



Security And Interoperability in Next Generation PPDR
Communication Infrastructures



Project Number: 313296

Deliverable 5.1

Security and privacy analysis of TETRA / TETRAPOL
PPDR, LTE and Wi-Fi networks

Scope	Scheduled deliverable
Lead Beneficiary	Instituto de Telecomunicações (IT)
Dissemination level	Public
Document creation date	03/Feb/2014
Document release date	10/Nov/2014
Contractual Date of Delivery	31/Aug/2014
Version	1.0
Status	Final

Abstract: Deliverable 5.1 describes state-of-the-art on seamless and secure mobility solutions, security aspects related to TETRA/TETRAPOL PPDR, LTE, Wi-Fi ad-hoc systems and sensor networks, and the risk analysis (in terms of ICT security) with focus on the SALUS scenarios. *This deliverable includes a RESTREIT UE Annex which contains security sensitive information.

[illegible]

Name	Organisation	Email
Galiotos Panagiotis	UPAT	pgaliot@gmail.com
Manfred Blaha	PSCE	manfred.blaha@gmx.net
Philippe Lasserre	ALU-I	philippe.lasserre@alcatel-lucent.com
Jérôme Brouet	ALU-I	jerome.brouet@alcatel-lucent.com

EXECUTIVE SUMMARY

Mission critical PPDR operations demand highly secure communications including a resilient, redundant and highly available infrastructure. These requirements mainly imply support for mutual authentication of infrastructure and terminals, methods for temporarily and permanently disabling terminals and smart cards, the capability to detect and compensate for jamming at the wireless link as well as air-interface-encryption and end-to-end-encryption of user and signalling data. Furthermore, core network elements must be protected physically against attackers.

Following this concern, this deliverable presents the security and privacy analysis of the technologies to be used by SALUS on the validation of the future PPDR system. This includes the security overview of LTE, TETRAPOL, TETRA, IEEE 802.11 (Wi-Fi) and sensor node networks (Bluetooth, IEEE 802.15.4 - Zigbee, IEEE 802.11ah). This deliverable also presents the ICT security risk analysis for the three SALUS Use Cases, along NIST SP 800-30 methodology and ISO/IEC 27005 standards.

This deliverable is two-fold:

- SALUS Deliverable 5.1 (this document);
- RESTREINT UE Annex to SALUS Deliverable 5.1 (a separate document).

This document is organized as follows: Section 1 presents the security and privacy analysis of LTE which includes the Evolved Packet System (EPS) architecture, the security architecture - including the security features at each security domain -, the LTE confidentiality and integrity protection mechanisms, the EPS key hierarchy, the currently existing handover mechanisms for interconnection with other trusted and untrusted networks, and LTE Proximity Services which are enhancements to the LTE standard to support Public Protection and Disaster Relief (PPDR), also known as Public Safety, applications. Section 2 addresses the security and privacy analysis of TETRAPOL, including the TETRAPOL architecture, mobile entities, type of users and TETRAPOL security principals. Section 3 provides the security and privacy analysis of TETRA which includes the TETRA architecture, the TETRA security principals, the authentication, encryption and the air interface key management mechanisms – including the TETRA security classes and the five types of managed keys. Section 4 describes the security and privacy analysis of short range wireless networks which include IEEE802.11 (Wi-Fi infrastructure/ad hoc) and sensor networks. A security overview is made for the more relevant ad hoc routing protocols and for the infrastructure mode – Wi-Fi related vulnerabilities are also presented. This section also presents a security overview for short range (Bluetooth), medium range (IEEE 802.15.4 – Zigbee) and long range (IEEE 802.11ah) sensor networks. Section 5 is part of the RESTREINT UE annex and finally, in Section 6 the concluding remarks, which include the foreseen security and privacy requirements of the future PPDR systems, are presented.

The RESTREINT UE Annex to this document 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 1.10 describes LTE security vulnerabilities which are mainly theoretical, including system architecture vulnerabilities, access and handover procedure vulnerabilities and security considerations for LTE confidentiality and integrity mechanisms, algorithms and key size. Section 3.3 describes the TETRA authentication, availability and confidentiality security vulnerabilities and presents considerations regarding the future of security within TETRA. Section 4.3 addresses the security vulnerabilities of IEEE 802.11 (Wi-Fi) networks both when operating in infrastructure and ad hoc mode. Finally, Section 5, deals with the ICT security risk analysis for SALUS use cases which establishes the foundation for the security & privacy requirements of SALUS, as well as risk mitigation plans to reduce the impact of the identified security risks

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
TABLE OF CONTENTS	4
TABLE OF FIGURES	6
1 SECURITY AND PRIVACY ANALYSIS OF LTE.....	7
1.1 Introduction	7
1.2 Evolved Packet System Architecture	7
1.2.1 Radio Protocol Architecture.....	8
1.2.2 LTE network elements.....	11
1.3 Overview of the LTE security architecture	11
1.4 Security features at each security domain	12
1.4.1 Network access security.....	12
1.4.2 Network domain security	14
1.4.3 User domain security.....	14
1.4.4 Application domain security.....	14
1.4.5 Visibility and configurability of security	14
1.5 Confidentiality.....	15
1.6 Integrity protection.....	16
1.7 EPS Key hierarchy	17
1.8 Support of multiple access technologies.....	18
1.8.1 Interworking with GERAN/UTRAN.....	19
1.8.2 Access security in trusted non-3GPP accesses.....	19
1.8.3 Access security in untrusted non-3GPP access	19
1.9 Proximity Services (ProSe) - LTE for Public Safety	20
1.9.1 ProSe Security, Authorization and Privacy Requirements	22
1.10 Group Communication Service Enablers for LTE (GCSE_LTE)	23
1.10.1 Interworking between GCSE_LTE and ProSe	24
1.10.2 Security requirements for Group Communication	25
1.10.3 Interaction with emergency calls and ProSe.....	25
1.11 LTE security vulnerabilities.....	25
2 SECURITY AND PRIVACY ANALYSIS OF TETRAPOL.....	26
2.1 TETRAPOL Architecture	26
2.1.1 System terminal	26
2.1.2 ISO services distribution.....	26
2.1.3 TETRAPOL users	27
2.1.4 Service table	28
2.2 TETRAPOL security principals	29
2.2.1 End-to-end ciphering	29
2.2.2 Mutual authentication	29

2.2.3	Signalling protection	29
2.2.4	Remote disabling of terminals	29
2.2.5	Automatic rekeying	29
2.2.6	Automatic network reconfiguration	29
2.2.7	Access control	29
2.2.8	Subscriber Identity Module	30
2.2.9	Encryption diversity	30
3	SECURITY AND PRIVACY ANALYSIS OF TETRA.....	31
3.1	TETRA Architecture	31
3.2	TETRA security principals	33
3.2.1	Authentication	34
3.2.2	Encryption	37
3.2.3	Air Interface key management mechanisms.....	38
3.3	TETRA security vulnerabilities.....	44
4	SECURITY AND PRIVACY ANALYSIS OF SHORT RANGE WIRELESS NETWORKS....	45
4.1	The role of Wi-Fi and sensor networks in SALUS platform [UL, UBITEL]	45
4.2	Threat model.....	45
4.2.1	Wi-Fi Ad Hoc Mesh Routing	45
4.2.2	Wi-Fi Infrastructure.....	45
4.2.3	Sensor-networks	46
4.3	Security and privacy analysis of Wi-Fi networks	46
4.3.1	Ad Hoc Mesh Routing Security.....	46
4.3.2	Infrastructure security.....	50
4.3.3	Wi-Fi security vulnerabilities	51
4.3.4	Security analysis of Wi-Fi applicability towards future PPDR communications	52
4.4	Security and privacy analysis of sensor networks.....	53
4.4.1	Short-range sensor networks	53
4.4.2	Medium range sensor networks	54
4.4.3	Long-range sensor networks	55
5	ICT SECURITY RISK ANALYSIS FOR SALUS USE CASES	57
6	CONCLUDING REMARKS - SECURITY AND PRIVACY REQUIREMENTS OF THE FUTURE PPDR SYSTEMS	58
7	Bibliography.....	60
	Acronyms	65

TABLE OF FIGURES

Figure 1: LTE Evolved Packet System [2]	7
Figure 2: LTE radio protocol architecture [3].	8
Figure 3: Control Plane UE – MME [4].	8
Figure 4: Protocol structure between UE and PDN GW [4].	9
Figure 5: Overview of the security architecture [15].	12
Figure 6: Mutual authentication procedure in LTE.	13
Figure 7: Procedures and building blocks for the ciphering of data in LTE [15].	16
Figure 8: Derivation of MAC-I/NAS-MAC (or XMAC-I/XNAS-MAC) [15].	17
Figure 9: EPS Key Hierarchy and Radio Interface Security (based on [2]).	18
Figure 10: Mapping security context in handover between E-UTRAN and UTRAN [16].	19
Figure 11: EAP-AKA' based access authentication for eHRPD [16].	19
Figure 12: (a) Authentication using IKEv2 and EAP-AKA between UE and ePDG; (b) User plane traffic is protected in IPSec tunnel between UE and ePDG [16].	20
Figure 13: a) ProSe direct communication; b) UE to UE relay	21
Figure 14: a) User Equipment to network relay; b) Group to network relay	22
Figure 15: High-level architecture for GCSE_LTE [95].	23
Figure 16: Media traffic with unicast and MBMS on Downlink [95].	24
Figure 17: ProSe-enabled UEs arranged in ProSe Groups (based on [94]).	24
Figure 18 - TETRAPOL Mobile entities.....	26
Figure 19 - Tele and bearer services	27
Figure 20 - Network and direct mode.....	27
Figure 21 - TETRAPOL users' positions.....	28
Figure 22 - TETRAPOL Security Mechanisms.....	30
Figure 23: General TETRA architecture.	32
Figure 24 - TETRA Security Model Layering	33
Figure 25 - MS authentication in TETRA [37]	34
Figure 26 - Infrastructure authentication in TETRA [37].	35
Figure 27 - Mutual Authentication in TETRA (SwMI triggered) [37].	36
Figure 28 - Mutual Authentication in TETRA (MS triggered) [37]	36
Figure 29 - Speech and control information encryption [37].	38
Figure 30: Derivation of the DCK from DCK1 and DCK2 using TB4 algorithm [37].	39
Figure 31: Distribution of a common cipher key [37].	40
Figure 32: Distribution of a group cipher key to an individual, based on [37].	41
Figure 33: Distribution of a group cipher key to a group member, based on [37].	41
Figure 34: a) Generation of MGCK from GCK and SCK in class 2 systems; b) Generation of MGCK from GCK and CCK in class 3 systems.....	41
Figure 35: Distribution of SCK to an individual MS by an authentication centre, based on [37].	42
Figure 36: Distribution of SCK to a group member by an authentication centre, based on [37].	43
Figure 37: Distribution of GSKO by an authentication centre [37].	43
Figure 38: Generation of EGSKO using TB7 [37].	43

1 SECURITY AND PRIVACY ANALYSIS OF LTE

1.1 Introduction

Long Term evolution (LTE), widely known as 4G, is a standard for high speed wireless communications, developed by the 3GPP (3rd Generation Partnership Project) and is specified in its Release 8 document series (first release). LTE is based on the GSM/EDGE and UMTS/HSPA network technologies towards an end-to-end all-IP system, achieving increased capacity and speed using a different radio interface together with core network improvements. LTE first release (release 8), provided downlink peak rates of 150Mbit/s, uplink peak rates of 50Mbit/s and QoS provisions enabling a transfer latency of less than 10ms in LTE network. Currently 3GPP works on Release 12 and 13 of the standard. With increased data rates, improved spectrum efficiency and packet-optimized system, LTE technology is set to drive machine to machine technology and data intensive applications [1]. 3GPP is also working in order to implement Public Protection and Disaster Relief (PPDR), also known as Public Safety, communications in LTE. These new LTE features have specific requirements related with security and reliability due to the sensitive information that is transmitted in these networks.

1.2 Evolved Packet System Architecture

The Evolved Packet System (EPS) is a 3GPP term which refers to a complete end-to-end system, that is, the User Equipment (UE), Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and Core Network (CN), designated in LTE by Evolved Packet Core (EPC) [16]. The main LTE module that constitutes the E-UTRAN is the Evolved NodeB (eNodeB or eNB), the LTE Relay Node shown in Figure 1 is a feature of release 10 and its purpose is to improve network coverage and bandwidth. The EPC can have multiple modules (depending on the network operator requirements), the main ones are the Mobility Management Entity (MME), Serving Gateway (SGW), Packet Data Network Gateway (PDN GW), Home Subscriber Server/Authentication Centre (HSS/AuC) and the Policy and Charging Rules Function (PCRF). When Interworking with other technologies the Evolved Packet Data Gateway (ePDG) and the 3GPP Authentication Authorization and Accounting Server (3GPP AAA) are also important modules that shall be considered. Figure 1 depicts the modules described above with the corresponding inter-module interfaces.

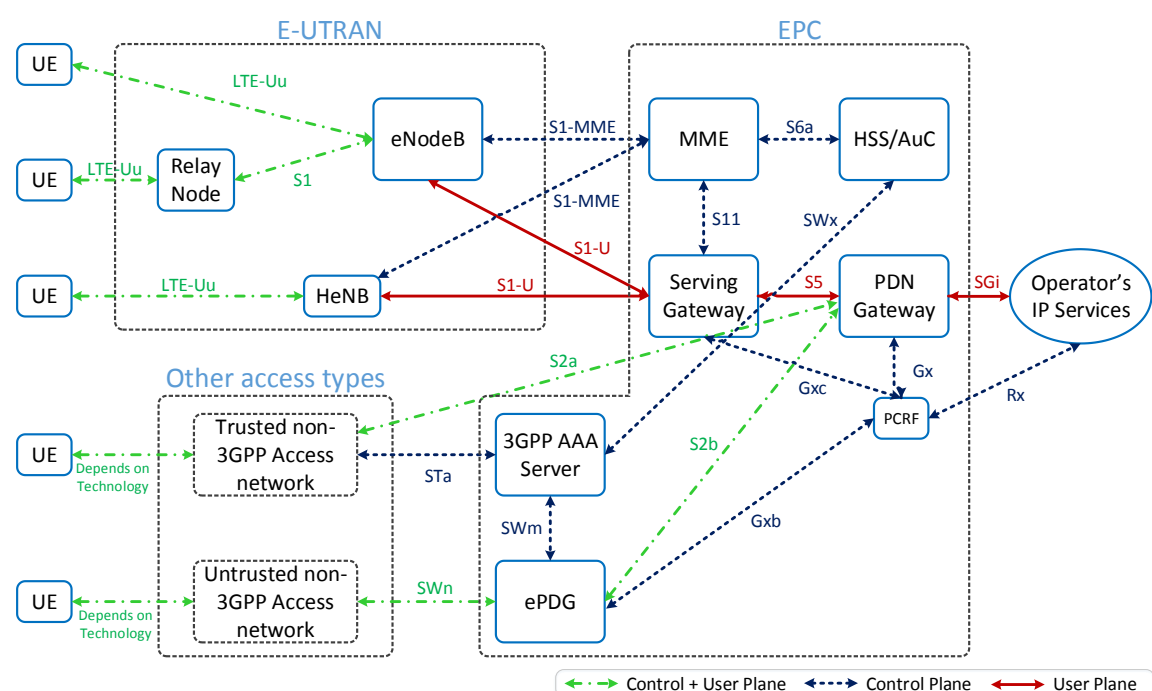


Figure 1: LTE Evolved Packet System [2]

1.2.1 Radio Protocol Architecture

The radio protocol architecture for LTE can be separated into Control Plane architecture and User Plane architecture, as shown in Figure 2 [3]:

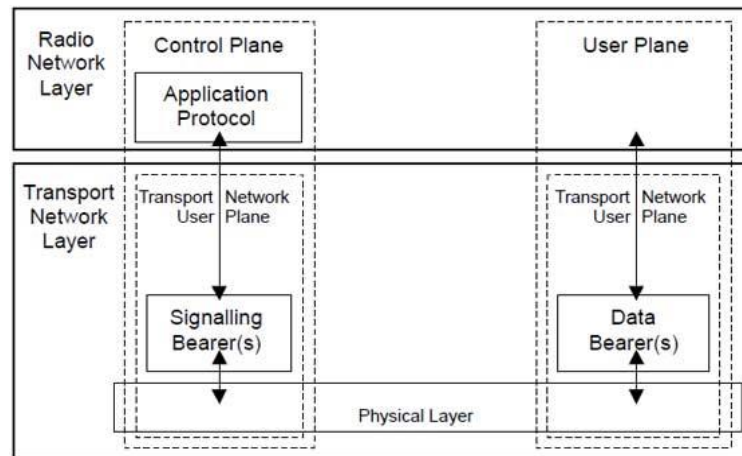


Figure 2: LTE radio protocol architecture [3].

At User Plane side, the application creates data packets that are processed by protocols such as TCP, UDP and IP, while in the Control Plane the radio resource control (RRC) protocol writes the signalling messages that are exchanged between the eNodeB and the UE. In both cases, the information is processed by the Packet Data Convergence Protocol (PDCP), the Radio Link Control (RLC) protocol and the medium access control (MAC) protocol, before being passed to the physical layer for transmission, see Figure 3.

Control Plane

The Control Plane consists of protocols for control and support of the User Plane functions [4]:

- Controlling the evolved UMTS Terrestrial Radio Access (E-UTRA) network access connections, such as attaching to and detaching from E-UTRAN;
- Controlling the attributes of an established network access connection, such as activation of an IP address;
- Controlling the routing path of an established network connection in order to support user mobility;
- Controlling the assignment of network resources to meet changing user demands.

Figure 3 refers to the control plane protocol stack between the UE and the MME. Additional variants can also be considered (i.e.: MME-MME, SGW-PDN GW, MME-HSS), which are outside the scope of this deliverable. For detailed information on these variants please refer to 3GPP TS 23.401 [4].

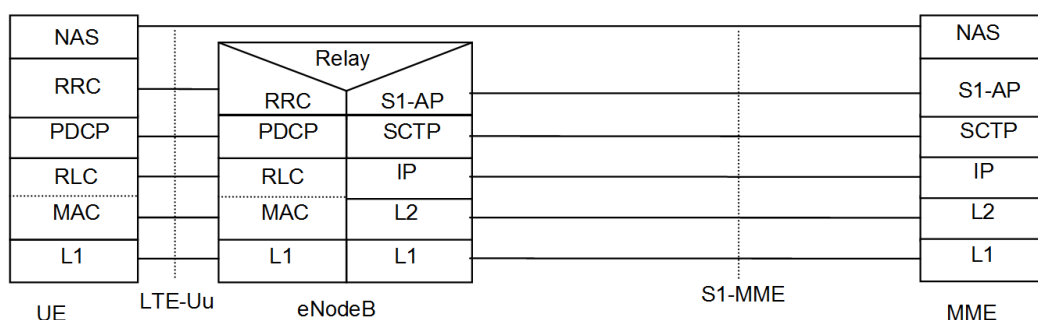


Figure 3: Control Plane UE – MME [4].

User Plane

The User Plane carries the network's user's traffic. The most common scenario used for User Plane and its protocol stack is depicted in Figure 4:

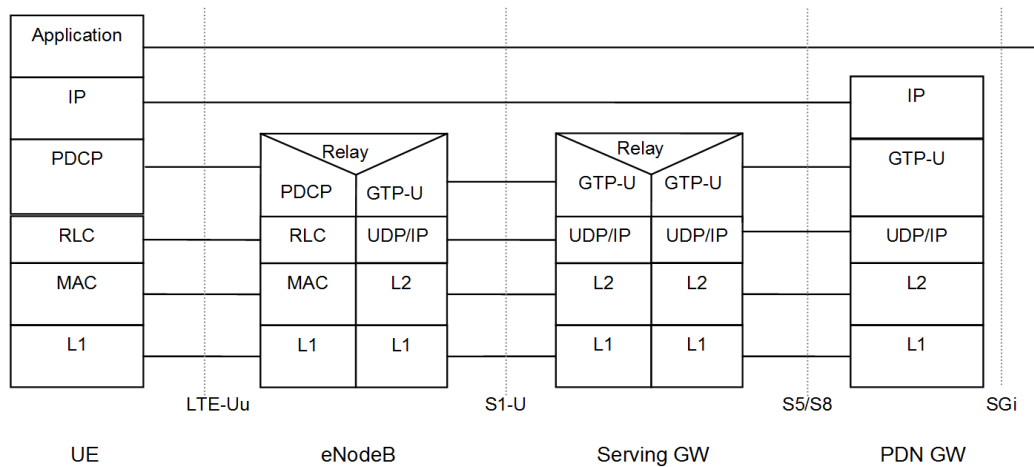


Figure 4: Protocol structure between UE and PDN GW [4].

The main functions for each of the LTE layers are briefly described in Table 1.

Table 1: Summary of the main functions in each LTE layer

Non Access Stratum (NAS) Protocols	NAS is specified in 3GPP TS 24.301 [5] and forms the highest stratum of the control plane between the UE and the MME. NAS protocols support the mobility of the UE and the session management procedures to establish and maintain IP connectivity between the UE and a PDN GW.
Radio Resource Control (RRC)	RRC is specified in 3GPP TS 36.331 [6]. The main services and functions of the RRC sublayer include [1]: - Broadcast of system information related to the non-access stratum (NAS); - Broadcast of system information related to the access stratum (AS); - Paging; - Establishment, maintenance and release of an RRC connection between the UE and E-UTRAN; - Security functions including key management; - Establishment, configuration, maintenance and release of point-to-point Radio Bearers; - Mobility functions; - QoS management functions; - UE measurement reporting and control of the reporting; - NAS direct message transfer to/from NAS from/to UE.
Packet Data Convergence Control (PDCP)	PDCP is specified in 3GPP TS 36.323 [7] and the main services and functions for the user plane include [1]: - Header compression and decompression: Robust Header Compression (ROHC) only; - Transfer of user data; - In-sequence delivery of upper layer protocol data units (PDUs) at PDCP re-establishment procedure for RLC acknowledged mode (AM); - Duplicate detection of lower layer Service Data Units (SDUs) at PDCP re-establishment procedure for RLC AM; - Retransmission of PDCP SDUs at handover for RLC AM;

	▪ Ciphering and deciphering; ▪ Timer-based SDU discard in uplink. The main services and functions of the PDCP for the control plane include: ▪ Ciphering and Integrity Protection; ▪ Transfer of control plane data.
Radio Link Control (RLC)	RLC is specified in 3GPP TS 36.322 [8]. The main services and functions of the RLC sublayer include [1]: ▪ Transfer of upper layer PDUs; ▪ Error Correction through ARQ (only for AM data transfer); ▪ Concatenation, segmentation and reassembly of RLC SDUs (only for unacknowledged mode (UM) and AM data transfer); ▪ Re-segmentation of RLC data PDUs (only for AM data transfer); ▪ In sequence delivery of upper layer PDUs (only for UM and AM data transfer); ▪ Duplicate detection (only for UM and AM data transfer); ▪ Protocol error detection and recovery; ▪ RLC SDU discard (only for UM and AM data transfer); ▪ RLC re-establishment.
Medium Access Layer (MAC)	MAC is specified in 3GPP TS 36.321 [9] and the main services and functions of the MAC sublayer include: ▪ Mapping between logical channels and transport channels; ▪ Multiplexing/demultiplexing of MAC SDUs belonging to one or different logical channels into/from transport blocks (TB) delivered to/from the physical layer on transport channels; ▪ Scheduling information reporting; ▪ Error correction through Hybrid ARQ (HARQ); ▪ Priority handling between logical channels of one UE; ▪ Priority handling between UEs by means of dynamic scheduling; ▪ Transport format selection; ▪ Padding.
Physical Layer (Layer 1)	Air Interface Physical Layer is specified in 3GPP TS 36.201 [10], 3GPP TS 36.211 [11], 3GPP TS 36.212 [12], 3GPP TS 36.213 [13] and 3GPP TS 36.214 [14]. The LTE air interface physical layer offers data transport services to higher layers. The access to these services is through the use of a transport channel via the MAC sub-layer. The physical layer is expected to perform the following functions in order to provide the data transport service: ▪ Error detection on the transport channel and indication to higher layers; ▪ FEC encoding/decoding of the transport channel; ▪ Hybrid ARQ soft-combining; ▪ Rate matching of the coded transport channel to physical channels; ▪ Mapping of the coded transport channel onto physical channels; ▪ Power weighting of physical channels; ▪ Modulation and demodulation of physical channels; ▪ Frequency and time synchronisation; ▪ Radio characteristics measurements and indication to higher layers; ▪ Multiple Input Multiple Output (MIMO) antenna processing; ▪ Transmit Diversity (TX diversity); ▪ Beamforming; ▪ RF processing.

