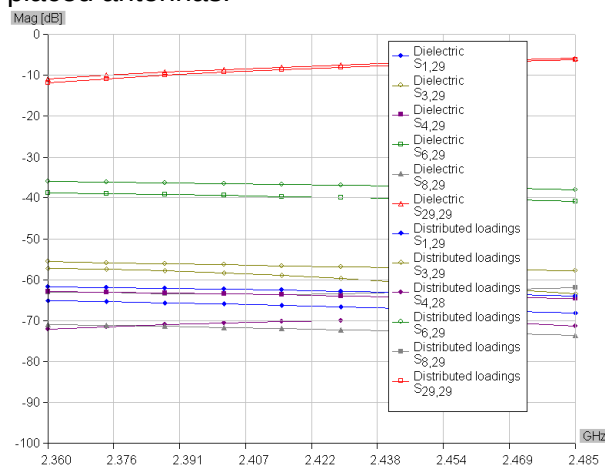


Figure 38 - Single human: comparison of s-parameters for horizontally placed antennas.

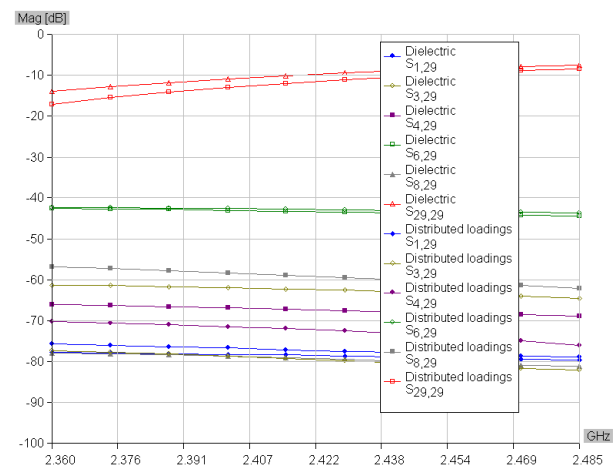


Figure 39 - Single human: comparison of s-parameters for vertically placed antennas.

The discrepancy between the magnitudes of calculated s-parameters is up to approximately 10 dB, regardless of the antenna's position and orientation. The total number of unknown coefficients that have to be found in the analysis for the dielectric model is 21.518 unknowns, while for the model with distributed loadings is 10.538 unknowns. Therefore, the model with

distributed loadings needs 2 times less unknowns for the analysis, which leads to 4 times less computer memory and up to 8 times faster overall analysis. Hence, the model with distributed loadings opens the possibility of analyzing larger human crowds while not compromising the final results significantly.

3.5.4 Human crowd

Two groups of humans with different body orientations were considered. The first one is with uniform distribution, as is shown in Figure 40a and Figure 40b. The second group has a stochastic orientation of standing humans in the group, as it is shown in Figure 41a and Figure 41b. Both groups have five people. In this case the model with the WBAN antennas is placed in the middle of the group. The distance between humans is chosen so that the surface density of humans in both groups is approximately 3 persons/m².

In this scenario, the total number of unknowns for the groups with dielectric model of humans is 112,044. On the other hand the total number of unknowns for the groups with humans modeled with distributed loadings is 53,371. The total analysis time, using one personal computer with graphical processing units (GPUs) is 12.1 hours for the dielectric model and 1.7 hours for the model with distributed loadings. Both models were solved using GPU accelerated out-of-core solver. The total memory consumption is around 87 GB of computer memory for the dielectric model and around 21 GB for the models with distributed loadings.

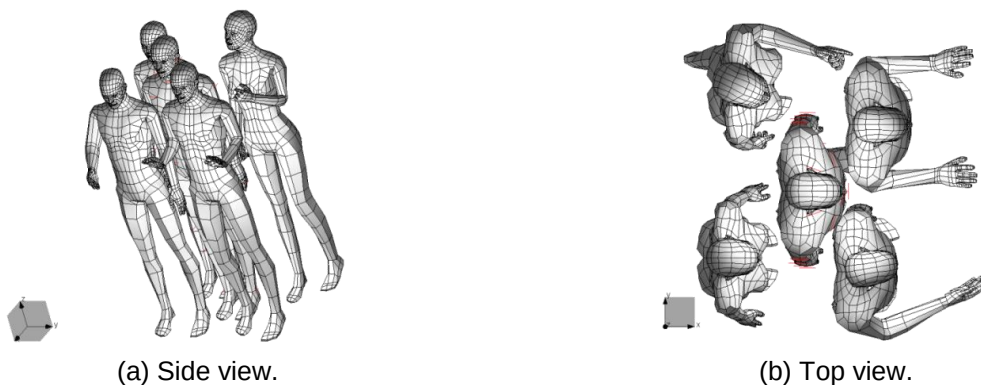


Figure 40 - Model of human group with uniform spatial distribution.

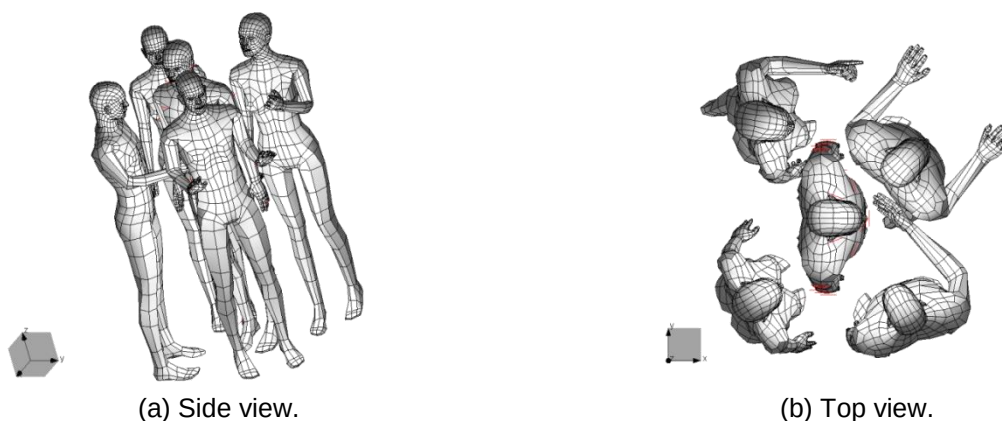


Figure 41 - Model of human group with stochastic spatial distribution.

The comparison of calculated s-parameters for the uniform crowd is shown in Figure 42 and Figure 43, for horizontally and vertically placed antennas.

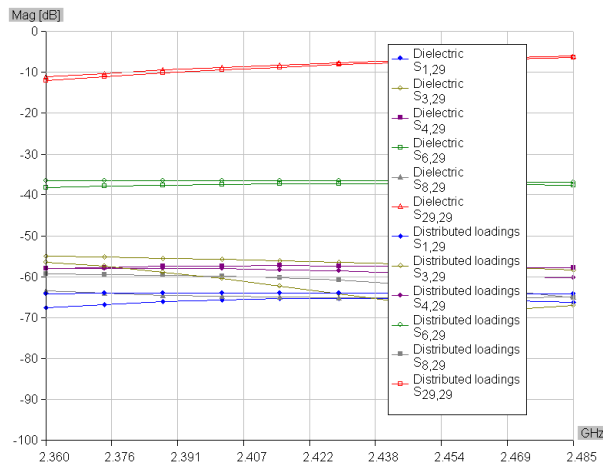


Figure 42 - Uniform crowd: comparison of s-parameters for horizontally placed antennas.