1.2.2 LTE network elements

For the scope of this deliverable, the most relevant EPS architecture components related to security are depicted in Table 2.

Table 2: EPS architecture components and their security features

Component	Security Features
UE	The <i>User Equipment</i> allows a user access to network services. ▪ Ciphering, integrity and replay protection of NAS signalling; ▪ Ciphering, integrity and replay protection of RRC signalling; ▪ Ciphering of User Plane data at PDCP layer.
eNodeB	The evolved NodeB 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). ▪ Ciphering, integrity and replay protection of RRC signalling; ▪ Ciphering of User Plane data at PDCP layer.
MME	The <i>Mobility Management Entity</i> is the key control-node for the LTE access-network. The main security feature is ciphering, integrity and replay protection of NAS signalling.
HSS/AuC	The <i>Home Subscriber Server/Authentication Centre</i> is a database that contains user-related and subscriber-related information [89]. It also provides support functions in: ▪ mobility management; ▪ call and session setup; ▪ user authentication and access authorization.
AAA Server	Provides authentication, authorization, policy control and routing information to packet gateways. It performs EAP-SIM/AKA authentication of Subscriber Identity Module (SIM) devices directly to the Home Location Register (HLR)/HSS for a seamless and secure access to the networks.
ePDG	The <i>Evolved Packet Data Gateway</i> is responsible for interworking between the EPC and untrusted non-3GPP networks that require secure access, such as a Wi-Fi, LTE metro, and femtocell access networks.
SGW	The <i>Serving Gateway</i> is the point of interconnect between the radio-side and the 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 [89].
PDN-GW	The <i>Packet Data Network Gateway</i> is the point of interconnect between the EPC and the external IP networks, it routes packets to and from the PDNs. The PDN GW also performs various functions such as IP address / IP prefix allocation or Policy control and charging [89].
PCRF	The <i>Policy and Charging Rules Function</i> is responsible mainly for supporting the detection of service data flow, the charging system based on this data flow, and policy enforcement [96].

1.3 Overview of the LTE security architecture

The 3GPP TS 33.401 [15] divides the security architecture into five different groups or domains, as depicted in Figure 5 below. This division is useful in order to describe the different security features of EPS since each domain may have its own set of security threats and security solutions. A brief description of each security domain is given below, based on [16]:

- **Network access security (I):** security features that provide a user with a secure access to the EPS;
- **Network domain security (II):** features that allow different network nodes to securely exchange data and protect against attacks on the network between the nodes;
- **User domain security (III):** security features that secure the access to terminals, i.e. the usage of the Personal Identification Number (PIN);

- **Application domain security (IV):** security features used by applications such as HTTP (for web access) or IP Multimedia Subsystem (IMS);
- **Visibility and configurability of security:** this is the set of features that allows the user to learn whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

The next subchapters provide a more detailed description about each security domain and the main security features used in each one.

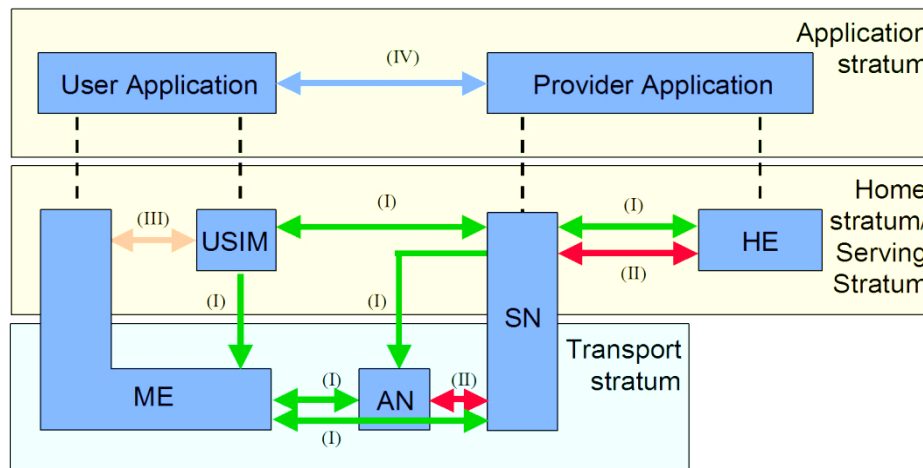


Figure 5: Overview of the security architecture [15].

1.4 Security features at each security domain

1.4.1 Network access security

The network access security domain focus on the security features that provide a user with a secure access to the EPS. This includes mutual authentication as well as privacy features, protection of signalling traffic and User Plane traffic (this protection may provide confidentiality and/or integrity protection). In short, at network access security domain the main security features are:

- User confidentiality (anonymity);
- Entity authentication;
- Data confidentiality;
- Data integrity.

A brief description of each security feature is given in the following subsections.

1.4.1.1 User confidentiality

In 3GPP TS 33.102 [17] three security features are provided which relate with user confidentiality (anonymity):

- **User identity confidentiality:** the permanent user identity (also known as *International Mobile Subscriber Identity* - IMSI) of a user to whom a service is delivered cannot be eavesdropped on the radio access link;
- **User location confidentiality:** the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link;
- **User untraceability:** an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

In order to achieve the features described above, the following mechanisms are used [17]:

- The user is normally identified by a temporary identity (known as *Globally Unique Temporary Identity* - GUTI) by which he is known by the visited serving network;

- The user should not use the same temporary identity for a long period of time;
- Any signalling or user data that might reveal the user's identity is encrypted on the radio access link.

1.4.1.2 Entity authentication

In LTE, the UE authenticates the network and the network authenticates the UE. This is called mutual authentication.

- **User authentication:** network authenticates the UE, network verifies if the connecting UE is who it claims to be.
- **Network authentication:** UE authenticates the network, verifies if it is connecting to the right network that he wants to connect.

The process of how mutual authentication is achieved in LTE is described in section 6.1 of TS 33.401 [15] and can be shortly described in the following steps:

- *Step 1:* the *Home Subscriber Server (HSS)/ Authentication Centre (AuC)* generates LTE authentication vectors;
- *Step 2:* HSS/AuC sends to the MME the vectors described above;
- *Step 3:* MME stores the *Access Security Management Entity Key (K_{ASME})* and the *expected result ($XRES$)* parameters and send towards UE the *authentication token ($AUTN$)*, the *random challenge ($RAND$)* parameters and the *Key Set Identifier of K_{ASME} (KSI_{ASME})*;
- *Step 4:* the UE uses the *Universal Subscriber Identity Module (USIM)* to compute local version of $AUTN$ using key K and compares it with the $AUTN$ received from MME. If they are consistent ($AUTN_{received\ from\ MME} = AUTN_{calculated\ by\ USIM}$), the USIM has successfully authenticated the network;
- *Step 5:* the UE sends to the MME the calculated *result (RES)* and the MME authenticates the terminal by verifying that $RES = XRES$.

Figure 6 summarizes this procedure.

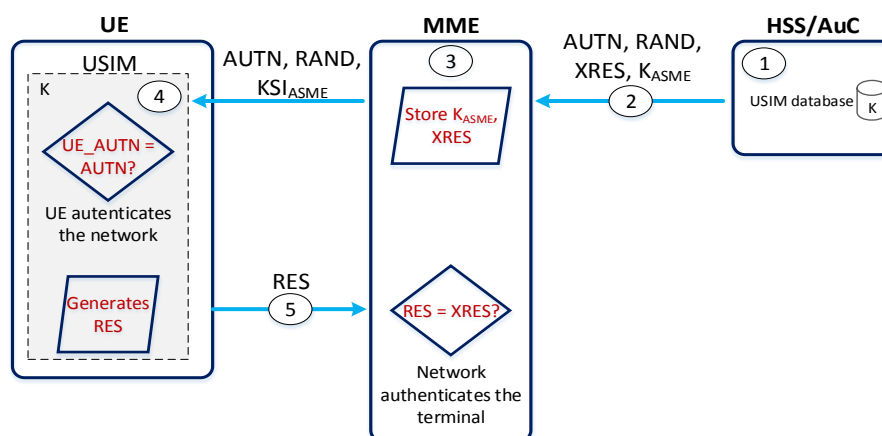


Figure 6: Mutual authentication procedure in LTE.

1.4.1.3 Confidentiality

The following security features are provided for data confidentiality on the network access link [17]:

- **Cipher algorithm agreement:** UE and the serving network (SN) can securely negotiate the algorithm that they shall use subsequently;
- **Cipher key agreement:** UE and the SN are able to agree on a cipher key that they may use subsequently;

- **Confidentiality of user data:** user data cannot be overheard on the radio access interface;
- **Confidentiality of signalling data:** signalling data cannot be overheard on the radio access interface;

Section 1.5.further details on how confidentiality is applied in LTE.

1.4.1.4 Data integrity

The following security features related to data integrity on the network access link are provided [17]:

- **Integrity algorithm agreement:** the UE and the SN can securely negotiate the integrity algorithm that they shall use subsequently;
- **Integrity key agreement:** the UE and the SN agree on an integrity key that they may use subsequently;
- **Data integrity and origin authentication of signalling data:** the receiving entity (UE or SN) is able to verify that signalling data has not been modified in an unauthorised way since it was sent by the sending entity (SN or UE) and that the data origin of the signalling data received is indeed the one claimed;

Section 1.6 further details on how data integrity protection is applied in LTE.

1.4.2 Network domain security

LTE contains many network entities and reference points between these entities. The network domain security refers to the features that allow these network nodes to securely exchange data and protect against attacks on the network between the nodes. The protection between network nodes can be provided by the *Network Domain Security for IP-based control planes (NDS/IP)*. The 3GPP TS 33.210 [97] contains the specifications for the NDS/IP. A case of special relevance to EPS and E-UTRAN is the S1-U interface between EPC and the E-UTRAN. This interface needs to be properly protected (physically and/or by NDS/IP) since the user plane data protection would otherwise be terminated in the eNodeB, potentially exposing sensitive data on S1 [16].

1.4.3 User domain security

At the current LTE specification (Release 12), the *user domain security* refers to the set of security features that secure the access to terminals. Currently the only defined user domain security feature is related to the *Personal Identification Number / PIN unlock key (PIN/PUK)* code before being able to access the terminal, as specified in [16].

1.4.4 Application domain security

Application domain security consists in the security features used by applications such as HTTP (for web access) or IMS. In [16] is also referred that application domain security is in general applicable end-to-end, between the application in the terminal and the peer entity providing the service. This is in contrast to the previous security features listed, which provide hop-by-hop security, meaning they apply to a single link in the network only. If each link (and node) in the chain that requires security is protected, the whole end-to-end chain can be considered secure.

1.4.5 Visibility and configurability of security

In [16] the “Visibility and configurability of security” is described as the set of features that allows the user to learn whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature. In most cases the security features are transparent to the user and the user is unaware that they are in operation. In [16] is also referred that for some security features the user should however be informed about the operational status. For example, usage of encryption in E-UTRAN depends on operator configuration and it should be possible for the user to know whether it is used or not, for example, by a symbol on the terminal display.

Configurability is the property that the user can configure whether the use or the provision of a service should depend on whether a security feature is in operation [16].

1.5 Confidentiality

Confidentiality prevents sensitive information from reaching the wrong people, while making sure that the right people can in fact get it [90]. In LTE, almost all data (mainly the Control Plane) is confidentiality protected. There are (up to date), four EPS Encryption Algorithms (EEA) that can be used to provide data confidentiality. Each is assigned a 4-bit identifier – which leaves space for 12 additional encryption algorithms for future releases. Currently, the following values have been defined for NAS, RRC and UP ciphering [15]:

- 0000_2 – EEA0 (Null cyphering algorithm)
- 0001_2 – 128-EEA1 (SNOW 3G based algorithm)
- 0010_2 – 128-EEA2 (AES based algorithm)
- 0011_2 – 128-EEA3 (ZUC based algorithm)

Table 3: LTE confidentiality algorithms

Algorithm	Description
EEA0 (Null cyphering algorithm)	This cyphering option <u>provides no security protection</u> , so this option should be avoided whenever possible. The EEA0 algorithm implementation should generate a KEYSTREAM of all zeroes with length equal to the LENGTH input parameter and all processing performed in association with ciphering shall be exactly the same as with any of the remaining ciphering algorithms [15].
128-EEA1 (SNOW 3G based algorithm)	128-EEA1 is based on SNOW 3G and <u>is identical to UEA2</u> , the 3GPP <u>confidentiality algorithm used in UMTS</u> , as specified in 3GPP TS 35.215 [91] ("Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications").
128-EEA2 (AES based algorithm)	128-EEA2 is based on 128-bit Advanced Encryption Standard (AES) algorithm [1] in Counter (CTR) Mode [16]. The AES algorithm is a <u>symmetric block cipher</u> capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. In LTE only 128 bit keys are used to encrypt data [18]. A detailed description about AES and CTR mode of operation is given in [18] and [19] respectively.
128-EEA3 (ZUC based algorithm)	128-EEA3 is based on ZUC and specified in [35]. ZUC is a word-oriented <u>stream cipher</u> . It takes a 128-bit initial key and a 128-bit initial vector as input, and outputs a key stream of 32-bit words (where each 32-bit word is hence called a key-word).

The use of "null cyphering algorithm", EEA0, on RRC is only allowed for the situations described in [22], i.e. an unauthenticated UE for which the establishment of emergency bearer services is allowed.

All the above mentioned algorithms use a 128-bit input key except the Null ciphering algorithm.

The procedures and building blocks for the encryption and decryption operations at the LTE sender and the receiver are depicted in Figure 7.

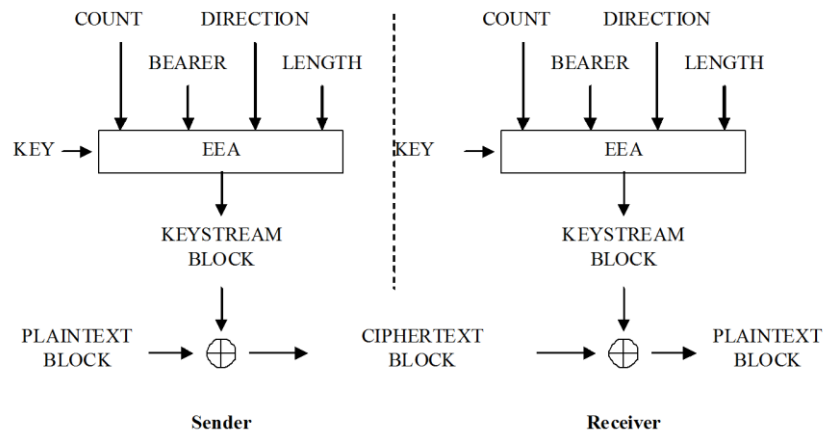


Figure 7: Procedures and building blocks for the ciphering of data in LTE [15].

1.6 Integrity protection

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people [90]. In LTE, almost all data (mainly the Control Plane) is integrity protected. There are (up to date), four EPS Integrity Algorithms (EIA) that can be used to provide Integrity protection. Each EPS Integrity Algorithm will be assigned a 4-bit identifier. Since 4-bit are assigned to each EPS Integrity algorithm and only 4 algorithms are used, it means that more 12 integrity algorithms can be added in future releases of LTE. Currently, the following values have been defined [15]:

- 0000₂ – EIA0 (Null Integrity protection algorithm)
- 0001₂ – 128-EIA1 (SNOW 3G based algorithm)
- 0010₂ – 128-EIA2 (AES based algorithm)
- 0011₂ – 128-EIA3 (ZUC based algorithm)

Table 4: LTE Integrity algorithms

Algorithm	Description
EIA0 Null integrity protection algorithm	The “Null integrity protection algorithm” EIA0 <u>provides no integrity protection</u>, and should be avoided whenever possible. According to [15], in the situations where EIA0 has to be applied, the following should be taken into account: The EIA0 algorithm shall be implemented in such way that it shall generate a 32 bit MAC-I/NAS-MAC and XMAC-I/XNAS-MAC of all zeroes; Replay protection shall not be activated when EIA0 is activated. All processing performed in association with integrity (except for replay protection) shall be exactly the same as with any of the integrity algorithms specified above except that the receiver does not check the received MAC.
128-EIA1 SNOW 3G based algorithm	128-EIA1 is based on SNOW 3G as described in the previous section and is <u>implemented in the same way as UIA2 in UMTS</u> . A detailed description on implementation of UIA2 can be found in [20].
128-EIA2 AES based algorithm	128-EIA2 is <u>based on 128-bit AES</u> as described in the previous section, but for integrity protection AES works in Cipher-based MAC (CMAC) mode. A detailed description about CMAC is given in [21].
128-EIA3 ZUC based algorithm	RRC (between UE and eNodeB) and NAS (between UEs and MMEs) signalling integrity protection shall be provided by 128-EIA1 or 128-EIA2 algorithms. <u>Usage of 128-EIA3 for integrity protection can be used but should be avoided</u> [15].

Figure 8, depicts the procedures and building blocks for the integrity operations at the LTE sender and receiver.

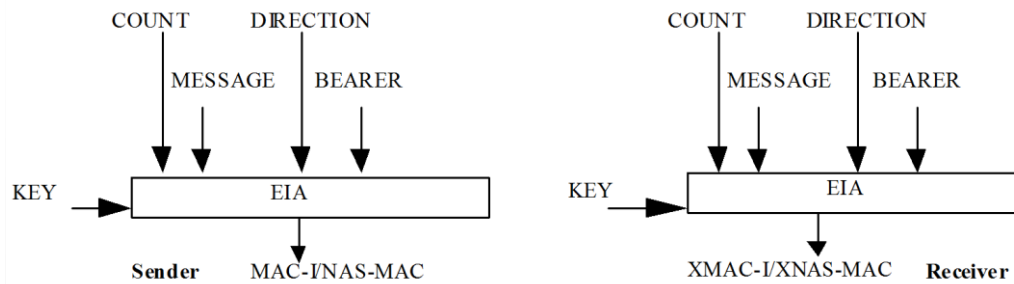


Figure 8: Derivation of MAC-I/NAS-MAC (or XMAC-I/XNAS-MAC) [15].

The use of "null integrity protection algorithm", EIA0, on RRC is only allowed for the situations described in [22], i.e. an unauthenticated UE for which the establishment of emergency bearer services is allowed.

All NAS signalling messages except those explicitly listed in TS 24.301 [23], as exceptions, shall be integrity-protected. EIA0 shall also not be used for integrity protection between a Relay Node (RN) and a Donor eNB (DeNB).

It is important to note that the User plane packets between the UE and the eNodeB should not be integrity protected on the Uu interface as described in [15]. The motivation for such recommendation is related to the fact that higher layer protocols (including applications) should do such control. As an example, audio and video applications, which may use UDP (loss tolerant), may not want layer 2 retransmissions due to frame integrity check errors.

1.7 EPS Key hierarchy

The EPS key hierarchy is triggered as soon as the identity of the mobile subscriber (i.e. GUTI or IMSI) is known by the MME. The multiple keys within the EPS Key hierarchy are obtained through a procedure known as the *Authentication and Key Agreement* (AKA). This procedure can be initiated by the network as often as the network operator wishes and, when triggered, the AKA procedure results in a new main key, known as K_{ASME} , that is stored both in the UE and the MME (additional information on the AKA procedures can be found on section 1.4.1.2 and also the 3GPP TS 33.401 [15]). The K_{ASME} is then used to derive the NAS, KeNB, RRC and UP keys using a Key Derivation Function (KDF), as specified in 3GPP TS 33.220 [92]. To increase key security, three main enhancements were considered in E-UTRAN [16]:

- Stronger key separation between networks and key-usage;
- Larger key sizes. E-UTRAN supports not only 128-bit keys but can (in future deployments) also use 256-bit keys;
- Increased protection against compromised base stations. Through the use of the forward/backward security, the air interface keys are updated each time the UE changes its point of attachment (or when the UE changes from IDLE to ACTIVE).

After a successful AKA procedure the encryption and integrity protection keys shall have been distributed according to the hierarchy depicted in Figure 9. As it can be seen, the main key in E-UTRAN is K_{ASME} . This key shall be created only by running a successful AKA as explained in [15]. In case the UE does not have a valid K_{ASME} , a key set identifier, known as KSI_{ASME} , with value "111", shall be sent by the UE to the network, which can initiate a (re)authentication procedure to get a new K_{ASME} .

Key refresh can also occur when the volume of packets exchanged by the PDCP protocol, in a specific radio channel (known as Radio Bearer), reaches a maximum threshold. This threshold

is related to the full cycle of the counter associated with the PDCP protocol (known as PDCP COUNT). Rekeying can also occur when an EPS NAS security context, different from the currently active one, is to be activated or during a handover. The model for the handover key chaining is provided in [15].

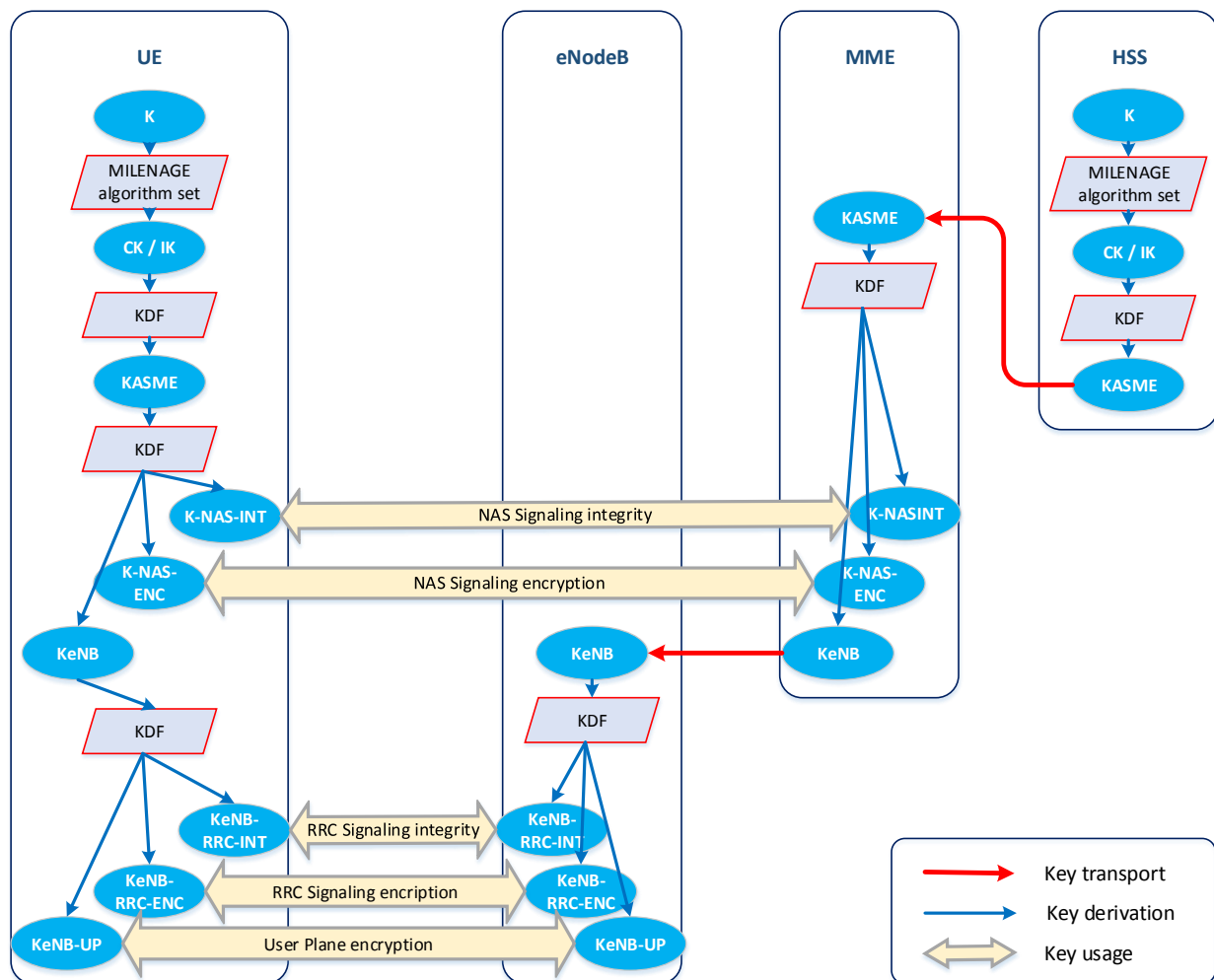


Figure 9: EPS Key Hierarchy and Radio Interface Security (based on [2]).