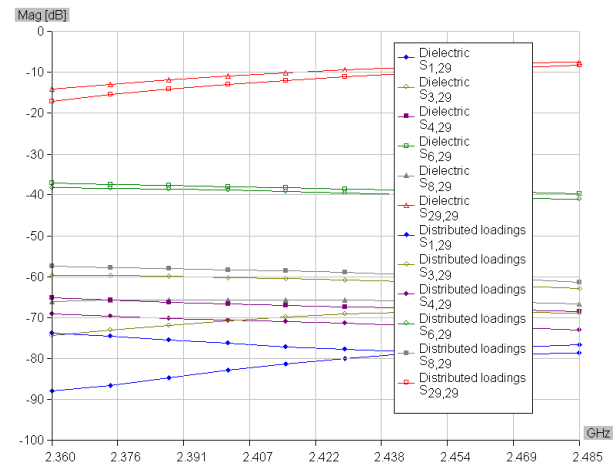


Figure 43 - Uniform crowd: comparison of s-parameters for vertically placed antennas.

The comparison of calculated s-parameters for the stochastic crowd is shown in Figure 44 and Figure 45, for horizontally and vertically placed antennas.

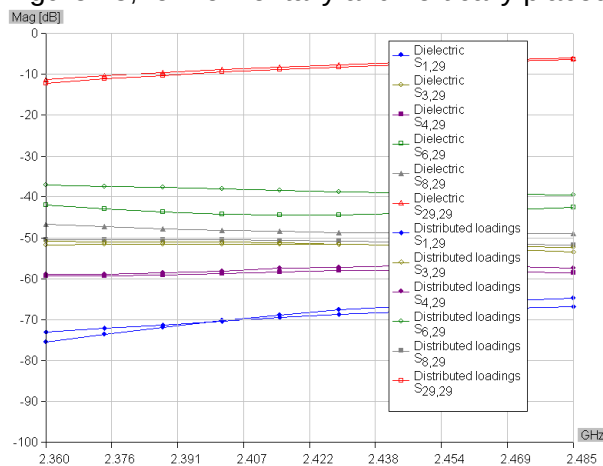


Figure 44 - Stochastic crowd: comparison of s-parameters for horizontally placed antennas.

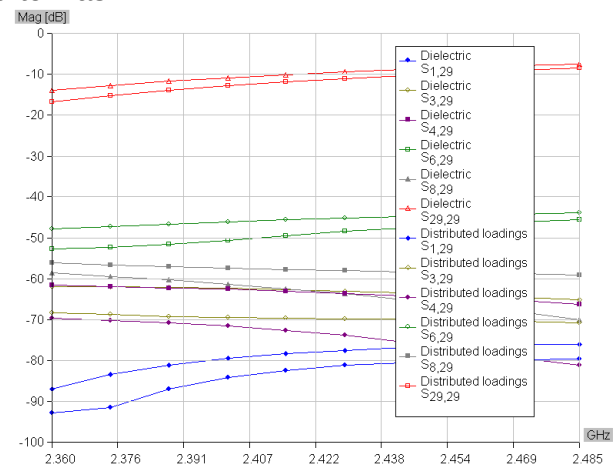


Figure 45 - Stochastic crowd: comparison of s-parameters for vertically placed antennas.

The described approach of EM modeling of human bodies at WBAN frequencies with distributed loadings lead to an efficient numerical EM analysis. The discrepancies between the fully dielectric model and the model with distributed loadings are typically at the order of several dB, with maximum of 15 dB discrepancy found only once⁴ (see Figure 43). Therefore, such an approach can be useful for statistical analysis of wireless channels and estimation of channel parameters in complex scenarios involving human crowds.

Parts of the results presented in this report have been published in [46].

3.5.5 Future research

The future research on wireless channel parameters, to be included in SALUS Deliverable 5.3, will involve the following scenarios:

⁴ 15 dB discrepancy occurred in the case of two antennas on the opposite sides of the body. Such placement results in huge attenuation (about -80 dB) as shown in Figure 43. In this case an approximate model based on distributed loadings introduces an error of 15 dB when comparing with the full dielectric model. Generally such approximate models introduce errors of plus/minus 1 dB per 10 dB attenuation between antennas, thus enabling about 10 times faster analysis than using a full dielectric model. We think that such approximation is justified in the case when many calculations should be performed to provide data for statistical analysis of wireless channels.

1. WBAN man down situation, shown in Figure 46;
2. in-crowd mobile device to base station (GSM/LTE) analysis, depicted in Figure 47;
3. Device-to-device communication in crowd, depicted in Figure 48.

The main objective of the upcoming research analysis will be to determine the additional attenuation of wireless channel due to the presence of human crowds.

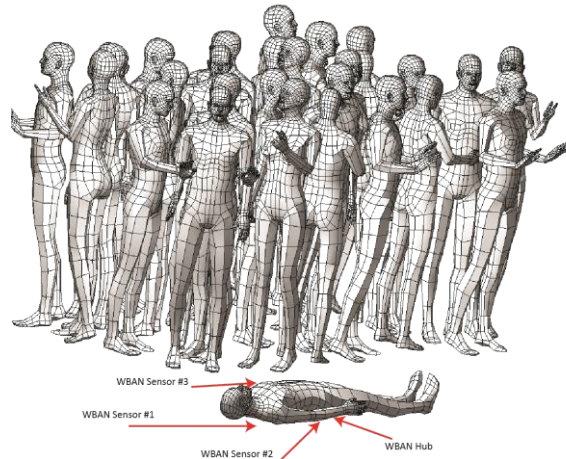


Figure 46 - WBAN man down situation.

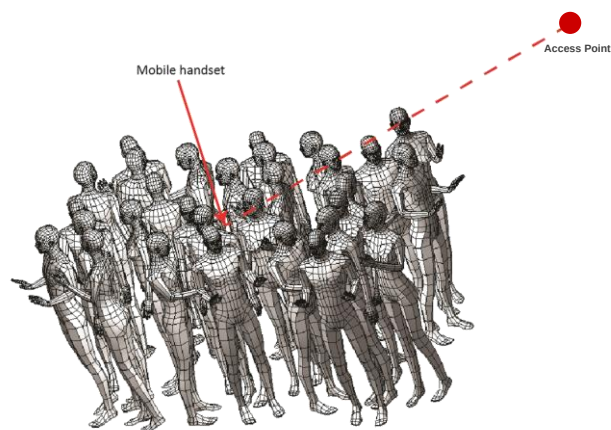


Figure 47 - In-crowd mobile device to base station communication.

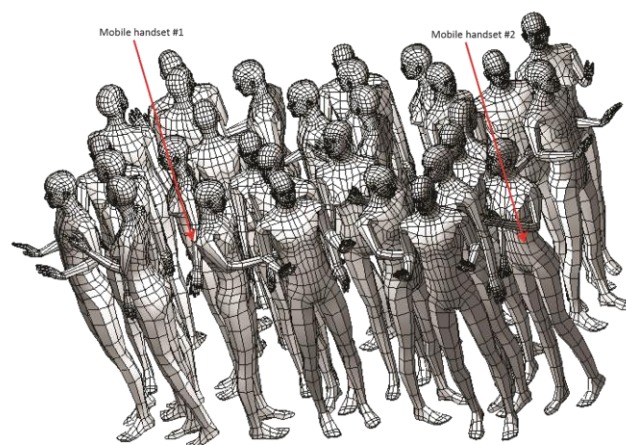


Figure 48 – Device-to-device wireless communication within crowd.

4 CONCLUDING REMARKS

The main objective of this document is to provide interim specification for the SALUS Security and Privacy Architecture, including its components, interfaces and behaviours. The proposed architecture took into consideration current discussions on WP4 on possible migration roadmaps from existing PPDR networks from simple cooperation with private LTE commercial operators, for non-mission critical interworking, towards a full mission critical LTE owned or shared network. The SALUS Security and Privacy Architecture also took into consideration the work been done in WP2, more specifically the final three SALUS Use Cases and the final user requirements as specified in SALUS deliverables 2.3 [15] and 2.4 [16], respectively. The current discussions in WP3 related to the System Architecture and Enterprise Architecture and on WP6 related to the production of D6.1 [11] were also taken in consideration. As such the SALUS Security and Privacy Architecture englobes a full range of technologies, such as LTE, TETRA, TETRAPOL, Wi-Fi (infrastructure, mesh and ad hoc) and Bluetooth (wireless body area networks).