1.8 Support of multiple access technologies

To bring convergence using a unique core network providing various IP-based services over multiple access technologies, 3GPP defined how the interworking is achieved between an E-UTRAN (LTE and LTE-Advanced), GERAN (radio access network of GSM/GPRS) and UTRAN (radio access network of UMTS-based technologies WCDMA and HSPA). The UE can also use non-3GPP technologies (e.g. WiMAX, CDMA2000, Wi-Fi, or fixed networks) to interconnect to the 3GPP EPC. Even though the 3GPP specification clearly don't mention interconnection with traditional Professional Mobile Radio (PMR) technologies, such as TETRA and TETRAPO, current market trends indicate such capability has the potential to be standardized in the next few years [24][25].

Non-3GPP accesses can be split into two categories as described in [26]: the "trusted" and the "untrusted" (as depicted in Figure 1):

- **Trusted non-3GPP** accesses can directly interact with the EPC;
- **Untrusted non-3GPP accesses** interwork with the EPC via a network entity called the *evolved Packet Data Gateway* (ePDG). The main role of the ePDG is to provide security mechanisms such as IPSec tunnelling for connections with the UE over untrusted non-3GPP access. It is important to note 3GPP does not specify which non-3GPP

technologies should be considered trusted or untrusted. This decision is made by the operator (clause 4.3.1.2 of [5]).

A summary description on how AKA is performed for the different accesses is provided in the following section.

1.8.1 Interworking with GERAN/UTRAN

Every time a UE enters a new access domain a new authentication and key agreement procedure occurs. In order to reduce handover delay, native (or cached) or mapped security contexts can be used. If the UE has previously been active in E-UTRAN access then moved to GERAN/UTRAN and later return to E-UTRAN, the UE and network may have cached a native security context for E-UTRAN (from the previous time the UE was in E-UTRAN) in order to avoid the need of a full AKA procedure during handover. If a native context is not available (considering the scenario where a UE is moving from UTRAN to E-UTRAN), the UE and MME may derive keys applicable to E-UTRAN access (e.g. K_{ASME}) based on keys used in UTRAN access (e.g. CK, IK) [16]. The derivation of K_{ASME} from CK and IK was explained in section 1.7. An example of such mapping is illustrated in Figure 10.

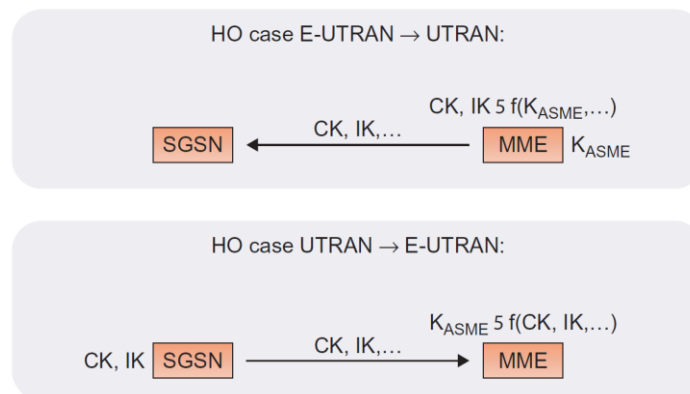


Figure 10: Mapping security context in handover between E-UTRAN and UTRAN [16].

1.8.2 Access security in trusted non-3GPP accesses

As stated before, LTE allows different networks to provide access to EPC. One example of a non-3GPP network that has access to EPC is the evolved High Rate Packet Data (eHRPD), the eHRPD and its security features are specified by 3GPP2 [93]. The eHRPD has the capabilities to provide a strong access control, mutual authentication as well as protection of signalling and user plane traffic sent over the HRPD radio link, thus can be considered that eHRPD has sufficient security features for providing access to EPC. As an example, the access authentication between E-UTRAN and eHRPD is based on EAP-AKA' [27]. EAP-AKA' runs between the UE and 3GPP AAA Server (Figure 11). In order to perform the AKA-based authentication, the 3GPP AAA Server downloads the Authentication Vector from HSS/AuC.

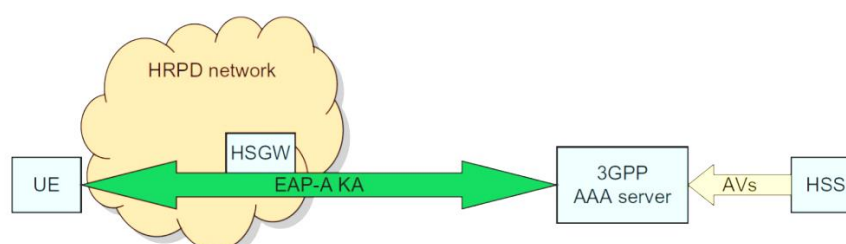


Figure 11: EAP-AKA' based access authentication for eHRPD [16]

1.8.3 Access security in untrusted non-3GPP access

The LTE specification also allows for untrusted networks to be connected to the LTE EPC. Wireless Local Area Networks (WLAN), commonly known as Wi-Fi networks, are a good example of a 3GPP untrusted network. The reason is that WLAN networks can be used in many

different scenarios such as corporate, home or public environments. Each scenario can use different security levels, for example, home and corporate use commonly use Wi-Fi Protected Access (WPA) or WPA2 security solutions. In public places, however it is common to turn off WLAN security. In this case the WLAN access does not provide any user plane encryption or integrity protection and is vulnerable to many types of attacks. Depending on the security level applied on these networks, the access can be considered trusted or untrusted, but the decision is always made by the operator once the 3GPP does not specify which non-3GPP technologies should be considered trusted or un-trusted [16].

In an untrusted scenario the solution to provide a user to connect securely with EPC, and solve the absent or very limited security environment in the WLAN, is to set up an IPSec tunnel between the UE and the ePDG as depicted in the Figure 12:

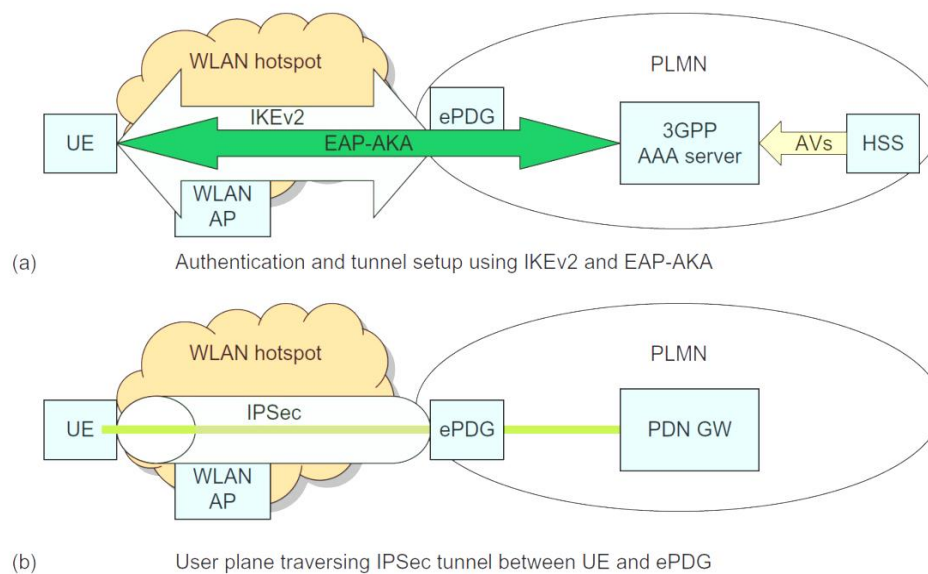


Figure 12: (a) Authentication using IKEv2 and EAP-AKA between UE and ePDG; (b) User plane traffic is protected in IPSec tunnel between UE and ePDG [16]

Once the UE has connected to the WLAN it can discover the ePDG IP address using a DNS server. The IPSec tunnel between the UE and ePDG is established using the IKEv2 protocol [28]. The authentication of the ePDG is based on digital certificates during the IKEv2 procedures and the UE is authenticated in a similar manner as for E-UTRAN (based on the credentials on the USIM). The EAP-AKA' procedure occurs in a similar manner as described in the previous section, but in this situation it happens as part of IKEv2.

1.9 Proximity Services (ProSe) - LTE for Public Safety

Currently, two major wireless wide-area communications technologies exist:

- Commercial cellular networks
- Dedicated public safety systems

Commercial cellular networks are characterized by meeting the needs of consumer and business users. By reaching a large number of users, these cellular networks led to excellent economies of scale and constant rapid innovation. This environment has produced advanced standards such as LTE that provides multi-megabit per second data rates and multimedia capabilities as well as traditional voice and messaging services. Public safety networks, on the other hand, have the main goal to provide mission critical communications services for public safety users. To accomplish the specific requirements for this type of communications, these networks need to be highly robust and resilient as well provide a strong and robust security environment [2]. Establishing common technical standards between these two technology families offers advantages to both communities. Public safety networks would receive more

investment and cellular networks could take advantage of some features only available yet in public safety networks (e.g. group calls or device-to-device (D2D) communications).

3GPP in collaboration with other groups such as ETSI TC TETRA, TCCA and US National Institute of Standards and Technology (NIST) are jointly working to deliver Public Safety communications on top of LTE [29]. 3GPP is already working in two main areas in Release 12¹:

- Proximity services (ProSe) that identifies mobiles in physical proximity and enables optimized device-to-device communications, even without infrastructural support.
- Group call system enablers (GCSE) that support the fundamental requirement for efficient and dynamic group communications operations such as one-to-many calling and dispatcher working.

Proximity Services intend to satisfy two main groups: the commercial area and the public safety users. In the commercial area proximity services can support features like new modes of social networking, convenient file transfer between devices belonging to the same user and targeted advertising [29]. In the public safety area, ProSe meets the need for communication among public safety users and includes some features like: "User equipment to network relay", where one mobile acts as a relay for another and provides access to network services outside the normal network coverage area or "User equipment to user equipment relay" where one mobile acts as a relay point between two others and allows communication to take place without going via the network even if the communicating mobiles are out of range for direct communication [29]. LTE Proximity services consist of two main elements:

- Network assisted discovery of users with a desire to communicate, who are in close physical proximity.
- Facilitation of direct communication between users with, or without, supervision from the network.

In order to save network resources and also to allow communications in areas outside network coverage ProSe can use direct communications. Direct communication means a radio connection is established between the users' mobiles without transiting via the network, see Figure 13 a). If the UE is out of coverage (out of range for direct communication), a relay can be used in order to establish (maintain) communication, as depicted in Figure 13 b):

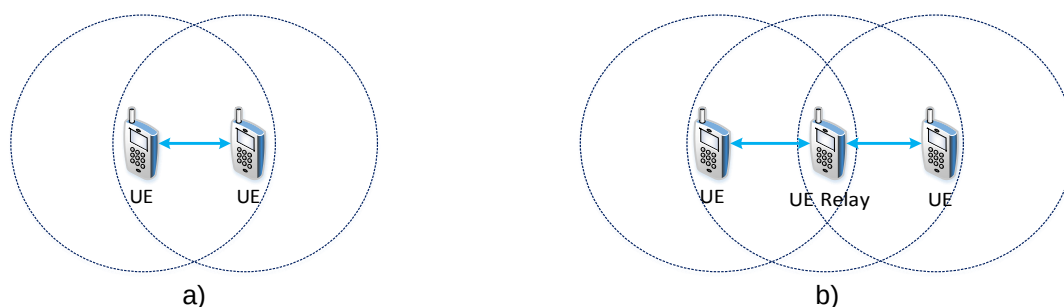


Figure 13: a) ProSe direct communication; b) UE to UE relay

In the "User equipment to network relay" (that has been described before), one mobile acts as a relay for another and provides access to network services outside the normal network coverage area, Figure 14 a) illustrates this scenario.

¹ There are currently 2 other areas being worked out in Release 13 for isolated E-UTRAN operations (IOPS) - this mimics the fallback mode of TETRA / TETRA POL - and mission critical push-to-talk (PTT) over LTE (MC PTT).

When using group communications in the "User equipment to network relay" scenario, the ProSe envisages this scenario to be extended to "Group to network relay", where the group is out of network coverage, as depicted in Figure 14 b).

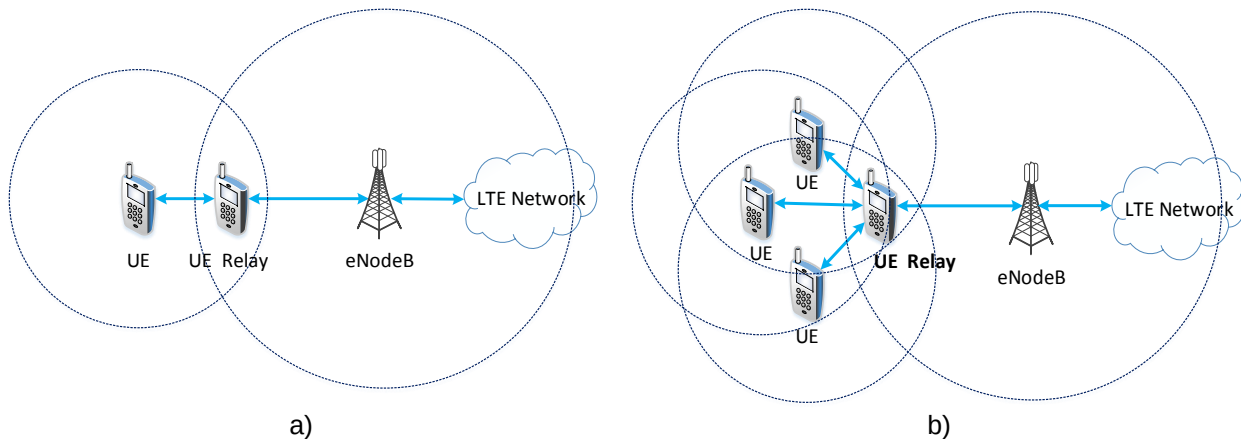


Figure 14: a) User Equipment to network relay; b) Group to network relay

1.9.1 ProSe Security, Authorization and Privacy Requirements

According to 3GPP TS 22.278 [30], the main requirements related with security, authorization and privacy that EPS shall support for ProSe are listed in Table 5:

Table 5: ProSe Security, Authorization and Privacy main requirements [30].

Regulatory requirements	When operating ProSe in general or public safety cases: - EPS shall support regional or national regulatory requirements (e.g. lawful interception, Public Warning System (PWS)); - ProSe shall respect local regulatory frameworks on the use of licensed spectrum.
Confidentiality and integrity requirements	- User data and signalling data over the ProSe communication path shall have a security level comparable with that provided by the existing 3GPP system. A mechanism shall be provided to ensure the confidentiality and integrity of user data and signalling over the ProSe Communication path for Public Safety UEs not served by E-UTRAN; - Whenever possible and appropriate existing 3GPP security mechanisms shall be reused, but the level of security provided by the existing EPS shall not be adversely affected when ProSe is enabled; - The EPS shall protect the confidentiality of the subscriber's UE's, and user's permanent identities used in the EPS when ProSe Discovery and/or ProSe E-UTRA communication are used.
Operator features	The operator shall be able to: - Enable or disable its ProSe Discovery feature; - Authorise discovery operations for each individual ProSe-enabled UE, including by pre-provisioning of the UE; - Authorise the ability of a ProSe-enabled UE to be discoverable and to discover other ProSe-enabled UEs; - Authorise the use of ProSe Discovery information by an application; - Authorise the ability of a ProSe-enabled UE to discover ProSe-enabled UEs served by the E-UTRAN of other PLMNs.

1.10 Group Communication Service Enablers for LTE (GCSE_LTE)

A *Group Communication Service* is intended to provide a fast and efficient mechanism to distribute the same content to multiple users in a controlled manner. As an example, the concept of group communications is used extensively in the operation of classical PMR systems used for, but not limited to, public safety organizations. At the moment, the primary use of a *Group Communication Service* in PMR is to provide "Push to Talk" (PTT) functionality, so a *Group Communication Service* based on 3GPP architecture, using LTE radio technology should enable PTT voice communications with at least comparable performance.

The GCSE_LTE service should allow flexible modes of operation as the users and the environment they are operating in evolves. For example, LTE capabilities allow for broadband communication, so *Group Communication Service* is expected to support group voice, video or data communication. Also GCSE_LTE envisages allowing users to communicate to several groups at the same time in parallel, e.g. voice to one group or different streams of video or data to several other groups.

The users of the *Group Communication Service* are organised into groups, where a user can be member of more than one group (see Figure 17). The overall view of the high level architecture for GCSE_LTE is depicted in Figure 15.

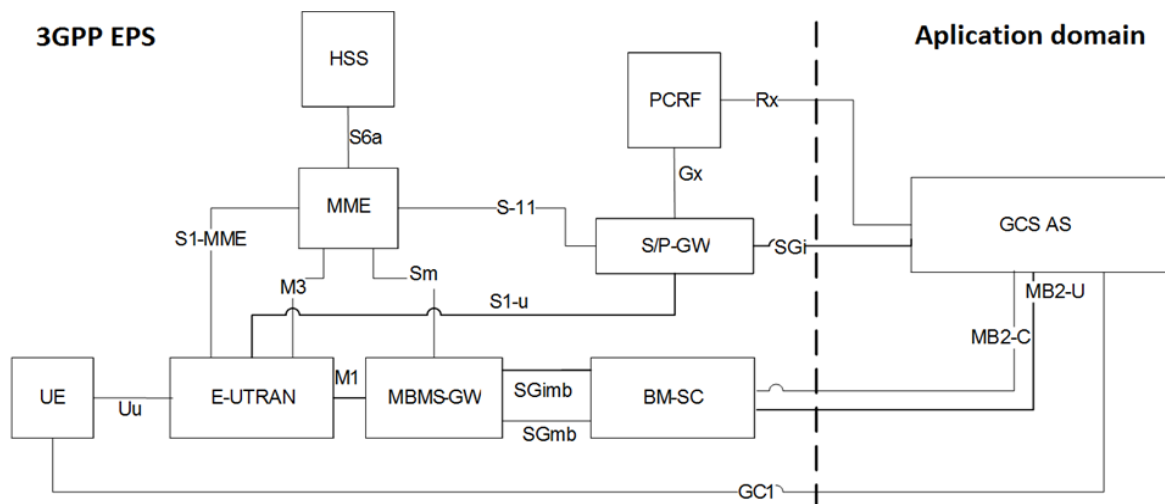


Figure 15: High-level architecture for GCSE_LTE [95].

The high-level GCSE_LTE architecture diagram presented in Figure 15 consists of Application domain and the 3GPP EPS domain. The Application domain contains the *Group Communication Service Application Server* (GCS AS). In the 3GPP EPS domain two modules were added for GCSE_LTE, the *Broadcast Multicast Service Centre* (BM-SC) and Evolved Multimedia Broadcast Multicast Services (eMBMS) Gateway (MBMS-GW). The BM-SC provides membership, session and transmission, proxy and transport, service announcement, security, and content synchronization while the MBMS-GW has as main goals to distribute MBMS user plane data to eNBs using IP multicast, and performs MBMS session control signalling towards the E-UTRAN via MME [95].

The GCS AS may use the GCSE_LTE for providing a GCS [95], as depicted in Figure 16 below. The GCS AS can distribute data in two different ways:

- Unicast – the data is sent to a single network destination identified by a unique address;
- eMBMS – data can be transmitted to more than one device, i.e. to a group of devices.

Even though UEs can be connected to the same eNodeB, different delivery modes may be used. For example, unicast may be used when an UE is in an area where the MBMS signal strength is weak [95]. Note that Figure 16 only illustrates the main purpose of GCSE_LTE, the

interworking between GCSE_LTE and ProSe is considered in Figure 17. Also, while in Figure 16 the scenario refers more to an application delivering data to users, in Figure 17 the main goal is the exchange of data between users within groups. In this scenario the users are combining the GCSE_LTE with the ProSe features.

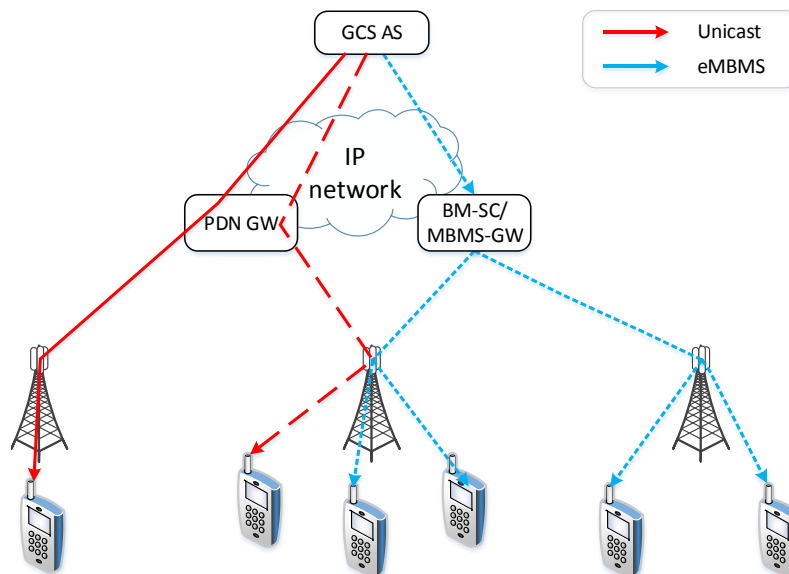


Figure 16: Media traffic with unicast and MBMS on Downlink [95].

1.10.1 Interworking between GCSE_LTE and ProSe

As discussed before, the GCSE_LTE should allow using the ProSe features. In the presented scenario Figure 17 it can be seen the users using ProSe functionalities with the GCSE_LTE features at the same time. Figure 17 illustrates some scenarios where the ProSe and GCSE_LTE can be used in conjunction – includes features for communications between devices to devices and devices to network.

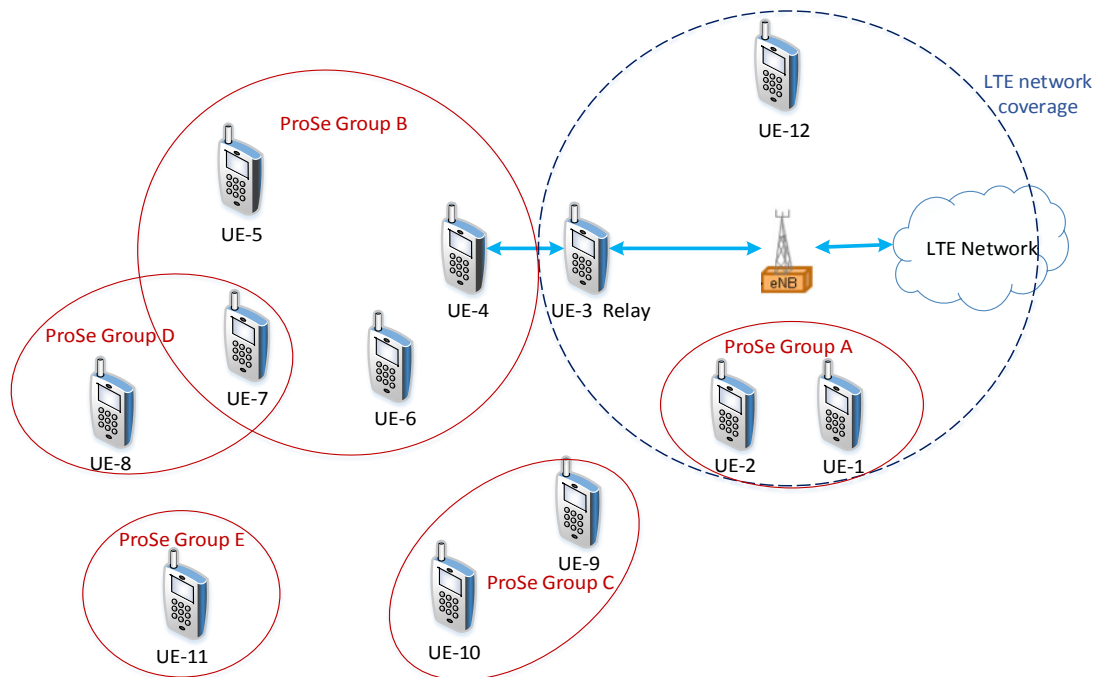


Figure 17: ProSe-enabled UEs arranged in ProSe Groups (based on [94]).