Some of current achievements described in this document will be integrated in WP7 for the first SALUS prototype. Furthermore, this document will also serve as a basis for the final definition of the PPDR Security Architecture including the end-to-end security, privacy mechanisms and intrusion detection approach, that will be included in SALUS Deliverable 5.3.

It is also important to note that some of the scientific and technological results achieved so far, have already been disseminated in WP8, after being aproved by the SALUS Security Advisory Board.

Summary of the achievements in this document:

- Interim description for SALUS Security and Privacy Architecture;
- Identification of security components, their interfaces and beahviour ;
- High-level description for the secure and seamless handovers between LTE and Wi-Fi networks (in cooperation with D6.1[11]);
- Decision on the secure routing approach to use for the wireless multi-hop networks;
- Description on how wireless body area networks would be incorprated in the overall architecture and how to achieve secure transactions of data;
- Preliminary results for the wireless channel propagation modelling in crowded environemtns, of most importance to the city Security and Temporary Protection SALUS Use Cases
- Interim description for the SALUS IDS approach and the Mobile forensics module

BIBLIOGRAPHY

- [1] 3GPP, TS 23.251, "Technical Specification Group Services and System Aspects; Network Sharing; Architecture and functional description", Release 11, 2013.
Available: http://www.3gpp.org/ftp/Specs/archive/23_series/23.251/23251-b50.zip
- [2] Tewfik Doumi, Mike F. Dolan, Said Tatesh, and Alessio Casati – Alcatel-Lucent, George Tsirtsis, Kiran Anchan, and Dino Flore – Qualcomm. LTE for Public Safety Networks. In IEEE Communications Magazine, vol. 51, no. 2, pp. 106-112, February 2013.
Available: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6461193>.
- [3] Electronic Communications Committee (ECC). User requirements and spectrum needs for the future European broadband PPDR system (Wide Area Network). Draft ECC Report 199, 2013. See also: Available: <http://www.tandcca.com/Library/Documents/Broadband/Draft%20ECCRep199%20on%20PPDR%20requirements%20for%20ECC%20for%20PC.DOCX>.
- [4] Industrieranlagen-Betriebsgesellschaft mbH (IABG). Study on Medium-Term and Long-Term Capacity Requirements of PPDR Services in Wireless Communications. Study on behalf of the German Federal Ministry of Economics and Technology (BMWi). 20th May 2010.
- [5] International Telecommunication Union (ITU). World Radiocommunication Conference 2015 (WRC-15). Agenda and Relevant Resolutions, November 2012.
Available: <http://www.itu.int/go/wrc-15>.
- [6] Law Enforcement Working Party (LEWP) – Radio Communication Expert Group (RCEG). Public safety applications matrix. Excel table. 2012.
Available: <http://www.tandcca.com/Library/Documents/Broadband/LEWP-RCEG%20Matrix.xls>.
- [7] TETRA + Critical Communications Association (TCCA) – Critical Communications Broadband Group (CCBG). Mission Critical Mobile Broadband: Practical standardisation & roadmap considerations. White Paper, February 2013.
Available: <http://www.tandcca.com/Library/Documents/CCBGMissionCriticalMobileBroadbandwhitepaper2013.pdf>.
- [8] WIK-Consult. PPDR Spectrum Harmonisation in Germany, Europe and Globally. Study on behalf of the German Federal Ministry of Economics and Technology (BMWi). 6th December 2010.
Available: http://www.wik.org/uploads/media/PPDR_Harmonisation_en_public_final_01.pdf.
- [9] FM49, On the Future Architecture of Mission Critical Mobile Broadband PPDR Networks, White paper from the German Federal Ministry of the Interior, November 2013.
Available: [http://www.cept.org/Documents/fm-49/14437/FM49\(13\)-071-Info_White-Paper-on-Mission-Critical-Mobile-Broadband-PPDR-Networks](http://www.cept.org/Documents/fm-49/14437/FM49(13)-071-Info_White-Paper-on-Mission-Critical-Mobile-Broadband-PPDR-Networks).
- [10] SALUS Deliverable 4.3, "Business Analysis – Intermediate", February 2015.
- [11] SALUS Deliverable 6.1, "Connectivity, QoS provisioning and Seamless Mobility for Hetnets - Intermediate", January 2015.
- [12] 3GPP TS 23.402, "Universal Mobile Telecommunications System (UMTS);LTE; Architecture enhancements for non-3GPP accesses", version 12.6.0 Release 12, 2014
- [13] 3GPP TS 23.401, "General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", version 12.6.0 Release 12, 2014.
- [14] SALUS Deliverable 5.1, "Security and privacy analysis of TETRA / TETRAPOL PPDR, LTE and Wi-Fi networks", November 2014.
- [15] SALUS Deliverable 2.3, "SALUS PPDR use cases – Final", December 2014.
- [16] SALUS Deliverable 2.4, "User Requirements Definition - Final", December 2014.
- [17] Egele, M. and Kruegel, C. and Kirda, E. and Vigna, G., Pios: Detecting privacy leaks in iOS applications, 2011
- [18] Yu, W. and Zhang, H. and Ge, L. and Hardy, R., On behavior-based detection of malware on Android platform., 2013 , pp. 814 - 819 Atlanta, GA, USA, 2013