Five groups can be identified in Figure 17:

- ProSe Group A: constituted by UE-1 and UE-2, group elements are under network coverage but do not receive network data;
- ProSe Group B: constituted by UE-4, UE-5, UE-6 and UE-7, group elements are outside network coverage but they can receive data through UE3 (relay to UE-4);
- ProSe Group C: constituted by UE-9 and UE-10, all the group elements are outside network coverage and do not receive network data;
- ProSe Group D: constituted by UE-7 and UE-8, group elements are outside network coverage but they can receive network data through ProSe Group B once UE-7 belongs to both ProSe Group D and ProSe Group B.
- ProSe Group E: constituted only by UE-11, group element is outside network coverage and is the only group element.

Note that: UE-7 belongs to more than one group, so UE-7 is able to communicate both in ProSe Group B and ProSe Group D; UE-12 does not belong to any ProSe group, so it will not be able to participate in any group communication; UE-11 is the only device in ProSe Group E, this way it will not participate in any group communication once it is the only device in that group.

1.10.2 Security requirements for Group Communication

Since security is a very important issue in critical communications such as public safety, security for group communication needs to be considered [43]. According to 3GPP TS 22.468 [32], the system shall support at least the same security level (e.g. for authentication, integrity, confidentiality and privacy) for group communication as a 3GPP LTE packet data bearer. The most relevant (up to date) 3GPP document related with security for GCSE_LTE is the 3GPP TR 33.888 [43]: “Study on security issues to support Group Communication System Enablers (GCSE) for LTE”. At the moment this document was written, the 3GPP TR 33.888 was under development by 3GPP.

1.10.3 Interaction with emergency calls and ProSe

The ability for a UE to make an emergency call shall be unaffected by being in a group communication. If the network supports ProSe and GCSE, the following scenarios should be taken into account [32]:

- EPC and E-UTRAN shall be able to make use of ProSe Group Communication and the public safety ProSe UE-to-Network Relay for Group Communication;
- A public safety ProSe-enabled UE not served by E-UTRAN shall be able to support Group Communication based on ProSe Communication paths;
- A public safety ProSe UE-to-Network Relay shall be able to relay Group Communication to/from ProSe Communication paths;
- GCSE Group Members shall be able to access Group Communication services using ProSe Communication paths and/or by EPC Path.

1.11 LTE security vulnerabilities

The information on this subsection has been considered security sensitive and it has been moved to D5.1 RESTREINT UE Annex, which is a separated document (SALUS_D5.1_Annex.docx)

2 SECURITY AND PRIVACY ANALYSIS OF TETRAPOL

2.1 TETRAPOL Architecture

2.1.1 System terminal

A general TETRAPOL System Terminal (ST) is the service access reference point provided to the user by the system, it may be:

- A mobile termination (MT);
- A line termination (LT).

The system terminal may be split into different entities:

- A terminal;
- A MT also called radio terminal (RT);
- A line connected terminal (LCT) also called the LT;
- A user data terminal (UDT) also called a terminal equipment (TE) connected to the MT or LT;
- A subscriber identity module (SIM).

The LT and UDT are called the Line Station (LS) and the MT and UDT are called the Mobile Station (MS). Internally a MT or LT can be split into the following entities described in the TETRAPOL Publicly Available Specifications (PAS):

- A CODEC for voice coding and decoding;
- An encryption entity for voice and data end-to-end encryption, where TETRAPOL provides the algorithms (algorithms are only provided by the custodian under controlled conditions);
- An authentication entity for authentication of the MT to the network, where TETRAPOL provides the algorithms (algorithms are only provided by the custodian under controlled conditions);
- A chipset including an ASIC (ARM processor and a digital signal processor) and a RF part.

Figure 18 shows the different TETRAPOL mobile entities:

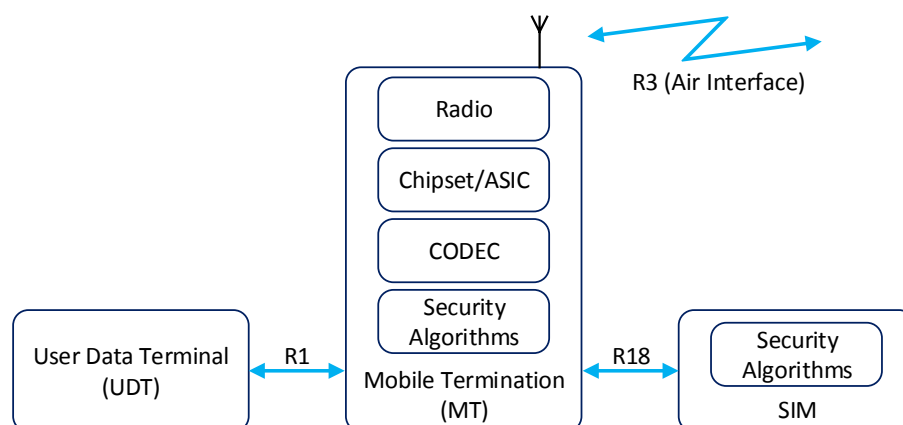


Figure 18 - TETRAPOL Mobile entities

2.1.2 ISO services distribution

TETRAPOL offers services defined as bearer, tele and supplementary services conforming to ISO as represented on Figure 19:

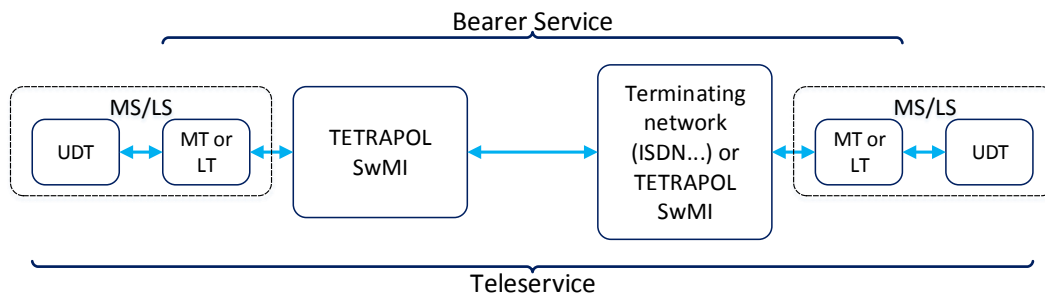


Figure 19 - Tele and bearer services

The terminating network may be a TETRAPOL network or an ISDN, PDN network.

2.1.3 TETRAPOL users

The services offered by a TETRAPOL system, concern different types of users, as explained in the following subsections.

2.1.3.1 Mobile users

A Mobile user has a RT with or without a SIM (Subscriber Identity Module), connected optionally to a UDT like a PC. Services offered are different depending of the working mode: network mode (communications through the fixed infrastructure) or direct mode (directly from terminal to terminal or extended through a repeater). A combination of the two modes is possible called dual watch for a direct mode mobile under network coverage or through a radio gateway as represented in Figure 20.

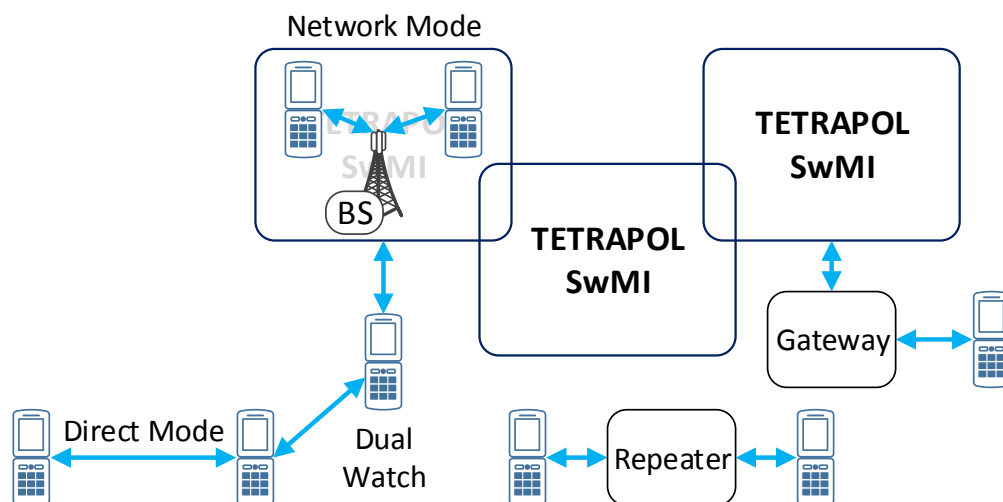


Figure 20 - Network and direct mode

2.1.3.2 Line connected users

Line connected users are connected through fixed lines to the Network with different types of Services offered:

- LCT user: this type of user has the same services offered to the mobile user but his terminal is connected through a fixed line through eventually an external network to TETRAPOL.
- Standalone dispatch position (SADP) user: this type of user has the same services offered to the LCT user plus some extra specific services (for example group merging, disable) and supplementary information (for example localisation) by mean of a connection to the operation and maintenance center (OMC).

- PABX users: are connected to an external PABX with standard Q signalling² (QSIG) services available;
- Dispatch Center (Dispatch Position) users: the operators or operational managers in a dispatch Center have all the SADP user services plus specific data and facilities for display and interrogation (for example network and cell configuration, location, others).
- Other users:
 - Network Management users: access Network Management services from different Network Management Terminals for example technical and tactical.
 - Inter system interface (ISI) users: the services offered across two TETRAPOL networks to users are a subset of the mobile user services. The services are also a subset for TETRAPOL - GSM 2+/TETRA users.

Gateways should offer services to external network users. In TETRAPOL they concern PSTN, ISDN, PDN, TCP IP. Figure 21 shows the location of the different types of users.

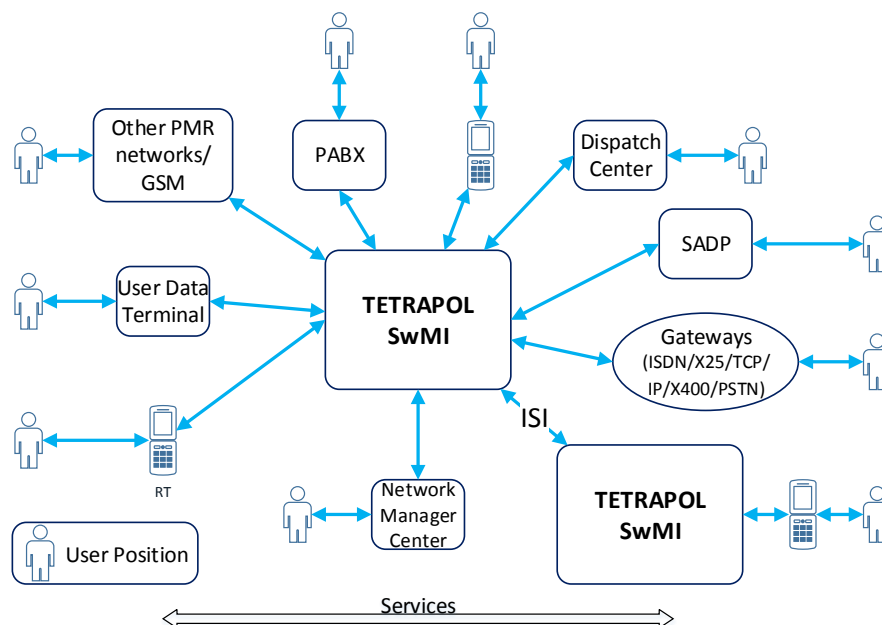


Figure 21 - TETRAPOL users' positions

2.1.4 Service table

Three working modes are considered:

- Network mode;
- Direct mode;
- Repeater mode.

For each mode the available voice teleservices and data services are:

- Individual call;
- Multiparty call;
- Talk group;
- Group call;
- Open channel;
- Emergency call;
- Broadcast call;

² QSIG - a protocol for Integrated Services Digital Network (ISDN) communications based on the Q.931 standard. It is used for signalling between digital private branch exchanges (PBXs).

- PABX call;
- Status;
- TCP/IP access.

For each teleservices and data services the following information is given :

- Voice Supplementary services;
- Data bearer services (Packet, connectionless...);
- Data services and facilities;
- Data applications (messaging...);
- Security services;
- Procedures (Registration...).

2.2 TETRAPOL security principals

2.2.1 End-to-end ciphering

Usually, safety force users work in groups, a user must be able to join an encrypted conference without waiting for unpredictable external synchronisation of the ciphering mechanism. Therefore the system uses a self-synchronising encryption algorithm which authorises fast 'late entry' into communications, for example in Group calls.

2.2.2 Mutual authentication

To avoid masquerading intrusion, periodically, or on request of the operator, the network authenticates the terminal and the terminal authenticates the network.

2.2.3 Signalling protection

In order to avoid traffic analysis by eavesdroppers, a temporary identity allocated by the network is used instead of the real subscriber address. Signalling is scrambled and due to digital vocoding, channel coding even in clear voice is very difficult to analyse. This method allows to avoid having security elements in the BS which would be the case if air interface encryption was done (Base Stations are not well protected due to the number of sites for example). As an option, air interface encryption may be added between the mobile and the BS depending of the requirements.

In some cases, detection of radio activity could indicate to hostile listeners that something is happening. To maintain apparent traffic during lulls, TETRAPOL control channels automatically insert dummy frames on the control channel link from base station to mobile.

2.2.4 Remote disabling of terminals

In case of doubt, the TETRAPOL operator can disable a terminal either temporarily or permanently (physical erasure) without the user noticing.

2.2.5 Automatic rekeying

The user does not need to perform any action for communication key loading. The system is fully automatic (over the air rekeying) and secure. All keys are transmitted and recorded in encrypted form.

2.2.6 Automatic network reconfiguration

Automatic network reconfiguration guarantees permanently and automatically the availability of services, by redundant critical components, automatic fall back mode, permanent OMC supervision of the network and dynamic reallocation of channel. This mechanism analyses the level of availability of components and determines the optimum use of resources.

2.2.7 Access control

This feature controls access to equipment by smart cards or passwords. Additional facilities include remote detection of physical intrusions and alarms to operators.

2.2.8 Subscriber Identity Module

As an option, a subscriber identity card (SIM) may be used conforming to ISO 7810, 7811 and 7816. A user profile mapping is defined with a PIN code control and authentication to the network. Other configurations are possible if public keys are used.

2.2.9 Encryption diversity

Multiple algorithms are permitted for end to end encryption, for example a national algorithm and a multinational algorithm can be implemented for roaming.

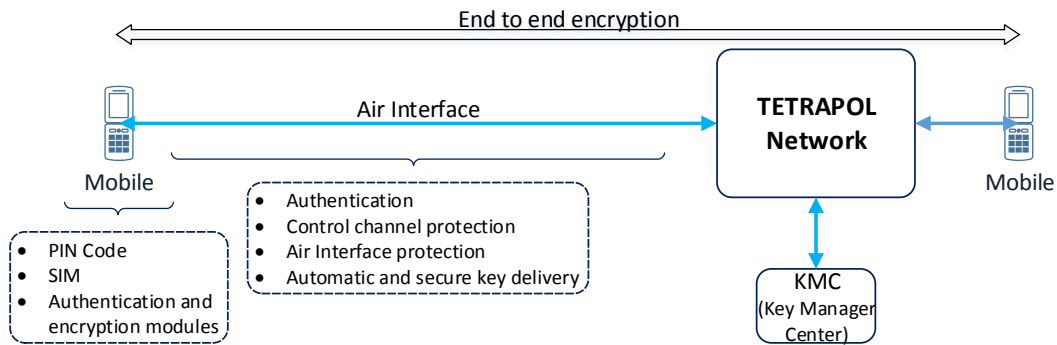


Figure 22 - TETRAPOL Security Mechanisms

3 SECURITY AND PRIVACY ANALYSIS OF TETRA

TETRA has been designed with the requirements of public safety in mind. This means that security is a critical requirement. TETRA provides the following mechanisms to fulfil the security requirements:

- Authentication to ensure trusted access of radios to the TETRA infrastructure and vice-versa (mutual authentication);
- Air Interface Encryption (AIE) to encrypt the voice, data and signalling over-the-air, which is critical to prevent eavesdropping and analysis of communication patterns;
- End to End Encryption (E2EE) to further enhance encryption of voice and data, including the transfer of voice and data within the transport and core components of a TETRA network;
- Enable and Disable to allow remote disabling of TETRA radios when the radio is lost or stolen

3.1 TETRA Architecture

The TETRA architecture Release 1 may differ within the three main TETRA standards: Voice plus Data (V+D), Packet Data Optimized and Direct Mode Operation, as depicted in Table 6.

Table 6: TETRA standards

Voice plus Data (V+D)	The Voice plus Data standard allows the simultaneous transmission of voice and data in a circuit switch mode, it provides a wide range of services and facilities in order to meet the needs of Professional Mobile Radio (PMR) user organizations. The most important services available on this standard are [33]: ▪ Voice Services ▪ Group Call ▪ Pre-Emptive Priority Call (Emergency Call) ▪ Call Retention ▪ Priority Call ▪ Dynamic Group Number Assignment (DGNA) ▪ Ambience Listening ▪ Call Authorised by Dispatcher ▪ Area Selection ▪ Late Entry ▪ Status Messaging ▪ Short Data Service ▪ Packet Data A description on each of the previous services can be found in [33].
Packet Data Optimized (PDO)	The PDO standard, not to confuse with TETRA Enhanced Data Service (TEDS), was developed for “Data Only” wireless communication applications, but in [34] is also referenced that: “To date, no manufacturer has developed PDO systems and products because all traditional Professional Mobile Radio (PMR) users require voice communications as well as data communications, hence the reason why the TETRA Voice plus Data (V+D) standard is very successful.”
Direct Mode Operation (DMO):	DMO is defined in [35] as a “mode of simplex operation where mobile subscriber radio units may communicate using radio frequencies which may be monitored by, but which are outside the control of the TETRA trunked-mode operation (TMO) network. DMO is performed without intervention of any base station.” Some typical DMO applications are described in [36].

Overall, the main network elements of the TETRA architecture, based on the standards described in Table 6, are depicted in Figure 23 below. A brief description on these network elements is also given in Table 7 below. Note that the Packet Data Network (PDN), Integrated Services Digital Network (ISDN), Private Telephone Network (PTN) and Public Switched Telephone Network (PSTN) presented in Figure 23 are external networks and can be managed by different operators.

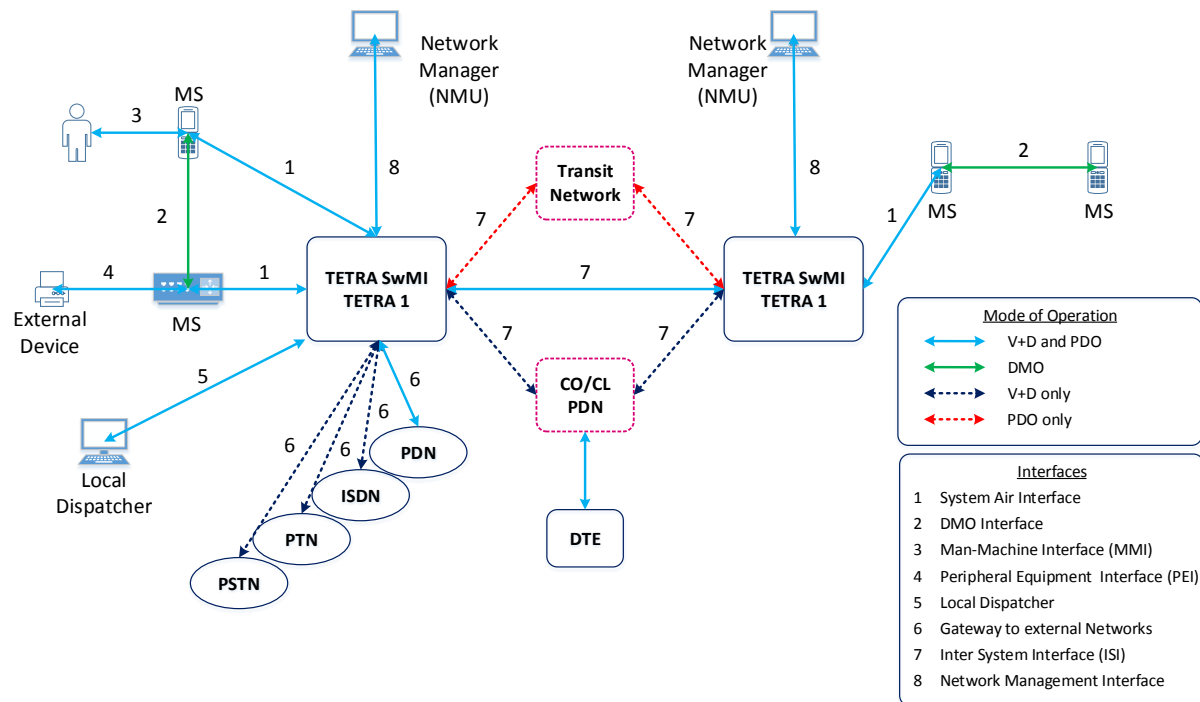


Figure 23: General TETRA architecture.

Table 7: TETRA network elements.

Mobile Station (MS)	The Mobile Station (MS) represents a physical grouping that contains all of the mobile equipment that is used to obtain TETRA services [87]. MS are TETRA radio terminals, including hand-held, mobile and fixed ones. MS are to TETRA what UEs are to LTE.
TETRA SwMI	The TETRA Switching and Management Infrastructure (SwMI) is mainly made of TETRA Base Stations (TBS).
CO/CL PDN	The connection/connectionless public data network (CO/CL PDN) can be an intermediate network that provides TETRA services to a DTE.
Network Management Unit (NMU)	The Network Management Unit (NMU) provides local and remote network management. These functions generally encompass system management, configuration, accounting, performance and planning.
Data Terminal Equipment (DTE)	The Data Terminal Equipment (DTE) can be considered as a device which acts as the source and/or destination of data and which controls the communication channel.
Transit Network (TN)	A Transit Network (TN) may be used for communication between different terminating networks.

A brief description on the main Tetra Standard Interfaces used in Figure 23 is given in Table 8 below.

Table 8: TETRA Standard Interfaces.

Air Interfaces (1 & 2)	The most important (and complex) interfaces are considered to be the 'air interfaces' between the base station and radio terminals (1) and the Direct Mode Operation (DMO) interface (2) [98].
Man-Machine Interface (3)	Typically this interface consists in an LCD display and a keypad, it allows interaction between the user and the MS.
Peripheral Equipment Interface (4)	This interface standardises the connection of the radio terminal to an external device, and supports data transmission between resident applications in the device and the connected TETRA radio terminal [98].
Remote Dispatcher Interface (5)	This interface was originally intended to allow connection to remote wire line dispatcher consoles like those located in major control rooms. Unfortunately, work on this interface was dropped in ETSI TC TETRA as the complexity to provide a universal interface without degrading performance was impractical.
Gateway to external Networks (6)	This standardised interface enables TETRA to interface with the PSTN, the ISDN and/or a PABX [98].
Inter-System Interface (7)	This standardised Inter-System Interface (ISI) allows infrastructures supplied by different TETRA manufacturers to inter-operate with each other allowing interoperability between two or more networks. There are two methods of interconnection in the standard, one covering information transfer using circuit mode and the other using packet mode [98].
Network Management Interface (8)	Like the local dispatcher interface, it was recognised during standardisation activities that a common network management interface was impractical. Fortunately, this early standardisation was not wasted as it was later turned into a comprehensive guide to assist users in defining network management requirements [98].

3.2 TETRA security principals

Before providing more specified details about the TETRA security principals, the TETRA security model is presented. The fundamental TETRA security service, which is the base for every security mechanism, has many similarities to the equivalent mechanism in GSM (use of symmetric key cryptography) and is “based on proof of knowledge of a secret that is shared between a terminal and the infrastructure’s authentication centre (AuC). Following an explicit authentication exchange, there is an on-going implicit authentication of a terminal as the cipher keys that are then used for the up-link air interface encryption are derived from that initial authentication exchange” [102]. There is no use of either asymmetric cryptography (public key) or digital certificates. The layers of the TETRA security model are depicted in the following figure.