- [19] Blasing, T. and Batyuk, L. and Schmidt, A.D., An android application sandbox system for suspicious software detection, pp. 55-62, 2010
- [20] Chandramohan, M. and Hee Beng, K. T., Detection of Mobile Malware in the Wild. Computer, 45(9), pp. 65-71, 2012
- [21] Shabtai, A. and Kanonov, U. and Elovici, U. and Glezer, C. and Weiss, Y., "Andromaly": a behavioral malware detection framework for android devices. Journal of Intelligent Information Systems, 38(1), pp. 161-190, 2011
- [22] Pathan, A.- S.K., The State of the Art in Intrusion Prevention and Detection, Auerbach Publications, 2014
- [23] Hofstede, R. and Celeda, P. and Trammel, T. and Drago, I. and Sadre, R. and Sperotto, A. and Pras, A., Flow Monitoring Explained: From Packet Capture to Data Analysis with NetFlow and IPFIX. In: IEEE Communications Surveys & Tutorials, 2014
- [24] Nakamura, E. T., and Geus, P. L. Segurança de Redes em Ambientes Cooperativos. Novatec, 2007
- [25] Golling, M. and Hofstede, R. and Koch, R., Towards multi-layered intrusion detection in high-speed networks. In: Proceedings of the 6th International Conference On Cyber Conflict, CyCon 2014, 3-6 Jun 2014, Tallinn, Estonia. pp. 191-206, 2014
- [26] Ranum, M. J. Coverage in Intrusion Detection Systems. NFRSecurity, Inc. Technical Publications, pp. 1–9, June 2001
- [27] Shah, B. How to Choose Intrusion Detection Solution. Whitepaper, SANS Institute, InfoSec Reading Room, July 2001
- [28] IEEE Std 802.21-2008, IEEE Standard for Local and Metropolitan Area Networks – Part 21: Media Independent Handover Services, IEEE, January 2009
- [29] IEEE Std 802.21a-2012, IEEE Standard for Local and Metropolitan Area Networks – Part 21: Media Independent Handover Services (Amendment 1: Security Extensions to Media Independent Handover Services and Protocol), IEEE, May 2012
- [30] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008
- [31] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012
- [32] NIST recommendation SP 800-38C, "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", May 2004.
- [33] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004
- [34] IEEE Std 802.11-2012, IEEE Standard for local and metropolitan area networks – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE, March 2012
- [35] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, October 2014
- [36] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006
- [37] R.F. Harrington, Time-Harmonic Electromagnetic Fields, John Wiley & Sons, Inc., Reprinted by IEEE, New York, 2001.
- [38] R.F. Harrington, Field Computation by Moment Methods, New York: Macmillan, 1968. Reprinted by IEEE Press, New York, 1993.
- [39] B.M. Kolundžija, A.R. Djordjević, Electromagnetic modeling of composite metallic and dielectric structures, Boston: Artech House, 2002.
- [40] WIPL-D version 11, 2013. available: www.wipl-d.com
- [41] MakeHuman, Open source tool for making 3-D characters, available: www.makehuman.org
- [42] Blender, Blender Foundation, available: www.blender.org