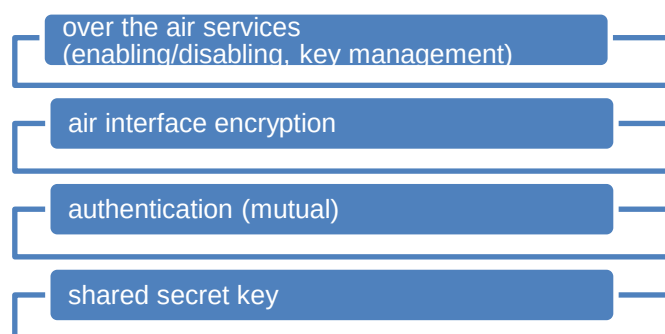


Figure 24 - TETRA Security Model Layering

3.2.1 Authentication

Authentication in TETRA systems can be performed in three levels: (1) authentication of a MS by the infrastructure; (2) authentication of the infrastructure by the MS and; (3) mutual authentication. In every case, authentication is taking place by the participants showing to each other that they are aware of the shared secret symmetric key that is already pre-shared between them. The entities participating in the authentication process are the MS and the SwMI. "The MS is considered, for the purposes of authentication, to represent the user as defined by the Individual TETRA Subscriber Identity (ITSI)" [37]. On the other hand, the SwMI design is more flexible, with a trusted base station (BS) representing an AuC. The knowledge provided by the AuC during the authentication exchange serves also as the session authentication key (KS). The authentication key of the MS (K) is only visible within the limits of the AuC. A common set of algorithms is responsible for generating the cipher keys over the air interface and the SwMi is responsible for the surveillance of the process. The procedure of authentication in TETRA systems is a two-pass challenge-response protocol and a successful completion of it allows further security related functions to be downloaded. In the next few paragraphs, each authentication type will be analytically explained.

3.2.1.1 Authentication of a MS by the infrastructure

The AuC generates the session authentication key (KS), also calculated by the TA11 algorithm at the MS side. From the infrastructure side (SwMI), algorithm TA12 is responsible to calculate the response and also generates a cipher key. A challenge value, RAND1, is produced by the SwMI to which the MS responds with the RES1 value, while the SwMI calculates the expected response, XRES1. This procedure is responsible for the generation of a part of the derived cipher key, namely DCK1. After receiving RES1, the SwMI compares it to its own XRES1. Result R1 is set to "true" when the values match and to "false" when they do not. This procedure is depicted in Figure 25.

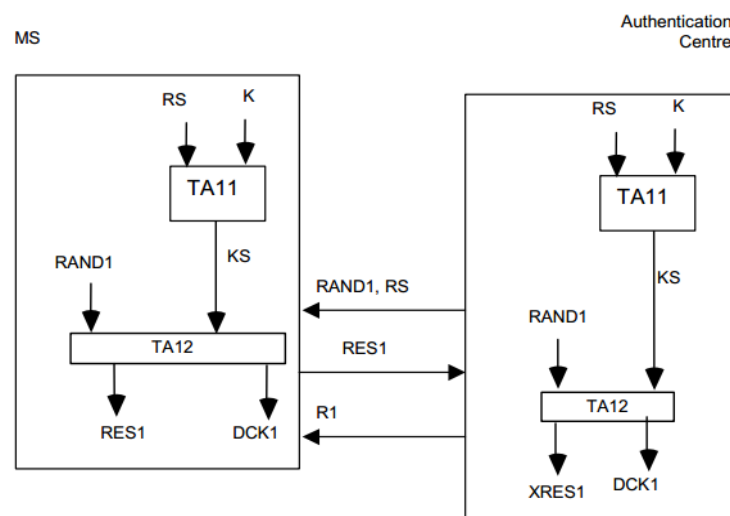


Figure 25 - MS authentication in TETRA [37]

3.2.1.2 Authentication of the infrastructure by the MS

The inverse procedure to the one mentioned in the previous section is taking place in the case of infrastructure authentication by the MS. The initial challenge, RAND2 is produced by the MS and RES2, the equivalent response is computed by the SwMI. By its turn, the MS also calculates XRES2 (the expected response value). The whole procedure results in the production of the DCK2 cipher key. Afterwards, RES2 and XRES2 are compared by the MS and if they match, the result R2 "true" is generated. In the opposite case, the result value is set to "false" and authentication fails. The authentication key (K) used is the same as in the authentication of the MS by the SwMI case, while a random seed RS also exists. However, the algorithms participating are different. TA21 and TA22 equivalently replace TA11 and TA12. As a

result, the session authentication key, KS' , is also different. Figure 26 demonstrates this specific authentication procedure.

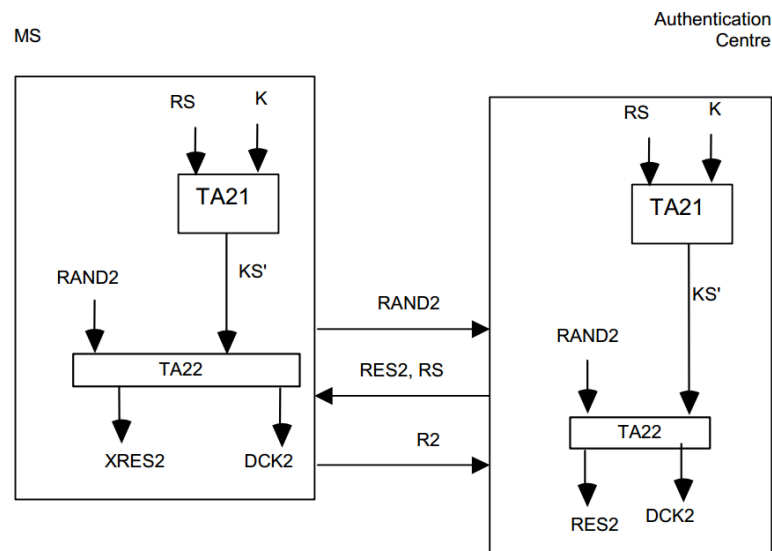


Figure 26 - Infrastructure authentication in TETRA [37]

3.2.1.3 Mutual Authentication

Unlike to the two previous categories, mutual authentication is carried out by the use of a three-pass mechanism, with the same algorithms and keys available in the two previous cases. The first entity to become challenged is the one taking the decision upon the mutual authentication. Thus, it is easily understandable that the procedure begins as one-sided authentication by the challenger and then becomes mutual by the challenged side. However, there is the possibility that mutual authentication is not supported by the challenging side. In that case it has the option of confirming the authentication exchange by providing the opposite side with a successful authentication result. When the MS is the side responsible to respond, it can either leave the serving cell or remain connected. The rules related to mutual authentication have to be followed strictly.

In case of failure of the first authentication, the second authentication should not take place.

This, however, does not restrict the challenged party which had already not responded to the first challenge, to challenge the other party from scratch. If the SwMI triggers the authentication process, then the session keys KS and KS' are produced by the contribution of K , the algorithms $TA11$ and $TA21$ and the random seed RS . Afterwards, it is responsible for providing the MS side with RS and the $RAND1$ random challenge. On its turn, the MS uses the $TA11$ and $TA21$ algorithms so as to calculate the values for KS and KS' as well, due to the mutual character of the authentication. Before the MS proceeds to sending the response $RES1$ to the SwMI, both participants use the algorithm $TA12$. Simultaneously, the MS sends the mutual challenge $RAND2$ to the SwMI. The actions taken by the SwMI are summarized below. Firstly, it compares $RES1$ to $XRES1$ and, due to the reception of a mutual challenge and in case of previous omission, it uses the $TA21$ algorithm for the calculation of KS' . Meanwhile, $TA22$ is running in order to compute the response $RES2$, which is then sent to the MS. The MS also uses $TA22$, generates the expected response $XRES2$ and compares the values. Results (in the value $R2$) "true" or "false" are returned according to the success or failure of the comparison. If $R2$ is "true", then the mutual authentication procedure is completed successfully. Moreover, $TA12$ is responsible for producing the cipher key $DCK1$, while $TA22$ does the same for $DCK2$. Those values are used as inputs for the $TB4$ algorithm (see section 3.2.3.2) and produce the value DCK , trademark of the mutual challenge. Figure 27 and Figure 28 depict the mutual authentication process, initiated by either the MS or the SwMI.

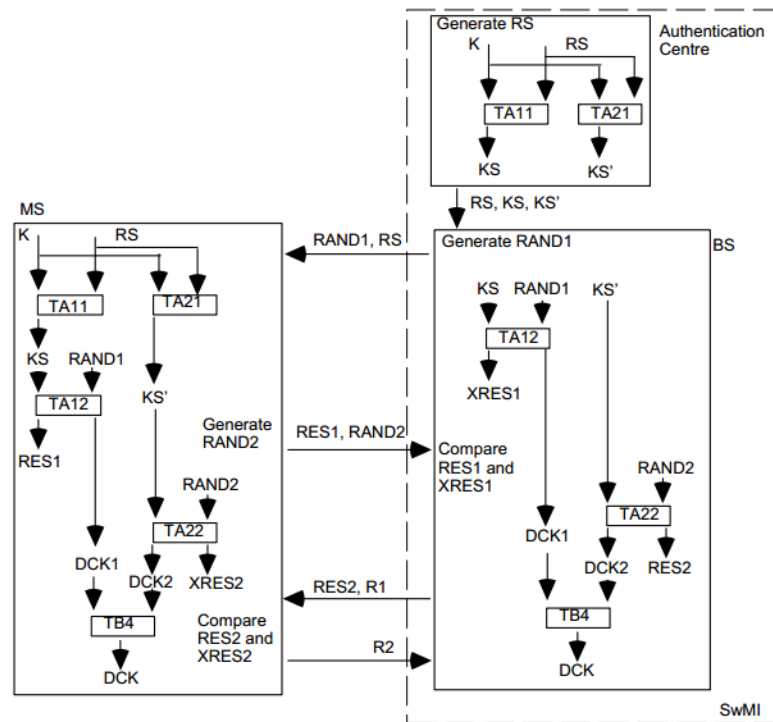


Figure 27 - Mutual Authentication in TETRA (SwMI triggered) [37]

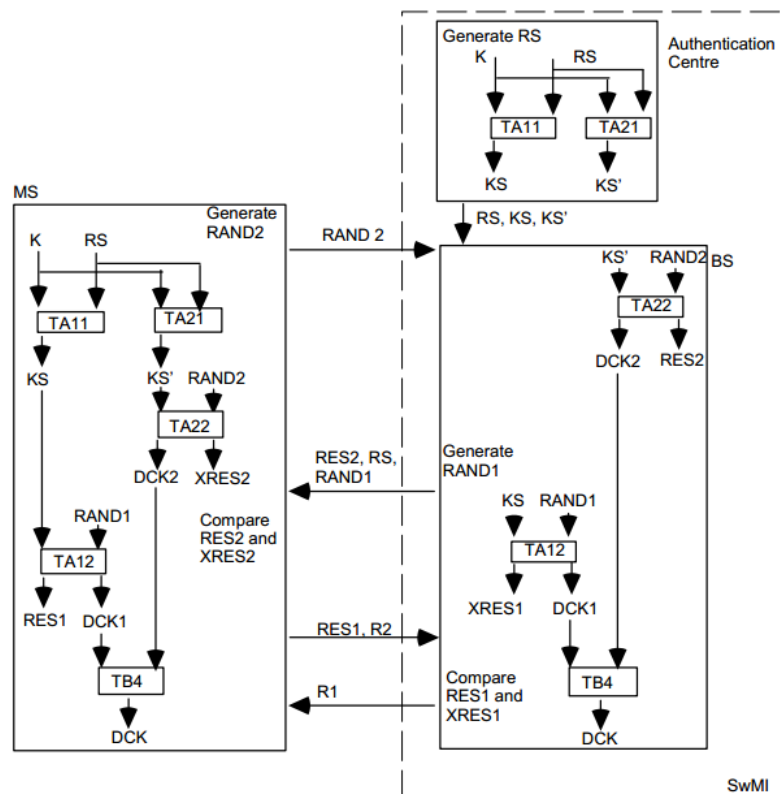


Figure 28 - Mutual Authentication in TETRA (MS triggered) [37]

There exists one standard for TETRA authentication and key management algorithms (TAA1), which can be acquired from ETSI under a “Non-disclosure and restricted usage licence”.

3.2.2 Encryption

TETRA is using two categories of encryption, Air Interface and End-to-End in order to preserve confidentiality, authenticity, integrity, availability and accountability within the network. Encryption aims to ensure that no entity other than the authorized receiver will gain access to the information that is sent.

3.2.2.1 Air Interface Encryption

Air interface security is essential for the TETRA networks, since eavesdropping is one of the most common vulnerabilities. “User traffic and signalling information can be encrypted over the air interface between the Mobile Station (MS) and the SwMI, both for individual and group communications. The air interface encryption mechanism is available for V+D in Trunked Mode Operation and in DMO” [101]. Many different standard and proprietary encryption algorithms are used. Traffic encryption is responsible for the protection of user generated content, such as voice and data. Signalling encryption is protected against eavesdropping, user behaviour and traffic analysis. Moreover, continuous authentication is guaranteed, since the encryption key derives from the authentication process. Air Interface encryption resides in the upper part of the MAC layer of the TETRA protocol stack. “Situating the encryption process at this point, prior to channel coding at the transmitting end and after channel decoding at the receiving end, enables the MAC headers to be left unencrypted. This allows the appropriate channel coding to be used, enables receiving parties to determine the applicability of a message received over air for them, and enables application of the correct key for the decryption process” [37].

TETRA Air Interface Encryption Algorithms

The TETRA standard supports four AIE TETRA Encryption Algorithms (TEAs), namely TEA1, TEA2, TEA3 and TEA4. They have been developed by ETSI's Security Algorithm Group of Experts (SAGE) and are owned by ETSI [98]. They are developed in a way that it currently makes it impossible for an individual or group to recover their design from their implementation. TEA2 and TEA3, the Restricted Export Algorithms are controlled under the rules of the 1998 Wassenaar Arrangement [99] that permit their use only on behalf of public safety organizations. More precisely, the use of TEA2 is limited to Public Safety and Military Organizations within European Union and related countries. On the other hand, TEA 3 is available to the countries which have no authorization to TEA2. TEA1 and TEA4 belong to the category of Readily Exportable Algorithms that are generally licenced for export. A number of certain entities/organizations are responsible for the maintenance and distribution of the TEAx algorithms [104]. More precisely, ETSI is the custodian for TEA1, TEA3 and TEA 4. The secretary of the TETRA SFPG in the Netherlands is responsible for the distribution of TEA2.

3.2.2.2 End-to-end Encryption

Air interface encryption is not enough for TETRA systems, because it does not provide support for communication between the MSs. End-to-end encryption (E2EE) is responsible for that particular part. There are no algorithms specifically designed for E2EE in TETRA. However, ETSI [100] provides a synchronization mechanism for E2EE, which is advised to be used simultaneously with a synchronous stream cipher. Below, the requirements for the use of the specific mechanism can be found.

- The mechanism is not applicable to self-synchronizing or block ciphers.
- The mechanism should be applied to mutual directions.
- Independence of the synchronization procedure for each of the directions is required.
- Encryption must take place on the top of AIE (MAC-residing).
- The integrity of E2EE voice and synchronisation frame should be maintained, requiring transparent transport of full-slot and half-slot traffic through the TETRA SwMI.
- The encryption mechanisms must be valid for one call instance.

The confidential document “TETRA SFPG Recommendation 02” [103] (available for members of the TETRA and Critical Communications Association under a signed non-disclosure

agreement) provides a detailed overview of the implementation of E2EE for speech and also contains potential implementations for two algorithms, IDEA and AES.

3.2.2.3 Speech and control information encryption

Figure 29 below depicts how speech and control information is encrypted. The *Key Stream Generator* (KSG), which resides both in a MS and the BS is responsible for the implementation of the encryption algorithm. It has two inputs, the Initial Value (IV) and a cipher key. The IV value is stored at the SwMI and broadcasted on the SYNC and SYSINFO PDUs (layer 2) and the composition of its slot and frame numbering input follows [105]:

- The first two bits IV(0) and IV(1) correspond to the slot number, and have values enumerated from 0 to 3, where 0 corresponds to slot 1, and 3 corresponds to slot 4. IV(0) is the least significant bit of the slot number.
- The following five bits IV(2) to IV(6) point to the frame number, and receive values from 1 (00001 binary) to 18 (10010 binary). IV(2) corresponds to the least significant bit of the frame number.
- The next six bits IV(7) to IV(12) correspond to the multiframe number, and have values from 1 (00001 binary) to 60 (111100 binary). IV(7) is the least significant bit of the multiframe number.
- The next 15 bits IV(13) to IV(27) should correspond to the 15 least significant bits of an extension that numbers the hyper-frames. These can take all values from 0 to 32 767. IV(13) should correspond to the least significant bit of the hyper-frame numbering extension.
- The final bit, IV(28), indicates the direction of transmission and receives the value 0 for downlink, and 1 for uplink transmissions.

The KSG produces one output as a sequence of key stream bits, namely *Key Stream Segment* (KSS). It is advisable that the *Cipher Key* (CK) should not be used directly at the air interface for encryption but shall be modified by the *Colour Code* (CC), *Location Area identification* (LA-id) and *Carrier Number* (CN) using algorithm TB5. With these combinations, the input to the encryption algorithm among the carriers of a single cell and between cells in a location area is randomized. CK is used in conjunction with a KSG so as to produce a key stream for encryption and decryption of information at the MAC layer. It can be considered a binary vector of 80 bits, labelled ECK(0) ... ECK(79) [37]. CKs associated to uplink and downlink encryption and decryption procedures should be different.

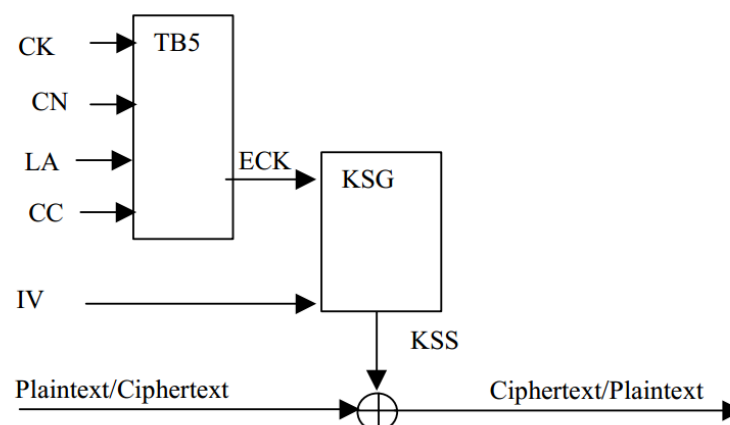


Figure 29 - Speech and control information encryption [37]

3.2.3 Air Interface key management mechanisms

This section describes how the TETRA devices securely exchange keys. Five types of key are managed over the air interface [37]:

- Derived Cipher Key (DCK);
- Common Cipher Key (CCK);
- Group Cipher Key (GCK);
- Group Session Key for Over the Air Rekeying (GSKO);
- Static Cipher Key (SCK).

As the usage of these keys depends on the security class applied, a description about security classes used in TETRA is given in section 3.2.3.1, whilst section 3.2.3.2 and below provide a description on how each key is managed.

3.2.3.1 Security classes

The usage of the cipher keys is dependent on the security class applied, where each class has associated features that are mandatory or optional. The list of these classes is depicted in Table 9.

Table 9: TETRA Air interface security classes.

Class	Encryption	Keys	Over The Air Re-keying (OTAR)	Authentication
1	No	-	No	Optional
2	Static Key	SCK	Optional	Optional
3	Dynamic Key	DCK, CCK	Mandatory	Mandatory
3G	Dynamic Key	DCK, CCK, GCK	Mandatory	Mandatory

A TETRA mobile station (MS) may support one, several, or all security classes. Each TETRA cell may support at any one time different security classes, i.e. class 1 and class 3. Combinations are permitted with the exception of class 2 and class 3/3G [37].

3.2.3.2 Derived Cipher Key (DCK)

DCK may be used to protect voice, data, and signalling sequences between the infrastructure and an individual MS after successful authentication has taken place. The DCK shall be derived by the MS and by the infrastructure (during the authentication process) from its two parts DCK1 and DCK2 by the procedure TB4 [37], as shown in Figure 30. DCK1 is derived from a random number (RAND1) (generated on the authentication centre) by algorithm TA12 and DCK2 is derived from another random number (RAND2) (generated on the MS) by algorithm TA22, both algorithms are also described in [37]. In case of unilateral authentication, either DCK1 or DCK2 shall be set to zero:

- Authentication of the infrastructure by the user: DCK1 = 0;
- Authentication of the user by the infrastructure: DCK2 = 0.

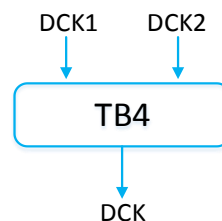


Figure 30: Derivation of the DCK from DCK1 and DCK2 using TB4 algorithm [37].

3.2.3.3 Common Cipher Key (CCK)

CCK is used to provide protection of voice, data, and signalling sequences between the infrastructure and the MSs when using group addresses on the downlink either as a key modifier of GCK or as a standalone key. CCK applies only to class 3 cells and shall be generated by the infrastructure and distributed to the MSs as depicted in Figure 31.

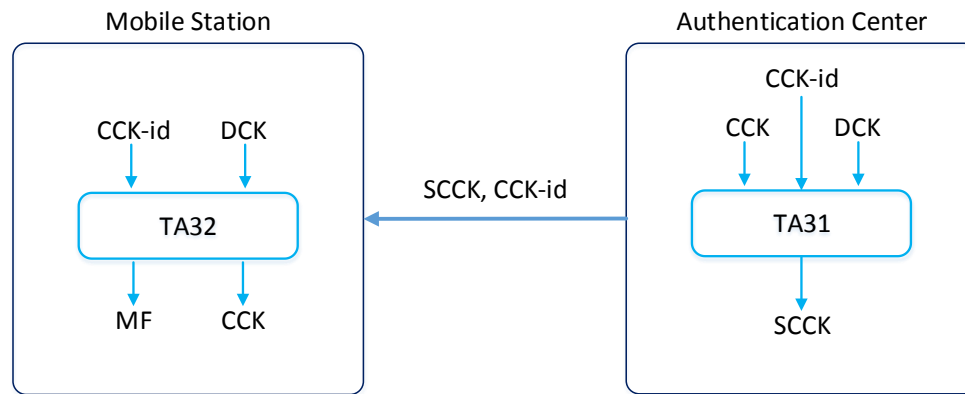


Figure 31: Distribution of a common cipher key [37].

In order to distribute the CCK in a secure manner to the MS's, the AuC generates a Sealed Common Cipher Key (SCCK) - taken as input of procedure TA31 - the CCK, DCK and a CCK Identifier (CCK-id). The AuC sends towards the MSs only the SCCK and the CCK-id. The mobile station recovers the CCK using procedure TA32 with CCK-id and DCK as inputs. A detected manipulation on the SCCK can be indicated by setting the manipulation flag MF [37].

There should be one such key for every Location Area (LA). A LA is defined in [87] as the area within radio coverage of a base station or group of base stations within which a MS is allowed to operate.

3.2.3.4 Group Cipher Key (GCK)

GCK may be used in partnership with the SCK (see section 3.2.3.5) or with the CCK to protect voice, data, and signalling sequences between the infrastructure and the MSs when using group addresses. GCK should not be used directly by the air interface encryption unit. Instead, a new key, known as *Modified Group Cipher Key* (MGCK), should be derived from the GCK. The derivation of MGCK depends on the security class and is described in more detail below. The GCK shall be known to the infrastructure and distributed to the MSs, where two different types of distribution could be used:

- Distribution of GCK to individuals;
- Distribution of GCK to a group.

Distribution of GCK to individuals

The parameters used to provide the security when distributing the GCK are:

- GCKN: the *Group Cipher Key Number* is associated with each GCK and can be used to identify association with multiple groups. The values of GCKN should be unique between all MSs sharing the same sets of GCK [37];
- GCK: the *Group Cipher Key* to be transmitted by the AuC to the MS's;
- KSO: when distributing a GCK to an individual it shall be protected by a KSO (Session Key for OTAR (Over The Air Re-keying)) on the algorithm TA81, the KSO is derived from a Random Seed (RSO) and from a user's *authentication key* (K) as described in [37]
- SGCK: the *Sealed Group Cipher Key* contains the GCK in a secure way.
- GCK-VN: The algorithm TA81 uses the group cipher key version number (GCK-VN) and the *Group Cipher Key Number* (GCKN) in order to allow the MS to discover if GCK has been corrupted due to transmission errors or manipulation. A detected manipulation can also be indicated by setting the manipulation flag MF [37] by the algorithm TA82.