- [43] C. Gabriel, S. Gabriel, E. Corthout, "The dielectric properties of biological tissues: I. Literature survey," *Physics in Medicine and Biology*, Vol. 41, No. 11, pp. 2231-2249, November 1996.
- [44] 802.15.6-2012 - IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks.
- [45] D. Oberhagemann, "Static and Dynamic Crowd Densities at Major Public Events," Technical Report TB 13-01, 1st Edition March 2012,
available: http://www.vfdb.de/download/TB_13_01_Crowd_densities.pdf
- [46] D.I. Olcan, A.J. Krneta, B.M. Kolundzija, "Modeling of human bodies for analysis of wireless body area networks in crowds," *Proceedings of 2014 IEEE International Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting*, Memphis, Tennessee, July 6-11 2014, pp. 406-407. ISBN: 978-1-4799-3539-0.

ACRONYMS

#	
3GPP	3rd Generation Partnership Project
A	
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AID	Action identifier
AIE	Air Interface Encryption
AKA	Authentication and Key Agreement
ARQ	Automatic Repeat Request
ASME	Access Security Management Entity
AuC	Authentication Centre
B	
BS	Base Station
BM-SC	Broadcast Multicast Service Centre
C	
CCC	Command and Control Centre
CCK	Common Cipher Key
CK	Cipher Key
CMAC	Cipher-based MAC
CML	ChaMeLeon (CML): A hybrid and adaptive routing protocol for Emergency Situations
D	
DCF	Distributed Coordination Function
DCK	Derived Cipher Key
DMO	Direct Mode Operation
DTLS	Datagram Transport Layer Security
E	
EAP	Extensible Authentication Protocol
EAP-AKA	EAP Method for 3rd Generation Authentication and Key Agreement
EAP-AKA'	Improved EAP Method for 3rd Generation Authentication and Key Agreement
E2EE	End-to-End Encryption
ECK	Encrypted Cipher Key
ENISA	The European Union Agency for Network and Information Security Agency
EM	Electromagnetic
eMBMS	Evolved Multimedia Broadcast Multicast Services
eNB	Evolved NodeB

eNodeB	Evolved NodeB
EPC	Evolved Packet Core
EPS	Evolved Packet System
ePDG	Evolved Packet Data Gateway
ERP	Extensible Re-authentication Protocol
ETSI	European Telecommunications Standards Institute
E-UTRA	Evolved Universal Terrestrial Radio Access
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
F	
FN	Fragment number
G	
GCK	Group Cipher Key
GERAN	GSM EDGE Radio Access Network
GCSE	Group Communication System Enablers
GSKO	Group Session Key for OTAR
GSM	Global System for Mobile Communications
GUTI	Globally Unique Temporary Identity
H	
HARQ	Hybrid Automatic Repeat Request
HE	Home Environment
HMAC	Keyed-Hashing for Message Authentication
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HWMP	Hybrid Wireless Mesh protocol
I	
IEEE	Institute of Electrical and Electronics Engineers
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IK	Integrity key
IKE	Internet Key Exchange Protocol
IKEv2	Internet Key Exchange Protocol Version 2
IPsec	Internet Protocol Security
ISDN	Integrated Services Data Network
ITSI	Individual TETRA Subscriber Identity
IV	Initial Value
J	
K	
K	Authentication Key

KS / KS'	Session Authentication Key
KSG	Key Stream Generator
KSS	Key Stream Segment
L	
LA-id	Location Area Identification
LAI	Location Area Identification
LAN	Local Area Network
LCT	Line Connected Terminal
LS	Line Station
LT	Line Termination
LTE	Long Term Evolution
M	
M2M	Machine-to-Machine
MAC (1)	Message Authentication Code
MAC (2)	Medium Access Control
MBMS-GW	eMBMS Gateway
ME	Mobile Equipment
MGCK	Modified Group Cipher Key
MF	More fragment
MIAC	Media Independent Authentication Key
MIC	Message Integrity Code
MIEK	Media Independent Encryption Key
MIH	Media Independent Handovers
MIHF	Media Independent Handovers Function
MIHU	Media Independent Handovers Users
MIIK	Media Independent Integrity Key
MITM	Man-In-The-Middle
MME	Mobility Management Entity
MN	Mobile Node
MOBIKE	IKEv2 Mobility and Multihoming Protocol
MoM	Method of Moments
MS	Mobile Station
MSA	Media Specific Authenticator
MSIN	Mobile Station Identification Number
MSK (1)	Master Shared Key
MSK (2)	Master Session Key
MSPMK	Media Specific Pairwise Master Keys
MSRK	Media Specific Root Key
MT	Mobile Terminal
N	
NDS/IP	Network Domain Security for IP-based control planes

NFC	Near Field Communication
O	
OMC	Operation and Maintenance Center
OP	Operator Variant Algorithm Configuration Field
OPCODE	Operation code
OTAR	Over The Air Re-keying
P	
P	Proactive authentication (bit)
P-TMSI	Same as TMSI
PABX	Private Automatic Branch Exchange
PCF	Point Coordination Function
PCRF	Policy and Charging Rules Function
PDCP	Packet Data Convergence Protocol
PDN GW	Packet Data Network Gateway
PDU	Protocol Data Unit
PEAP	Protected Extensible Authentication Protocol
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PMK	Pairwise Master Key
PMR	Professional Mobile Radio
PoA	Point of Access
PoS	Point of Service
PPDR	Public Protection and Disaster Relief
ProSe	Proximity Services
PSK	Pre-Shared key
PUK	PIN unlock key
PWS	Public Warning System
Q	
QoS	Quality of Service
R	
RAN	Radio Access Network
RFC	Request For Comments
S	
SA	Security association
SADP	Standalone Dispatch Position
SAE (1)	System Architecture Evolution (LTE)
SAE (2)	Simultaneous Authentication of Equals
SAGE	ETSI's Security Algorithm Group of Experts
SAID	Security Association Identifier

SIE	Surface Integral-Equation
SIM	Subscriber Identity Module
SQN	Sequence Number
SwMI	Switching and Management Infrastructure
T	
T _{Axx}	TETRA Algorithm
TB	Transport Blocks
TE	Terminal Equipment
TEDS	TETRA Enhanced Data Service
TETRA	Terrestrial Trunked Radio
TLV	Type Length Value
TLS	Transport Layer Security
TMO	trunked-mode operation
TMSI	Temporary Mobile Subscriber Identity
U	
UDT	User Data Terminal
UE	User Equipment
UM	Unacknowledged Mode
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
V	
V+D	Voice and Data
VBS	Voice Broadcast Service
VGCS	Voice Group Call Service
W	
WBAN	Wireless Body Area Networks
WEP	Wired Equivalent Privacy
WIPL-D	Software tool for high-frequency simulations of arbitrary electromagnetic structures. url: http://www.wipl-d.com
WLAN	Wireless LAN
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPAN	Wireless Personal Area Networks
WPS	Wi-Fi Protected Setup
X	
Y	
Z	