By applying algorithm TA81 to the parameters described above, a Sealed Group Cipher Key is obtained that is transmitted to the MS with the GCK-VN, RSO and GCKN in order to the MS to recovery the GCK. Figure 32 depicts this procedure, i.e. how the GCK can be securely distributed to individuals.

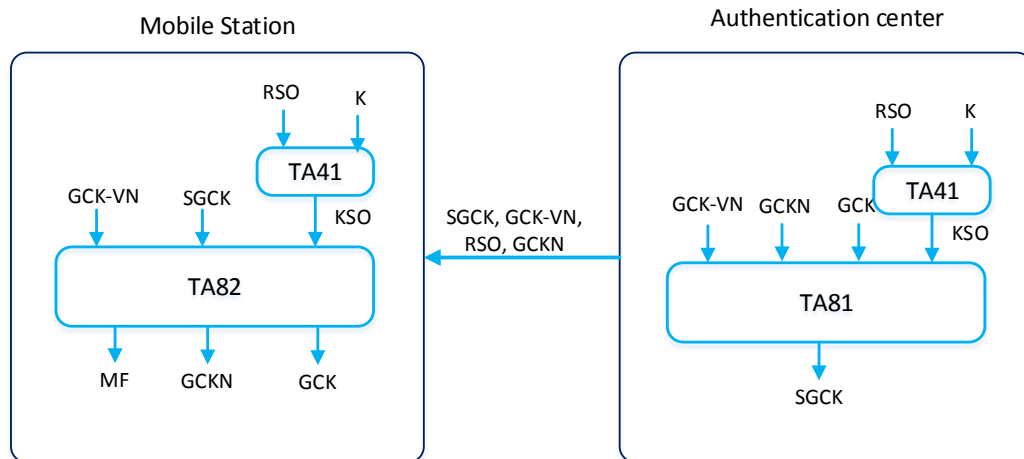


Figure 32: Distribution of a group cipher key to an individual, based on [37].

Distributing GCK to a group

When distributing GCK to a group address, beyond the parameters described above, an *Extended Group Session Key for OTAR* (EGSKO) is used, instead of KSO, as input of procedure TA51, as depicted in Figure 33. A brief description about EGSKO is given in section 3.2.3.6.

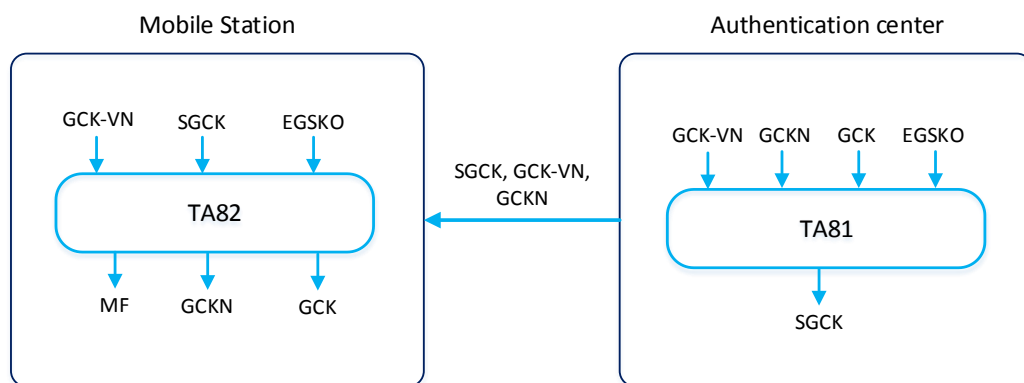


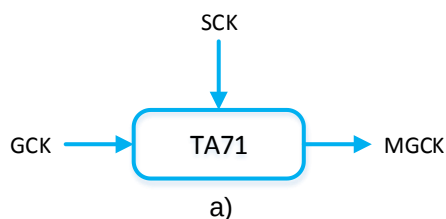
Figure 33: Distribution of a group cipher key to a group member, based on [37].

Derivation of MGCK from GCK

In order to protect voice, data, and signalling sequences between the infrastructure and an MS when using group addresses, a derivation of GCK, the *Modified GCK* (MGCK), shall be used instead of GCK. The MGCK depends on the security class applied, as described in Figure 34.

Class 2 systems

When deriving MGCK in class 2 systems, SCK and GCK should be used as inputs of procedure TA71.



Class 3 systems

When deriving MGCK in class 3 systems, CCK and GCK should be used as inputs of procedure TA71.

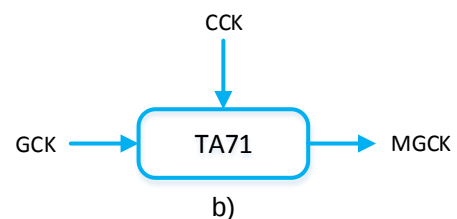


Figure 34: a) Generation of MGCK from GCK and SCK in class 2 systems; b) Generation of MGCK from GCK and CCK in class 3 systems

If GCK is not defined for a group, the value of MGCK shall be equal to that of SCK (class 2 systems), or of CCK (class 3 systems) and algorithm TA71 would not be invoked.

3.2.3.5 Static Cipher Key (SCK)

The SCK is the only one type of cipher key defined for DMO and applies to class 2 cells [38]. According to EN 300 396-6 [38], the SCK can be chosen by the system manager and may be distributed using the OTAR mechanism described below or be manually configured in the MS. This means the initial allocation of SCK shall be carried out in advance of communication.

SCK is used to protect voice, data, and signalling sequences between the infrastructure and an individual MS in a class 2 cell. In addition, SCK protects voice, data and signalling when DMO is selected, to enable communication between radios when no infrastructure is available. The SCK may be protected for distribution in a similar manner to the GCK , and can be distributed in two different ways:

- Distribution of SCK to individuals
- Distributing SCK to a group

Distribution of SCK to individual MS's

When distributing SCK to an individual MS by an OTAR mechanism (algorithms TA51 and TA52), the KSO is used to protect the SCK. KSO should be individual to each user and is derived from the user's *authentication key* (K) and a random seed (RSO) with algorithm TA41 [37], as depicted in Figure 35.

A Static Cipher Key Version Number (SCK-VN) identifies the version of each SCK identified by the SCK-id parameter (each MS can have up to 32 SCK). Using SCK-VN, SCKN, SCK and KSO as inputs of algorithm TA51, it produces a Sealed Static Cipher Key (SSCK) that is transmitted to the MS's. The parameters SCK-VN, RSO and SCKN are also sent to MS's.

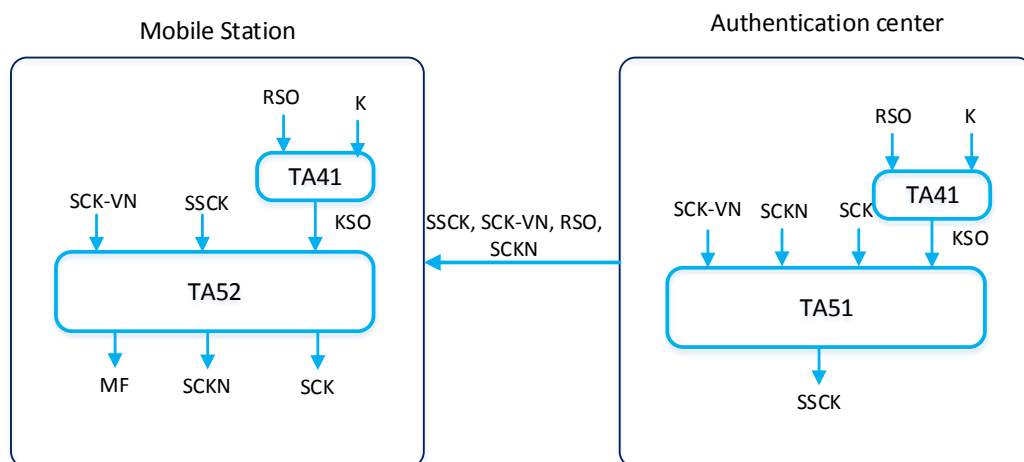


Figure 35: Distribution of SCK to an individual MS by an authentication centre, based on [37].

Distributing SCK to a group

When distributing SCK to a group, the procedure is the same as for Distributing SCK to individual MS's except that EGSKO shall be used in place of KSO as input to algorithms TA51 and TA52 (a brief description on EGSKO is given in section 3.2.3.6) and the RSO is not sent to MS's, as depicted in Figure 36.

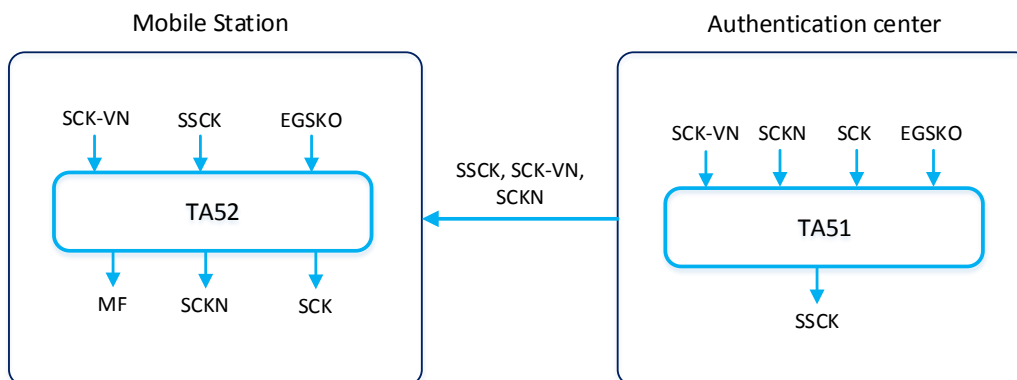


Figure 36: Distribution of SCK to a group member by an authentication centre, based on [37].

3.2.3.6 Group Session Key for OTAR (GSKO)

As previously stated, the GCK and SCK are keys distributed by infrastructure to MSs to be used in group communications. In some cases these keys may be simultaneously distributed to all group members. In order to achieve such scenario a new key, known as GSKO, is generated by the infrastructure and distributed to each group member individually. The GSKO is protected by two parameters using algorithm TA91 before the AuC sends it to the MS, the KSO and the GSKO-VN (Group Session Key for OTAR Version Number). The KSO is derived by K and RSO in a same manner as described above in section 3.2.3.4, the GSKO-VN is an associated version number of GSKO which can be used for replay protection.

The Sealed Group Session Key for OTAR (SGSKO) is then sent to the MS with GSKO-VN and RSO. The MS can check the validity of received GSKO by the state of manipulation flag (MF) produced by algorithm TA92.

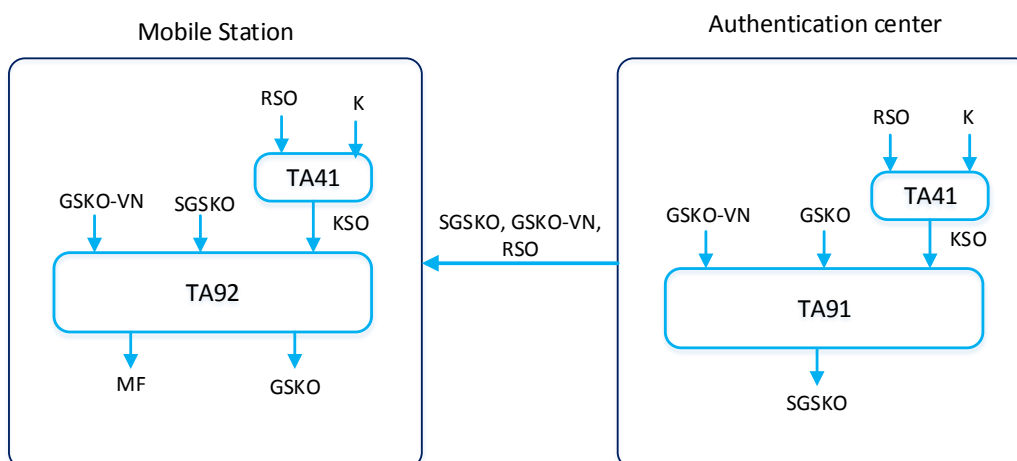


Figure 37: Distribution of GSKO by an authentication centre [37].

After receiving the GSKO, the MS shall derive EGSKO as depicted in Figure 38.

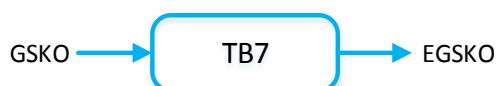


Figure 38: Generation of EGSKO using TB7 [37].

This new derived key, EGSKO, should replace KSO when distributing GCK and SCK to group addresses.

3.2.3.7 Summary of the TETRA air interface keys

A summary of the TETRA air interface keys, the security classes were they are used and their usage/purpose is provided in Table 10.

Table 10: Summary of the TETRA air interface keys.

Key	Class applied	Protection	Usage
DCK	3	Voice, data, signalling	Individual communications
CCK	3	Voice, data, signalling	Group communications
SCK	2	Voice, data, signalling	Individual / Group communications
GCK	2/3	n/a	Derivation of MGCK
MGCK	3G	Voice, data, signalling	Group communications
GSKO	2/3	n/a	Protects the distribution of SCK and GCK to groups

3.3 TETRA security vulnerabilities

The information on this subsection has been considered security sensitive and it has been moved to D5.1 RESTREINT UE Annex, which is a separated document (SALUS_D5.1_Annex.docx/pdf)

4 SECURITY AND PRIVACY ANALYSIS OF SHORT RANGE WIRELESS NETWORKS

4.1 The role of Wi-Fi and sensor networks in SALUS platform [UL, UBITEL]

The use of short range wireless networks in the SALUS platform is mainly envisaged for the following two purposes. First, the Wi-Fi is planned to be used as a complementary connectivity technology (a fall-back mechanism) to interconnect PPDR personnel in cases when the mobile connectivity (3G/LTE) is either reduced or lost. Second, the Wi-Fi is also envisaged to interconnect remote devices such as sensors.

To implement the fall-back mechanism, SALUS intends to make use of both modes of Wi-Fi: ad hoc mesh networking and the (classic) infrastructure mode. The ad hoc mesh networking is intended to enable P2P communications between nearby Wi-Fi capable hand-held devices of PPDR users in the absence of a communications infrastructure, while the infrastructure mode is intended to provide wireless access to a backbone communications infrastructure. The overview of existing security solutions is thus presented separately for each mode.

4.2 Threat model

The section describes the threats that can emerge when using Wi-Fi in above scenarios.

4.2.1 Wi-Fi Ad Hoc Mesh Routing

One of the most common security concerns in the ad hoc mesh routing is the security of the routing protocol. It directly affects the ability of devices to securely interconnect and exchange messages. A common attack features an adversary participating in the ad hoc network that causes various network anomalies. For instance, the adversary could selectively drop packets and thus subvert the network in his vicinity; black hole and grey hole attacks are such examples. Moreover, the adversary could modify the contents of the protocol messages and thus impede part of the network that extends over his immediate vicinity. These attacks increase the amount of packet loss and delay in the network and thus render it unavailable.

Since the Wi-Fi is inherently broadcast, the attacker can passively scan the wireless traffic and inspect the contents of the exchanged information. This way the attacker can access information that is not intended to be disclosed. Since this is a passive attack, it is not required that the attacker actively participates in network; he only needs to position himself in the range of the radio signal. Moreover, if the attacker does actively participate in the network, he can modify the contents of the exchanged information. This way the attacker could send false (application layer) messages and severely impede the operational capabilities of the PPDR organizations.

4.2.2 Wi-Fi Infrastructure

In cases when PPDR operatives enter buildings that have Wi-Fi access points, the operatives may use such infrastructure to reach the Internet. But since such infrastructure will not always be managed by PPDR institutions, it cannot be blindly trusted. Access points may not connect to the Internet directly, but through a series of gateways. The attacker, particularly an insider, such as a malicious network administrator, could read or modify the contents of exchanged information at the access point or at any of those gateways.

Another threat can emerge when Wi-Fi is used in infrastructure mode in buildings that are managed by PPDR organizations. Here the main threats represent attackers that, like above, passively scan the wireless and read the contents of the exchanged information.

A comprehensive set of Wi-Fi related threats/vulnerabilities is provided in section 4.3.3.

4.2.3 Sensor-networks

Smart sensors and meters play an important role in all three SALUS Use Cases. From the security point of view, sensor networks have similar threats to Wi-Fi ad hoc. Attackers can cause significant interference, or exhaust the bandwidth occupied by the sensor network to temporary shut off connectivity (e.g. to disable video control over a selected area). Attackers are also able to passively scan the wireless traffic and obtain information on the quantity of sensors and the type of exchanged traffic (e.g. an attacker can detect a hidden camera or intrusion detection sensor just by scanning the wireless network). Attackers can also try to include a modified 'fake sensor into the network and create fake alerts or control the sensor network behaviour (e.g. corrupt routing messages to perform re-routing of traffic). One more type of attacks is related to so-called "energy exhaustion". Attackers can transmit fake service messages forcing the other nodes to perform some heavy computations or transmissions in response to received fake message. Proper data encryption and trusted security protocols can significantly reduce the vulnerabilities of sensor networks. One of the solutions to protect from energy exhaustion type of attacks is to authenticate the service frames as well as the data ones.

More details on these vulnerabilities/threats are provided on sections 4.4.1.2 and 4.4.2.2.

4.3 Security and privacy analysis of Wi-Fi networks

4.3.1 Ad Hoc Mesh Routing Security

To establish an ad hoc mesh network the participating devices require a routing protocol. Many such routing protocols exist [47]. They are usually characterised based on the methods for creating routes between nodes: reactive protocols have nodes discover routes only when needed; proactive protocols require that nodes maintain routing tables and actively propagate route updates; hybrid protocols combine elements of both. However, we do not intend to survey all of the existing protocols, but merely identify and briefly describe those that provide security elements. Security in ad hoc network routing protocols is a rather recent topic, therefore not many solutions are available. Moreover, we concentrate on those that are somewhat mature and could be considered for implementation in SALUS. In light of this, the field of ad hoc routing is dominated by the following four solutions: Babel [45], B.A.T.M.A.N [53], ChaMeLeon [54] and the IEEE 802.11s [48]. The latter is not a routing protocol but a standard that defines how wireless devices interconnect to create a mesh network. The following subsections describe these protocols and their security extensions in more detail.

4.3.1.1 Babel protocol

The workings of Babel protocol is eloquently explained in its experimental RFC [45]: "Babel is a loop-avoiding distance-vector routing protocol that is designed to be robust and efficient both in networks using prefix-based routing and in networks using flat routing (mesh networks), and both in relatively stable wired networks and in highly dynamic wireless networks." Babel is a layer 3 routing protocol, which means that it routes using IP addresses. However, it should be stressed that the original Babel proposal is inherently insecure.

The security extension is proposed in Internet-Draft [46]. The extension secures the protocol by (i) ascertaining that only the intended nodes participate in routing table construction and by (ii) protecting the contents of the exchanged routing information from being modified by a third party. This is achieved by adding two data structures to the protocol packets:

- A cryptographic sequence number that protects from replay attacks. These are attacks in which an adversary overhears a valid transmission, caches it, and retransmits it later in order to manipulate an honest node into resending the packet and thus revealing some information.
- A field that represents the result of the Keyed-Hashing for Message Authentication (HMAC) construct computed over the meaningful items of the packet and the shared secret key. The HMAC (i) detects any illegal data modifications and (ii) mutually

authenticates the communicating nodes, since only those that know the secret key are able to compute the HMAC.

The security extension thus uses a pre-shared key (PSK) to authenticate nodes and to detect data tampering. However, the security mechanism explicitly allows multiple HMAC results in a single authenticated packet, which allows nodes to be authenticated in multiple domains: each particular HMAC result can correspond to a particular secret key.

The security extension does not provide any key management mechanism. Thus the procedures to generate, distribute, and revoke keys (and other relevant key management procedures) are left unspecified. Both implementations of the Babel protocol, *insecure*³ and *secure*⁴, can be freely obtained under open-source licences. More importantly, both versions of the protocol are being actively developed and maintained.

4.3.1.2 B.A.T.M.A.N protocol

The inner workings of the B.A.T.M.A.N (Better Approach To Mobile Ad hoc Networking) protocol are provided in the Internet-Draft [53]. It states that “B.A.T.M.A.N is a proactive routing protocol for Wireless Ad-hoc Mesh Networks, including (but not limited to) Mobile Ad hoc Networks (MANETs). The protocol proactively maintains information about the existence of all nodes in the mesh that are accessible via single-hop or multi-hop communication links. The strategy of B.A.T.M.A.N is to determine for each destination in the mesh, one single-hop neighbour which can be utilized as best gateway to communicate with the destination node. In order to perform multi-hop IP-based routing, the routing table of a node must contain a link-local gateway for each host or network route.” B.A.T.M.A.N is a layer 2 protocol, which means that it routes using MAC addresses. It should be noted that the B.A.T.M.A.N Internet-Draft has already expired, but the development of the protocol is ongoing and very active. The implementation efforts are led by the Freifunk⁵ community. The protocol is actively used in several wireless network communities, such as Freifunk in Germany or Ninux⁶ in Italy. As with Babel, the default B.A.T.M.A.N implementation is inherently insecure.

The security extension for B.A.T.M.A.N is described in [55]. It is based on the idea of short-lived certificates, called proxy certificates that are issued on site by a special node, called service proxy. These certificates are used to authenticate nodes in the initial handshake, while the actual packet exchange uses symmetric cryptographic primitives.

First, the service proxy authenticates a new node via an out-of-band channel and issues it a proxy certificate. This is a X.509 certificate that is not signed by a certificate authority, but by an end-entity certificate. Moreover, various restrictions can be put on the proxy certificate, which means that the issuer can fine-grain the delegated rights. Once the proxy certificate has been issued, the service proxy broadcasts the authentication list that carries the public keys of all nodes that have been granted access to the network; including the public key of the node to whom the proxy certificate has just been issued.

Once the node receives the issued proxy certificate, it broadcasts signed packets to all immediate neighbours. These packets carry elements from which the node (in a pairwise fashion) constructs security associations with each of its immediate neighbours. Each security association consists of a symmetric key stream. When sending a routing packet, the sender simply appends two bytes from the key stream associated with the outgoing link to the routing packet, while the receiver can verify that the two bytes are correct by comparing it with the two bytes from its own key stream. If the packet needs to be forwarded, the sender first replaces the two bytes it has already verified with the two bytes from the key stream associated with the new

³ <http://www.pps.univ-paris-diderot.fr/~jch/software/babel>

⁴ <https://github.com/Quagga-RE/quagga-RE>

⁵ <http://www.open-mesh.org>

⁶ <http://wiki.ninux.org>

out-going link. In this way every node only authenticates its immediate neighbour. This solution assumes that every node in the network can be trusted, since it has been verified by the service proxy.

Both implementation of the B.A.T.M.A.N protocol, insecure⁵ and secure⁷, can be obtained under open-source licenses. But while the insecure version is being actively managed and developed, the secure version is not.

4.3.1.3 ChaMeLeon Protocol

ChaMeLeon (CML) is an adaptive and hybrid routing protocol designed for Mobile Ad hoc NETWORKS (MANETs) supporting emergency communications [54]. The main concept behind CML is the adaptability of its routing mechanisms towards changes in the physical and logical state of a MANET. It consists of 3 phases of operation namely *Proactive*, *Oscillation* and *Reactive*. The *Proactive* (p-) and *Reactive* (r-) phases operate in the same way as the core functions of [56] respectively and are discrete from each other. The *Oscillation* phase (o-phase), therefore, acts as an intermediate between p- and r- phases and decides on whether a shift from p-phase to r-phase is appropriate based on some predefined criteria. The main purpose of the o-phase is to avoid the oscillation problem. CML introduces an Adaptive module which runs in parallel to and is accessible by all phases of operation. The module is designed to monitor relevant MANET characteristics, detect a certain quantitative threshold exhibited by specific monitored characteristics and in such an event, transfer the control to the o-phase. CML does not specify advanced security countermeasures, however, different security mechanisms in AODV and OLSR have been utilized within it. A secured variant of CML called Secured ChaMeLeon (SCML) [57] focusing on message and origin authentication, confidentiality and message integrity have been designed by using a hybrid version of Authentication Header (AH) and Encapsulating Security Payload (ESP) in transport mode of IPsec tailored for MANETs.

4.3.1.4 IEEE 802.11s

The IEEE 802.11s [48][49] is a standard for mesh networking. It extends the IEEE 802.11 MAC standard by defining an architecture and protocol that support packet delivery using radio-aware metrics over self-configuring multi-hop topologies. The 802.11s mandates that all implementations support the Hybrid Wireless Mesh protocol (HWMP), but it also allows other protocols (such as OLSR [52] or B.A.T.M.A.N to be used instead. HWMP is a hybrid routing protocol inspired by AODV [51] and tree-based routing. It routes using MAC addresses.

The IEEE 802.11s defines an authentication and key-establishment protocol called “Simultaneous Authentication of Equals” (SAE). The protocol is based on Diffie-Hellman key exchange and uses a PSK together with the MAC addresses to mutually authenticate the communicating peers. If SAE completes successfully, each node is assured the other party knows the pre-shared key; the nodes are now mutually authenticated. As a by-product of SAE, the peers also arrive at a pairwise master key (PMK) that they use to encrypt their frames, including routing traffic. Since the PMKs are different for every pair of communicating peers, each link is independently secured. However, while 802.11s does encrypt frames, it does not provide end-to-end encryption, since each peer is able to see the contents of exchanged frames.

The Open 802.11s [50] is an implementation of the IEEE 802.11s and it can be downloaded under an open-source licence. It has also been part of the Linux kernel since version 2.6.26.

4.3.1.5 Some remaining solutions

This section provides an overview of some additional solutions to secure routing protocols. These solutions, however, are rather confined to academic environments and often their implementations are not available nor are they well tested in real environments.

⁷ <https://github.com/espengra/secure-ad-hoc-network>

The first such example is *Authenticated routing for ad-hoc networks* (ARAN) [83]. ARAN provides authentication, message integrity and non-repudiation in all control messages exchanged between nodes. ARAN is based on a Public Key Infrastructure (PKI) and it uses a trusted Certification Authority (CA) that issues certificates to nodes. This happens prior to any communication via an out-of-band channel. ARAN secures route discoveries and route setups, where the communication initiator signs all control messages before sending it to the intended receiver. The intermediary nodes – the nodes on the path between the communication initiator and the intended receiver – also sign messages. The first intermediary adds its own signature (and certificate) to the message and forwards the message to the next intermediary en route to the intended receiver. Each remaining intermediary first verifies the signature (and the certificate) of the previous one, replaces it with its own and forwards the message. Such chain of pairwise signatures prevents message spoofing. The signature of the originating message, however, always remains with the message, so the intended receiver can verify its authenticity. Similarly, ARAN secures the messages for maintaining routes. All error messages – messages that announce broken links – are also signed. This, however, still allows an adversary to send false error messages, but since such messages are signed, the adversary's identity is revealed; the non-repudiation is ensured. Revocation of certificates is performed by CA by broadcasting the identity of revoked certificates.

In summary, in ARAN, unauthorized nodes – nodes without valid certificates – cannot participate in the ad-hoc network; authorized nodes cannot spoof messages, because the originator always signs them (link error messages can be fabricated, however, but the identity of such adversaries gets revealed); integrity of messages is ensured, because the meaningful message contents do not change it transit: there is no increasing of hop count or similar. However, the latter means that this protocol does not find the shortest (or globally optimal) path, but it finds the quickest path that was available during the route discovery. While ARAN features many appealing security properties, they generate notable computational overhead. Moreover, its performance results were only simulated and there exist no known publicly available or maintained implementation of this protocol.

Ariadne [84] is other example of a secure routing protocol. It is based on the *Dynamic Source Routing* (DSR) protocol, which is an on-demand (reactive) protocol; it discovers routes when needed and not periodically. Ariadne provides mechanisms for authenticating routing messages: to prove validity of route requests, to authenticate the list of nodes in route requests and route replies, and a mechanism called per-hop hashing technique to prevent malicious nodes from changing the node lists in route replies. Ariadne provides three different mechanisms to authenticate the node list in route requests and route replies: by using shared secrets between each pair of nodes, by using shared secrets between communicating nodes combined with broadcast authentication mechanism called TESLA, or by using digital signatures.

TESLA (Timed Efficient Stream Loss-Tolerant Authentication) [85] is a broadcast authentication mechanism that requires loose time synchronization. The problem of authenticating broadcast messages with shared secrets is that within the circle of nodes that know the shared secret, each node can forge messages and impersonate other nodes. So to authenticate broadcast messages, one needs an asymmetric primitive, which would allow the sender to generate authentication information and the receiver to verify it, but would also prevent the receiver to impersonate the sender. While traditional asymmetric protocols like RSA derive this asymmetry from expensive one-way trapdoor functions, TESLA achieves this by using clock synchronization and delayed key disclosure.

When Ariadne uses TESLA, each intermediary node en route to destination authenticates new information in the route request message. Once the destination node receives the route requests, it buffers it until all nodes that forwarded the message release their corresponding TESLA keys. The destination then verifies the message and returns a route reply. When the route discovery is performed with symmetric MACs, each intermediary node en route to

destination computes the MAC with the secret that it shares with the destination rather than with its current TESLA key. When using digital signatures, each node simply signs the newly added information to the route message with its private key. Similar to ARAN, Ariadne is rather confined to academic environment and has no known or publicly available implementation.

4.3.2 Infrastructure security

This section presents Wi-Fi security solutions in the infrastructure mode. In this mode, a special device - called access point - usually mounted to a fixed location, is used to connect nodes to other (wired) networks, for instance the Internet. Such access points are expected to be used near or inside established infrastructures, such as buildings.

Here we have two security concerns. First, because access points will often be managed by organizations not necessarily associated with PPDR organizations, PPDR personnel will consequently use third-party network equipment. Such equipment cannot be blindly trusted, because potential attackers, particularly insiders like network administrators, could read or modify the contents of exchanged information as it traverses the access point. And second, since Wi-Fi is inherently broadcast, anyone in the range of radio coverage can listen to radio traffic. This concern applies whether the access point is managed by the PPDR organization or whether by a third party.

To mitigate the first concern, SALUS platform should employ security solutions on the upper layers of the communication protocol stack, for instance by using IPsec, establishing virtual private networks or by securing communication at the application level. However, such solutions are not in scope of this section; we mention them because Wi-Fi can be a source of such threats, while the actual counter-measures are not related to Wi-Fi. Nonetheless, these threats must be addressed by the SALUS security architecture.

To mitigate the second concern, the exchanged frames - datagrams on layer 2 - need to be protected. Wi-Fi provides several solutions for this. However, these solutions exist due to historical reasons, and all of them, except the most recent, called Wi-Fi Protected Access 2 (WPA2), which is defined in IEEE 802.11i [59], have been found to be vulnerable. For instance, the initial solution, Wired Equivalent Privacy (WEP), was discovered to be very insecure [60], while its amendment Wi-Fi Protected Access (WPA), which is based on the draft of IEEE 802.11i, also exhibited several vulnerabilities [58]. As stated, the newest solution, Wi-Fi Protected Access 2 (WPA2), addresses the flaws of WEP and WPA. It mandates the use of better encryption and integrity algorithms that are currently considered secure.

Independent from the ways of providing encryption and integrity, Wi-Fi allows several authentication methods with which nodes and access points authenticate each other. In Personal mode (WPA2-PSK) the nodes and the access point share a common secret (a pre-shared key) from which they derive security associations. In the Enterprise mode (IEEE-802.1X [62]), the nodes get authenticated by a dedicated authentication server that supports RADIUS and EAP alike protocols.

Another mode of authentication, entitled Wi-Fi Protected Setup (WPS), was introduced to aid the unexperienced users in securing their home Wi-Fi networks. However, this feature inadvertently introduced a new security flaw that allows an attacker to obtain the WPA/WPA2 pre-shared key within hours of performing a brute-force attack [61]. It is therefore recommended to disable the WPS functionality.

It is important to note that the solutions presented in this section do not provide end-to-end security, but merely authenticate nodes to the access points and protect information exchanged between nodes and access points. These solutions do not protect data as it traverses the network beyond the access point.

4.3.3 Wi-Fi security vulnerabilities

This section introduces known Wi-Fi vulnerabilities. Although Wi-Fi is a technology that (in the ISO/OSI reference model) belongs to the physical and link layer, we also describe network layer vulnerabilities that arise from the use of ad-hoc routing protocols

4.3.3.1 Physical layer vulnerabilities

Because Wi-Fi is inherently broadcast, its radio signals can be easily overheard or jammed. Adversaries may thus remotely eavesdrop or physically disrupt the communication. Eavesdropping occurs when unintended receivers intercept and read (or possibly modify) the contents of messages. This threat is easily addressed by providing encryption and integrity checks at the upper layers of the protocol stack, usually at the link layer. Jamming occurs when an adversary uses a powerful transmitter to generate strong signals that overwhelm signals from legitimate Wi-Fi devices. Such jammers need not to emit any particular messages, random noise and pulse suffice. Jamming attacks are problematic because jamming equipment can be readily obtained and because they can be remotely launched.

4.3.3.2 Link layer vulnerabilities

Ad-hoc mesh network is an open multipoint peer-to-peer network, where one-hop connectivity (between neighbouring nodes) is provided by link layer protocols, while network layer protocols extend the connectivity over multiple hops. Adversaries targeting the link layer protocols thus try to subvert the connectivity between 1-hop neighbours.

Since all Wi-Fi devices share the same wireless medium, at any time only one device may emit radio signals. Therefore a medium access control (MAC) protocol is required to coordinate transmissions of multiple Wi-Fi hosts. The IEEE 802.11 Working Group has provided two algorithms for contention resolution [59]: a point coordination function (PCF), which is used in infrastructure mode, and a distributed coordination function (DCF), which is used in ad-hoc mesh networks. The PCF is implemented as a centralized protocol that runs on the access points, while the DCF is implemented as a carrier sense multiple access/collision avoidance protocol (CSMA/CA) that runs on each node of the ad-hoc network.

Since existing wireless MAC protocols assume that Wi-Fi nodes behave cooperatively, an adversary can simply ignore the contention resolution protocol and thus effectively break connectivity between communicating peers. For instance, an adversary may corrupt the frames by interfering with the ongoing transmissions or exploit the binary exponential backoff mechanism to completely capture the wireless medium and thus create a Denial of Service (DoS) attack. It is well known that heavily loaded nodes tend to capture the channel and thereby force lightly loaded nodes to backoff endlessly – this is called a capture effect [63]. Similarly, an attacker could exploit the information provided in the network allocation vector (NAV) field of control frames to direct DoS attacks at particular nodes.

Although all above attacks are performed at the link layer, they can all be classified as jamming attacks since they jam the wireless medium and degrade the performance of the wireless medium. However, link layer jamming is more challenging to detect, since one has to actively scan and examine the contents of the exchanged frames to locate attackers. The vulnerabilities of the Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) protocols and the vulnerabilities present in the Wi-Fi Protected Setup (WPS) functionality (described in section 4.3.2) should also be regarded as link layer vulnerabilities.

4.3.3.3 Network layer vulnerabilities

Network layer protocols provide connectivity between nodes that are separated by more than one hop. Because Wi-Fi falls below the network layer, we provide an overview of only those vulnerabilities that can emerge from the use of various Wi-Fi ad-hoc network routing protocols. The attacks described below allow adversaries to absorb network traffic, inject themselves into paths between honest nodes and thus control the flow in the network. The taxonomy of attacks is adopted from [64].

- **Routing table overflow.** The main idea of this attack is to overflow victims' routing table and thus render the network unavailable. Malicious nodes simply advertise routes to many non-existent nodes, while benign (authorized) nodes in good faith store them and thus overflow their routing tables. Proactive protocols are more prone to such attacks, since they usually exchange routing information more frequently.
- **Routing cache poisoning.** Some protocols take advantage of promiscuous mode of operation to optimize routing: upon overhearing a packet – that otherwise was not intended for that node – they store the contained routing information and use it for optimization. The adversary can attack such protocols by sending many spoofed packets that will eventually corrupt the routing caches of nodes that overhear them.
- **Routing maintenance attacks.** One of the most costly operations that nodes in the ad-hoc networks perform is maintaining routes; whenever a link breaks, all paths that pass through it, have to be invalidated and new ones need to be built. In these attacks the adversary simply sends false control messages stating, for instance, that a link is broken, when in fact it is not. These messages invoke costly operations and consequently reduce the availability of the network.
- **Data forwarding attacks.** In these attacks malicious nodes behave cooperatively when discovering and maintaining routes, but they misbehave when relaying data packets; they quietly ignore them, they modify their contents or they introduce large delays.
- **Wormholes.** This attack occurs when a node receives packets at one location in the network and tunnels them to another location; the tunnel between two colluding nodes is called a wormhole. Wormholes are particularly disruptive in reactive protocols, such as AODV, since they can prevent discovery of all routes other than those that traverse the tunnel.
- **Blackholes.** In this attack the adversary falsely advertises to be on a valid path to some destination, although the path through the adversary may not be the optimal or even exist. The goal of such false advertisements is to reroute traffic to intercept packets: when other valid nodes send packets to the destination and through the adversary, the latter simply drops them. A modified version in which the adversary selectively drops packets is called a Greyhole attack.
- **Rushing.** Rushing attack is formed by two colluders by setting up a fast wormhole; possibly by using an alternative communication medium. If the packets traversing the wormhole travel faster than packets traversing through the normal route, all routing protocols will favour paths through the wormhole. Once such paths are established, the data that traverses them is under adversaries' complete control.
- **Resource consumption.** Nodes that participate in the ad-hoc network often have limited power supply. By issuing excessive requests an adversary can expedite the power drain of valid nodes and thus reduce the network lifetime.
- **Location disclosure.** In this attack the adversary tries to establish the topology of the network and identify the participating nodes by examining the exchanged information. The goal of these types of attack is to obtain information to mount future attacks

4.3.4 Security analysis of Wi-Fi applicability towards future PPDR communications

The information on this subsection has been considered security sensitive and it has been moved to D5.1 RESTREINT UE Annex, which is a separated document (SALUS_D5.1_Annex.docx/pdf).

4.4 Security and privacy analysis of sensor networks

Existing and future sensor networks are to play an important role in the SALUS infrastructure. There are three major types of applications where sensor networks are planned to be used in SALUS:

- Alternative technology for connectivity on short and medium ranges, when usage of centralized infrastructure-based wireless network is impossible or not feasible from technical or economical perspective.
- Additional technology for positioning, when conventional satellite-based or cellular-assisted technologies cannot be efficiently applied. Indoor positioning could be considered as one of the examples;
- Primary technology to relay sensor data (biometric signals, data for smart meters, intrusion detection devices, etc.) to PPDR network.

The following sections present a high-level overview of the security mechanisms implemented in existing widely deployed sensor solutions with major focus on aspects crucial for the applications listed above.

4.4.1 Short-range sensor networks

In particular, Bluetooth [70] and Bluetooth Low Energy [69] are to be taken into account, as de-facto standards for Wireless Body Area Networks (WBAN) and Wireless Personal Area Networks (WPAN). The security level of Bluetooth technology is based on two techniques:

- Pairing mode phase: in which occurs the device pairing, which triggers the generation of the encryption key;
- Main mode phase: in which actual data is exchanged between the Bluetooth devices. Data are encrypted using the encryption key derived in the Pairing phase.

The only method available for Bluetooth v2.0 and lower is so-called “legacy 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. Three different options are possible:

- Pre-defined PIN for simple sensors or actuators (e.g. 0000 or 1234).
- Random 4 digit PIN selected by User/random generator for mobile devices.
- Random alpha-numeric PIN, selected by User for mobile devices with qwerty or similar keyboard.

Despite the fact this type of authentication is still widely used, 4 digit PIN is no longer sufficient for sensitive applications such as PPDR due to lack of valid PINs power set (less than 10 000 keys only, which gives high enough probability of guessing of PIN by an attacker) [65].

Another pairing technique, introduced in Bluetooth v2.1, is the Secure Simple Pairing (SSP, [71][70]). Currently, 4 variations of SSP are distinguished:

- Just works, replacing “Pre-defined key” option in legacy pairing. Requires no user interaction, however is vulnerable to Man-In-The-Middle (MITM) attack [71].
- Numeric, replacing interactive modes of legacy pairing. Displays on both sides as well as user confirmation are required to proceed with this option.
- Passkey entry option, when User enters two 6-digit codes on both devices or confirms the 6-digit code, generated by the device itself. This type of pairing is secure against majority of attacks including simple MITM.
- Out Of Band pairing. This method is similar to the previous one, despite the fact the out of band technology – usually, Near Field Communication (NFC) [72] – is used for key exchange instead of User. This method is also secure against the majority of known attacks [66][67].

Starting from Bluetooth v4.0 Advanced Encryption Standard (AES) [73] is used as the encryption algorithm for data transfer. Due to the fact no crucial vulnerability has been found in AES-128 so far [74], communication confidentiality could be considered secure enough. As such, the main focus from security point of view has to be put on the secure pairing (authentication) of PPDR devices.

4.4.1.1 PPDR-aware applications

WBAN and WPAN networks are considered the major solutions for short-range sensor networks in a PPRD-oriented infrastructure. In particular, wearable sensing and computing devices can be carried by emergency services (e.g. fire brigades) during the action. In this case, the security of proposed solutions could easily rely on the assumption that there is enough time before the action starts to establish secure connection between all wearable devices. When performing this type of pre-configurations, administrative personnel should also take into account the fact, that any sensor can be stolen by an attacker at any moment after deployment. As such, sensor encryption keys and all in-sensor sensitive data should be saved in a way that prevents unauthorized reading or modification. The particular technology to implement this requirement is independent from protocols used in PPDR and highly depends on type of sensor and its functionality. A possible technique (if applicable) is based on encrypting keys and sensitive data with TPM [75] or MTM [76] modules.

If encryption keys have to be updated after the sensor network is deployed in an untrusted environment, administrative personnel have to consider that in-band key establishment protocols may be vulnerable to MITM attacks. As such, the better alternative might be to use out-of-band signalling (e.g. NFC for SSP in Bluetooth).

4.4.1.2 Vulnerabilities in existing solutions

Despite the fact that currently deployed solutions for short-range wireless networks (namely, Bluetooth and Bluetooth Low Energy) are considered secure, there are many hardware and software available on the market that do not support the latest security algorithms and protocols. In particular, all Bluetooth v2.0 and lower devices are vulnerable to on-the-fly attacks during both pairing and main phase of communication. To the best of SALUS consortium knowledge, there is no feasible attack on latest Bluetooth v4.0 protocols. Therefore, usage of Bluetooth v4.0 certified devices and SSP pairing mode is proposed for SALUS infrastructure. In particular, *passkey* entry mode seems to be the most applicable from simplicity point of view. First, the usage of wireless human-unattended interface (which requires very limited human participation) can rapidly decrease the time required for configuration phase - in particular, there is no need to type all the PIN codes/passphrases on a set of devices. Secondly, the presence of a PIN facilitates the joining of additional devices into the network later on. Moreover, a PIN length of 6 digits increases the difficulty for an attacker to violate the security mechanisms and insert a 'fake' device into the PPDR sensor infrastructure. Please note that pairing mode does not require the presence of keyboards on the devices. The PIN can be stored and read in different ways (e.g. by an RFID or NFC reader).

4.4.2 Medium range sensor networks

In this subsection the security level of medium-range sensor networks is assessed. The most popular solution in commercial deployments is IEEE 802.15.4 (i.e. ZigBee) [75] and as such this is the reference medium-range sensor technology to be used in SALUS.

4.4.2.1 PPDR-aware applications

Medium-range sensor networks are considered as an enabler technology for indoor positioning and outdoor positioning on limited area, when conventional positioning techniques (GPS, A-GPS, etc.) are not available. Security and reliability, related to accurate positioning, are required for the three SALUS Use Cases, where PPDR units have to share their location with each other to coordinate activities. Considering IEEE 802.15.4 is a de-facto standard for medium-range sensor networks and indoor positioning plus being supported by a variety of equipment it would be selected for location purposes.

4.4.2.2 Vulnerabilities in existing solutions

The security of IEEE 802.15.4 relies on security of the channel encryption algorithm, Master Secret Key (MSK) storage and distribution, application layer security mechanisms that operate on top of MAC, and network layer encryption.

By default, ZigBee uses 128-bit encryption keys. Depending on the settings, the selected key could be associated with either the whole network or a particular link. If the key is network-wide it is typically pre-installed on devices during the configuration phase. If key is link-specific it can be pre-installed, established or delivered during the authentication phase of the protocol. If link encryption keys are not pre-installed on the device, then a security key establishment protocol is performed with assistance of special entity so-called “Trust Center”. This entity derives a set of link encryption keys from a single pre-installed encryption key called *Master Secret Key* (MSK). To provide the required level of security the MSK has to be installed to the Trust Center in a trusted environment (to prevent unauthorized key reading or modification by MITM attack). There are two recommended ways to perform this operation. One of the possible solutions is to pre-install MSK in the Trust Center before the sensor network is deployed. Another one is to distribute the MSK on the already deployed sensor network, but use a short-range out-of-band technology (e.g. keyboard or NFC).

Unfortunately the key transport protocol used in ZigBee is vulnerable to a variety of attacks that aim to either disclose the data transmitted via the network or even compromise/modify the data, which is very dangerous for positioning or similar type of PPDR applications [76][77].

One specific attack on a ZigBee network aims to force all the devices (group of devices) to switch to the most power-hungry mode for a long period of time, usually up to battery exhaustion [78]. Since the sensor nodes used for PPDR users are battery-powered, this type of attack has to be taken into account when designing future PPDR networks.

Summarizing, the security of existing deployments of IEEE 802.15.4 is high-enough for PPDR applications only if all the keys have been securely configured (e.g. pre-installed) on the sensors and sensor network infrastructure (such as the Trust Center). If there is no guarantee of such condition, there is a set of attacks that may reveal the MSK or link-specific keys during key transport. If network configuration is likely to be dynamic (e.g. adding/removal of devices), usage of additional application level security mechanisms is strongly recommended for PPDR usage. Application of network-wide Public Key Infrastructure (PKI) to authenticate all the PPDR devices without respect to their type (sensor/meter/server/etc.) is a good example.

4.4.3 Long-range sensor networks

IEEE 802.11ah is effectively almost the only notable standard for long-range sensor networks. As such, this standard is almost the only solution to be used for long-range sensor networks under SALUS use cases. At the same time, the IEEE 802.11ah is effectively not an independent standard rather than an amendment to IEEE 802.11-2007 (with some features of IEEE 802.11-2012 + modified PHY and MAC layers). The major difference is operating in sub GHz channel instead of 2.4 GHz and 5GHz channels for 2007 and 2012 standards. This all helped to “exchange” rate for distance and get up to 1 km range with up to 100 Kbps link layer throughput. At the same time, the P802.11- Task Group *ah* [79] claims they save as many subsections of the initial documents as possible. Therefore, the security procedure was taken directly from IEEE 802.11-2012: namely, WPA and WPA2.

Due to this fact, this is effectively the same infrastructure-based IEEE 802.11 Wi-Fi with same security procedures. IEEE 802.11ah has same pros and cons in terms of security and privacy as previously described in section 4.3.3.

All in all, there are less than 10 security-related contributions for the IEEE 802.11ah standardization group by Nokia, Motorola, etc. All of them suggest minor fixes in security mechanisms. But they do not modify the protocols rather than propose minor changes in their

implementation with respect to changed communication range (from 50 meters to 1 km) and number of nodes per cluster (from 10-20 up to 5000-7000). Example of these suggestions is to update the way of storing encryption keys on a router to optimize search time and memory consumption (which does not matter with 10-20 keys, but does with 5000-7000). All the “external” procedures are effectively the same.

Summarizing, despite playing on a different market and having a title “Protocol for sensor networks”, the IEEE 802.11ah, from security point of view, is effectively the same IEEE 802.11-2012 protocol with security features taken directly from IEEE 802.11i. IEEE 802.11i (WPA2) was already extensively described in Section 4.3.3.

5 ICT SECURITY RISK ANALYSIS FOR SALUS USE CASES

The information on this section has been considered security sensitive and it has been moved to D5.1 RESTREINT UE Annex, which is a separated document (SALUS_D5.1_Annex.docx/pdf).

6 CONCLUDING REMARKS - SECURITY AND PRIVACY REQUIREMENTS OF THE FUTURE PPDR SYSTEMS

Considering what has been described in previous sections, Table 11 identifies the most crucial security services to be safeguarded when deploying mission critical PPDR systems.

Table 11: Security and privacy requirements of the future PPDR systems

Security Service	Description	Relevance for future PPDR Systems
Sender authentication	The data was in fact sent from the user the message is pretended to be from (lawful interception may be applicable).	High End-user to end-user End-user to infrastructure (vice-versa) Between infrastructure components
Data authentication	The data belongs to the current conversation.	High End-user to end-user End-user to infrastructure (vice-versa) Between infrastructure components
User confidentiality	The user identification cannot be disclosed by non-authorized parties.	High End-user to non-authorized parties
Data confidentiality	The data exchanged by protected parties cannot be eavesdropped / disclosed by non-authorized parties (lawful interception may be applicable).	High End-user to non-authorized parties Infrastructure to non-authorized parties
Data Integrity	The data were not modified on their way from sender to receiver.	High End-user to non-authorized parties Infrastructure to non-authorized parties
Non-Repudiation	The sender of the data cannot deny he did in fact sent the data (implies asymmetric cryptography and assumes the signing key is properly safeguarded by the original owner, otherwise digital forgery can become a major concern).	High Between infrastructure components Medium End-user to end-user End-user to infrastructure (vice-versa)
Availability	Refers to the non-ability of either legitimate users or malicious third parties, with limited resources, to disable the communications infrastructure (or some of its features) without direct permission.	High End-user to infrastructure (vice-versa) Between infrastructure components

Please note that to safeguard the non-repudiation service, the proper deployment of Public Key Infrastructures (PKI) and support for digital certificates must be assured. Even though the implementation of such service is desirable, the operation/authentication of PPDR terminals based on digital certificates has not yet been achieved. The reasons behind this assumption relies on the fact that there are not yet regulatory guidelines for the implementation of a European-wide trusted PPDR Public Key Infrastructure (PKI), besides the fact that asymmetric encryption still has a high computation cost (which introduces delays) when compared with the current SIM-based symmetric encryption. Nevertheless, 3GPP is currently working on such a solution (TR 33.833 [44]).

From the description of the LTE, TETRAPOL and TETRA technologies, it can be derived that the security requirements mentioned in Table 11 are fulfilled. Other limitations may apply when dealing with untrusted 3GPP networks (as explained in section 1.8.3). For these networks in particular, initial terminal and infrastructure (mutual) authentication is ensured by the usage of pre-configured keys (SIM hardcoded, or similar) and the confidentiality and integrity services are safeguarded by cryptographic operations using well-defined and robust key derivation mechanisms and hierarchy. As described in the RESTREINT UE annex to this deliverable, the

major vulnerabilities to these technologies mainly exist on the theoretical plane, the centralized secure-by-design architecture of these technologies makes it difficult for third parties to successfully disrupt the PPDR operation - a considerable amount of resources is needed to crack the currently defined cryptographic operations. This is mainly the reason why TETRA and TETRAPOL are still considered robust to implement mission-critical PPDR operations. With the introduction of LTE Proximity Services (section 1.9), LTE is seen as the natural candidate to replace both TETRA and TETRAPOL in the next few years, but the LTE standard in general has still 5 to 8 years to be developed until it can match the TETRA and TETRAPOL reliability (availability), scalability and security requirements, therefore a significant large coexistence time-window between these technologies will exist. Further development on this topic will be addressed by SALUS Deliverables 4.3 and 4.6.

As for the IEEE 802.11 (Wi-Fi) networks, if proper care is taken with terminal and network (mutual) authentication, these networks can be protected against the majority of third-party security attacks – internal/inside attacks still pose a problem, mainly when operating in ad hoc mode, and need additional security control measures. Infrastructure mode has the capability to provide enhanced security services due to the deployment of centralized authentication services (such as the use of IEEE 802.1x with RADIUS/Diameter) on the infrastructure side. The main restrictions for the usage of IEEE 802.11 networks for mission critical PPDR operations are currently related to the limited range of operation and Quality of Service (QoS) support. The latter can be addressed by the IEEE 802.11e standard [80], but not completely assured since no dedicated spectrum exists specifically for PPDR Wi-Fi applications. In addition, as in many wireless networks, the IEEE 802.11 networks are susceptible to jamming.

Sensor networks can safely be used for PPDR operations, given the appropriate technology and precautions are used. Short range sensor networks such as Bluetooth v4.0 or medium range such as the ones based on IEEE 802.15.4 (as ZigBee) mainly need additional care on the configuration of the master session keys both on sensors and the pairing or infrastructure devices. The usage of key transport protocols is currently not advised for such configuration. Long range networks, based on IEEE 802.11ah, share the same security concerns as IEEE 802.11 networks described above. In general, sensor networks, with the exception of the non-repudiation and user confidentiality, support the security services described in Table 11.

The ICT security risk analysis for SALUS use cases, presented in the RESTREINT UE annex to this deliverable (section 5), establishes the foundation for the security & privacy requirements of SALUS, as well as risk mitigation plans to reduce the impact of the identified security risks. This analysis was made taking in consideration not only the currently defined SALUS Use cases, User Requirements, System and Enterprise Architecture, but also information from projects that share common principals with SALUS.

The survey presented in this deliverable and its RESTREINT UE annex serve as a base for the on-going work being developed in WP5, of main relevance to the SALUS Security and Privacy Architecture, to be presented on SALUS Deliverables D5.2 and D5.3.

7 BIBLIOGRAPHY

- [1] LTEWorld, "LTE Protocols & Specifications," [Online]. Available: <http://lteworld.org/lte-protocols-specifications> [on: 07-05-2014].
- [2] P. S. - N. S. N. Research, "How to secure an LTE-network: Just applying the 3GPP security standards and that's it?," 20 03 2012. [Online]. Available: https://www.troopers.de/wp-content/uploads/2011/10/TR12_TelcoSecDay_Schneider_LTE.pdf [on: 18-12-2103].
- [3] tutorialspoint, "LTE Radio Protocol Architecture," 2014. [Online]. Available: http://www.tutorialspoint.com/lte/lte_radio_protocol_architecture.htm [on: 07 05 2014].
- [4] 3GPP TS 23.401, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".
- [5] 3GPP TS 24.301 V12.4.0, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3," [on: 2014-03-17].
- [6] 3GPP TS 36.331 V12.1.0, "Radio Resource Control (RRC); Protocol specification," [on: 2014-03-19]
- [7] 3GPP TS 36.323 V11.2.0, "Packet Data Convergence Protocol (PDCP) specification," [on: 2013-03-18].
- [8] 3GPP TS 36.322 V11.0.0, "Radio Link Control (RLC) protocol specification," [on: 2012-09-12].
- [9] 3GPP TS 36.321 V12.1.0, "Medium Access Control (MAC) protocol specification," [on: 2014-03-20].
- [10] 3GPP TS 36.201 V11.1.0, "LTE physical layer; General description," [on: 2012-12-20].
- [11] 3GPP TS 36.211 V12.1.0, "Physical channels and modulation," [on: 2014-03-21].
- [12] 3GPP TS 36.212 V12.0.0, "Multiplexing and channel coding," [on: 2013-12-20].
- [13] 3GPP TS 36.213 V12.1.0, "Physical layer procedures," [on: 2014-03-21].
- [14] 3GPP TS 36.214 V11.1.0, "Physical layer; Measurements," [on: 2012-12-20].
- [15] 3GPP TS 33.401 v12.10.0, "3GPP System Architecture Evolution (SAE); Security architecture," [on: 2013-12-20].
- [16] M. Olsson, S. Sultana, S. Rommer, L. Frid e C. Mulligan, SAE and the Evolved Packet Core, Linacre House, Jordan Hill, Oxford OX2 8DP, UK: Elsevier Ltd., 2009.
- [17] 3GPP TS 33.102, "3G security; Security architecture".
- [18] Federal Information Processing Standards - Publication 197, "ADVANCED ENCRYPTION STANDARD (AES)," [on: 2001-11-26].
- [19] National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation - Methods and Techniques," 2001-12.
- [20] ETSI/SAGE, "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2," 2006.
- [21] National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," 2005.
- [22] 3GPP TS 36.331 V12.0.0, "Radio Resource Control (RRC); Protocol specification," [on: 2014-01-10].
- [23] 3GPP TS 24.301 V12.3.0, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)," [on: 2013 12 20].
- [24] LTE (Long Term Evolution) for public safety, Alcatel-Lucent website. Available: <http://www.alcatel-lucent.com/public-safety/lte> [on: 05-08-2014]
- [25] Transform Public Safety Communications Through Broadband Innovation, Motorola website. Available: <http://bit.ly/19XbhcO> [on: 05/08/2014]
- [26] 3GPP, "The Evolved Packet Core," [Online]. Available: <http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core> [on: 17-03-2014].
- [27] IETF RFC 5448, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," 2009-05.
- [28] IETF RFC 5996, "Internet Key Exchange Protocol Version 2 (IKEv2)," 2010-09.

- [29] 3GPP, "Public Safety," 07 2013. [Online]. Available: <http://www.3gpp.org/news-events/3gpp-news/1455-Public-Safety> [On: 15-05-2014].
- [30] 3GPP TS 22.278 V12.4.0, "Technical Specification Group Services and System Aspects; Service requirements for the Evolved Packet System (EPS)," 2013-09-20].
- [31] 3GPP TR 23.768 V2.0.0, "Study on architecture enhancements to support Group Communication System Enablers for LTE (GCSE_LTE)," [on: 2014-03-10].
- [32] 3GPP TS 22.468 V12.0.0, "Group Communication System Enablers for LTE (GCSE_LTE)," [on: 2013-07-02].
- [33] TETRA and Critical Communications Association, "Voice + Data (V+D)," [Online]. Available: <http://www.tandcca.com/about/page/12025> [on: 03-06-2014].
- [34] TETRA and Critical Communications Association, "Packet Data Optimised (PDO)," [Online]. Available: <http://www.tandcca.com/about/page/12028> [on: 03-06-2014].
- [35] ETSI EN 300 396-1 V1.2.0, "Technical requirements for Direct Mode Operation (DMO)," 2011-08.
- [36] TETRA and Critical Communications Association, "Direct Mode Operation (DMO)," [Online]. Available: <http://www.tandcca.com/about/page/12026> [on: 03-06-2014].
- [37] ETSI EN 300 392-7, "Voice plus Data (V+D); Part 7: Security".
- [38] ETSI EN 300 396-6, "Direct Mode Operation (DMO); Part 6: Security".
- [39] ETSI/SAGE Version: 1.4, "Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 2: ZUC Specification,"[On: 2010-07-30].
- [40] ETSI/SAGE Version: 1.4, "Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 1: 128-EEA3 and 128-EIA3 Specification," 2010-07-30.
- [41] Cryptography Research, "DPA Countermeasures," [Online]. Available: <http://www.cryptography.com/technology/dpa.html> [on: 27-02-2014].
- [42] T. Ming, C. PingPan e Q. ZhenLong, "Differential Power Analysis on ZUC Algorithm," Wuhan University, Wuhan 430072, China.
- [43] 3GPP TR 33.888 V0.2.0, "Study on security issues to support Group Communication System Enablers for LTE (GCSE_LTE)," 2014-02-21.
- [44] 3GPP TR 33.833 V0.4.0, "Study on security issues to support Proximity Services," 2014-02-24
- [45] RFC 6126, "The Babel Routing Protocol", April 2011. Available: <http://tools.ietf.org/html/rfc6126>
- [46] Internet-Draft, "Babel HMAC Cryptographic Authentication". Available: <http://tools.ietf.org/html/draft-ovsienko-babel-hmac-authentication-09>
- [47] Azzedine Boukerche, et al. Routing protocols in ad hoc networks: A survey, Computer Networks, 2011.
- [48] IEEE 802.11s standard, "IEEE Standard for Information Technology -Telecommunications and information exchange between systems - Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 10: Mesh Networking", 2011
- [49] Guido R. Hiertz, et al. IEEE 802.11s: the WLAN mesh standard. IEEE Wireless Communications, 2010.
- [50] Open 802.11s: Open-source implementation of 802.11s. <http://open80211s.org>
- [51] RFC 3561, "Ad hoc On-Demand Distance Vector (AODV) Routing", 2003. Available at: <http://tools.ietf.org/html/rfc3561>
- [52] RFC 3626, "Optimized Link State Routing Protocol (OLSR)". Available at: <http://tools.ietf.org/html/rfc3626>
- [53] B.A.T.M.A.N Internet-Draft, "Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N.)", 2008. Available at: <http://tools.ietf.org/html/draft-wunderlich-openmesh-manet-routing-00>
- [54] T. Ramrekha, E. Panaousis, G. Millar and C. Politis, "ChaMeLeon (CML): A hybrid and adaptive routing protocol for Emergency Situations", IETF draft-ramrekha-manet-cml-00.txt, 2010. Available: <http://tools.ietf.org/html/draft-ramrekha-manet-cml-00>
- [55] Bowitz, A.G., et al. BatCave: Adding security to the B.A.T.M.A.N. protocol. Sixth International Conference on Digital Information Management (ICDIM), 2011.

- [56] Perkins, C., Belding-Royer, E., and Das S., "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003.] and [Clausen, T. and P. Jacquet, "The Optimized Link State Routing Protocol", RFC 3626, October 2003.
- [57] E. Panaousis, T. Ramrekha, G. Millar, and C. Politis, "Adaptive and secure routing protocol for emergency mobile ad hoc networks," International Journal of Wireless and Mobile Computing, vol. abs/1005.1740, pp. 62–78, May 2010], [E. Panaousis, C. Politis, K. Birkos, C. Papageorgiou, and T. Dagiuklas, "Security model for emergency real-time communications in autonomous networks," Information Systems Frontiers, Springer Netherlands, vol. 14, pp. 541–553, 2012.
- [58] Toshihiro Ohigashi and Masakatu Morii. A practical message falsification attack on WPA. Proceedings of Joint Workshop on Information Security, Cryptography and Information Security Conference System, 2009.
- [59] IEEE 802.11i standard, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements", 2004
- [60] Scott Fluhrer, Martin Itsik and Adi Shamir. Weaknesses in the key scheduling algorithm of RC4. Selected areas in cryptography. Springer Berlin Heidelberg, 2001.
- [61] Jared Allar. Vulnerability Note VU#723755 – Wi-Fi Protected Setup PIN brute force vulnerability. Vulnerability Notes Data-base. US CERT. <http://www.kb.cert.org/vuls/id/723755>. [on: 29-04-2014].
- [62] IEEE 802.1x standard, "802.1X-2010 - IEEE Standard for Local and metropolitan area networks-- Port-Based Network Access Control ", 2010.
- [63] Hao Yang, et al. Security in mobile ad hoc networks: challenges and solutions. IEEE Wireless Communications, 2004.
- [64] Bing Wu, et al. A survey of attacks and countermeasures in mobile ad hoc networks. Wireless Network Security, 2007. 103-135.
- [65] Y. Shaked , A. Wool, CRACKING THE BLUETOOTH PIN, In Proc. 3rd USENIX/ACM Conf. Mobile Systems, Applications, and Services (MOBISYS), 2005.
- [66] A. Becker, BLUETOOTH SECURITY AND HACKS, 2007.
- [67] G.Padgette et al., "Guide to Bluetooth Security", Recommendations of The National Institute Of Standards and Technology (NIST),2012. [Available: http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf](http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf)
- [68] Bluetooth Special Interest Group. Available: <http://www.bluetooth.org>
- [69] "BT Low Energy", <http://www.bluetooth.com/Pages/Bluetooth-Smart.aspx>.
- [70] BT SIG, "Bluetooth Core Specification", version 4.1, December, 2013.
- [71] MITM attack, <http://www.veracode.com/security/man-middle-attack>.
- [72] ISO/IEC 11770-1, "Near Field Communications", (revised) 2013.
- [73] Advanced Encryption Standard, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>, 2011.
- [74] A. Bogdanov, D. Khovratovich, and C. Rechberger, Biclique Cryptanalysis of the Full AES, ASIACRYPT 2011.
- [75] Trusted Platform Module Version 1.2
http://www.trustedcomputinggroup.org/resources/tpm_main_specification
- [76] Mobile Phone Work Group Mobile Trusted Module Specification, Version 1.0, Revision 7.02.
[Available: http://www.trustedcomputinggroup.org/resources/mobile_phone_work_group_mobile_trusted_module_specification](http://www.trustedcomputinggroup.org/resources/mobile_phone_work_group_mobile_trusted_module_specification)
- [77] IEEE 802.15.4-2011, "IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)". Available:
<http://standards.ieee.org/about/get/802/802.15.html>
- [78] Cisco, ZigBee Wireless Security: A New Age Penetration Tester's Toolkit, 2012
- [79] IEEE P802.11- Task Group AH - Meeting Update, available:
http://www.ieee802.org/11/Reports/tgah_update.htm [on: 16-08-2014]
- [80] IEEE 802.11e, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part

- 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements”, 2005
- [81] L. Hongwei, Application and Analysis of ZigBee Security Services Specification, In Proc. of Second International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010.
- [82] N. Vidgren et al. Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned
- [83] Kimaya Sanzgiri, et al. A secure routing protocol for ad hoc networks. 10th IEEE International Conference on Network Protocols, 2002.
- [84] [Yih-Chun Hu, et al.](#) Ariadne: A secure on-demand routing protocol for ad hoc networks. Wireless networks, 2005.
- [85] RFC 4082, “Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction”, 2005.
Available at: <http://tools.ietf.org/html/rfc4082>
- [86] ETSI EN 300 812-3 V2.3.1, “Terrestrial Trunked Radio (TETRA); Part 3: Integrated Circuit (IC); Physical, logical and TSIM application characteristics,” 2005-12.
- [87] ETSI EN 300 392-1 V1.4.1, “Voice plus Data (V+D); Part 1: General network design,” 2009-01.
- [88] The TETRA + Critical Communications Association (TCCA), “Glossary and Definition of Terms in TETRA,” [Online]. Available: <http://www.tandcca.com/about/page/12023> [Accessed 31 07 2014].
- [89] 3GPP, “The Evolved Packet Core,” [Online]. Available: <http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core> [on: 03-07-2014].
- [90] Techtarget, “What is confidentiality, integrity, and availability (CIA)?,” [Online]. Available: <http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA> [Accessed 03 07 2014].
- [91] 3GPP TS 35.215 V11.0.0, “Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications,” 2012-09.
- [92] 3GPP TS 33.220 V12.3.0, “Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA),” 2014-06.
- [93] Third Generation Partnership Project 2 (3GPP2), “Welcome to the 3GPP2 Homepage!,” [Online]. Available: <http://www.3gpp2.org> [on: 04-07-2014].
- [94] 3GPP TR 23.703 V1.1.0, “Study on architecture enhancements to support Proximity-based Services (ProSe),” 2014-01.
- [95] 3GPP TS 23.468 V12.0.0, “Group Communication System Enablers for LTE (GCSE_LTE); Stage 2,” 2014-02.
- [96] Mobile Internet, “What is PCRF LTE and what does it mean to businesses?,” [Online]. Available: <http://cellinternet.wordpress.com/2011/10/13/what-is-pcrf-lte-and-what-does-it-mean-to-businesses> [on: 08-07-2014].
- [97] 3GPP TS 33.210 V12.2.0, “Network Domain Security (NDS); IP network layer security,” 2012-12.
- [98] TETRA and Critical Communications Association, “TETRA Release 1” [Online]. Available: <http://www.tandcca.com/about/page/12024> [on: 07-08-2014].
- [99] The Wassenaar Arrangement, [Online]. Available: <http://www.wassenaar.org/> . [on:06-08-2014]
- [100] ETSI EN 302 109 V1.1.1, “Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption”, 2003-06
- [101] TETRA MoU Association, “TETRA Security”. London , 2006.
- [102] Parkinson, D. W., “TETRA Security”. [2001, BT Technology Journal, Vol. 19, pp. 81-88](#)
- [103] TETRA Association Security and Fraud Prevention Group (SFPG), “SFPG Recommendation 02 – End-to-End Encryption”
- [104] TETRA Association Security and Fraud Prevention Group (SFPG), “Overview of Standard TETRA Cryptographic Algorithms and their rules for management and distribution”, 2008. [\[Online\]. Available: http://www.tandcca.com/Library/Documents/Files/Documents/Overviewofstandardcryptographicalgorithms.pdf](#) . [on: 01-08-2014]

- [105] ETSI EN 300 392-2 V2.3.2, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)", 2001-03

ACRONYMS

#	
3GPP	3rd Generation Partnership Project
A	
AAA	Authentication Accounting and Registration
AES	Advanced Encryption Standard
AIE	Air Interface Encryption
AKA	Authentication and Key Agreement
AM	Acknowledgement Mode
AMF	Authentication Management Field
AN	Access Network
ARQ	Automatic Repeat Request
ASME	Access Security Management Entity
AUC	Authentication Centre
AUTN	Authentication Token
AV	Authentication Vector
B	
BS	Base Station
BM-SC	Broadcast Multicast Service Centre
C	
CC	Color Code
CCK	Common Cipher Key
CK	Cipher Key
CMAC	Cipher-based MAC
CML	ChaMeLeon (CML): A hybrid and adaptive routing protocol for Emergency Situations
CN (1)	Core Network
CN (2)	Carrier Number
D	
DCF	Distributed Coordination Function
DCK	Derived Cipher Key
DeNB	Donor eNB
DMO	Direct Mode Operation
E	
EAP-AKA	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement
EAP-AKA'	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement

E2EE	End-to-End Encryption
ECK	Encrypted Cipher Key
EDGE	Enhanced Data rates for GSM Evolution
EGSKO	Extended Group Session Key for OTAR
ENISA	The European Union Agency for Network and Information Security Agency
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
ETSI	European Telecommunications Standards Institute
E-UTRA	Evolved Universal Terrestrial Radio Access
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
F	
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
HeNB	Home eNodeB
HMAC	Keyed-Hashing for Message Authentication
HLR	Home Location Register
HRPD	High Rate Packet Data
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HWMP	Hybrid Wireless Mesh protocol
I	
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IK	Integrity key
IKE	Internet Key Exchange Protocol
ISDN	Integrated Services Data Network
ITSI	Individual TETRA Subscriber Identity
IV	Initial Value

J	
K	
K	Authentication Key
KASME	Access Security Management Entity Key
KS / KS'	Session Authentication Key
KSI	Key Set Identifier
KSG	Key Stream Generator
KSS	Key Stream Segment
L	
LA-id	Location Area Identification
LAI	Location Area Identification
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
MITM	Man-In-The-Middle
MME	Mobility Management Entity
MS	Mobile Station
MSIN	Mobile Station Identification Number
MSK	Master Shared Key
MT	Mobile Terminal
N	
NAS	Non Access Stratum
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
OTAR	Over The Air Re-keying
P	

P-TMSI	Same as TMSI
PABX	Private Automatic Branch Exchange
PCF	Point Coordination Function
PCRF	Policy and Charging Rules Function
PDCCP	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
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	
RAI	Routing Area Identification
RAN	Radio Access Network
RAND	Random challenge
RANDx	Random Challenge
RESx	Response
RLC	Radio Link Control
RLC AM	Radio Link Control Acknowledgement Mode
RLC UM	Radio Link Control Unacknowledged Mode
RN	Relay Node
ROHC	Robust Header Compression
RRC	Radio Resource Control
RT	Radio Terminal
Rx	Result
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
SCK	Static Cipher Key
SDU	Service Data Unit

SEGs	Security Gateways
SFPG	Security and Fraud Protection Group
SIM	Subscriber Identity Module
SN	Serving Network
SQN	Sequence Number
SSP	Secure Simple Pairing
SwMI	Switching and Management Infrastructure
T	
TAxx	TETRA Algorithm
TB	Transport Blocks
TE	Terminal Equipment
TEAxx	TETRA Encryption Algorithm
TEDS	TETRA Enhanced Data Service
TETRA	Terrestrial Trunked Radio
TMO	trunked-mode operation
TMSI	Temporary Mobile Subscriber Identity
U	
UDT	User Data Terminal
UE	User Equipment
UEAx	UMTS Encryption Algorithm Suite x
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
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPAN	Wireless Personal Area Networks
WPS	Wi-Fi Protected Setup
X	
XRESx	Expected Result/Response
Y	

Z	