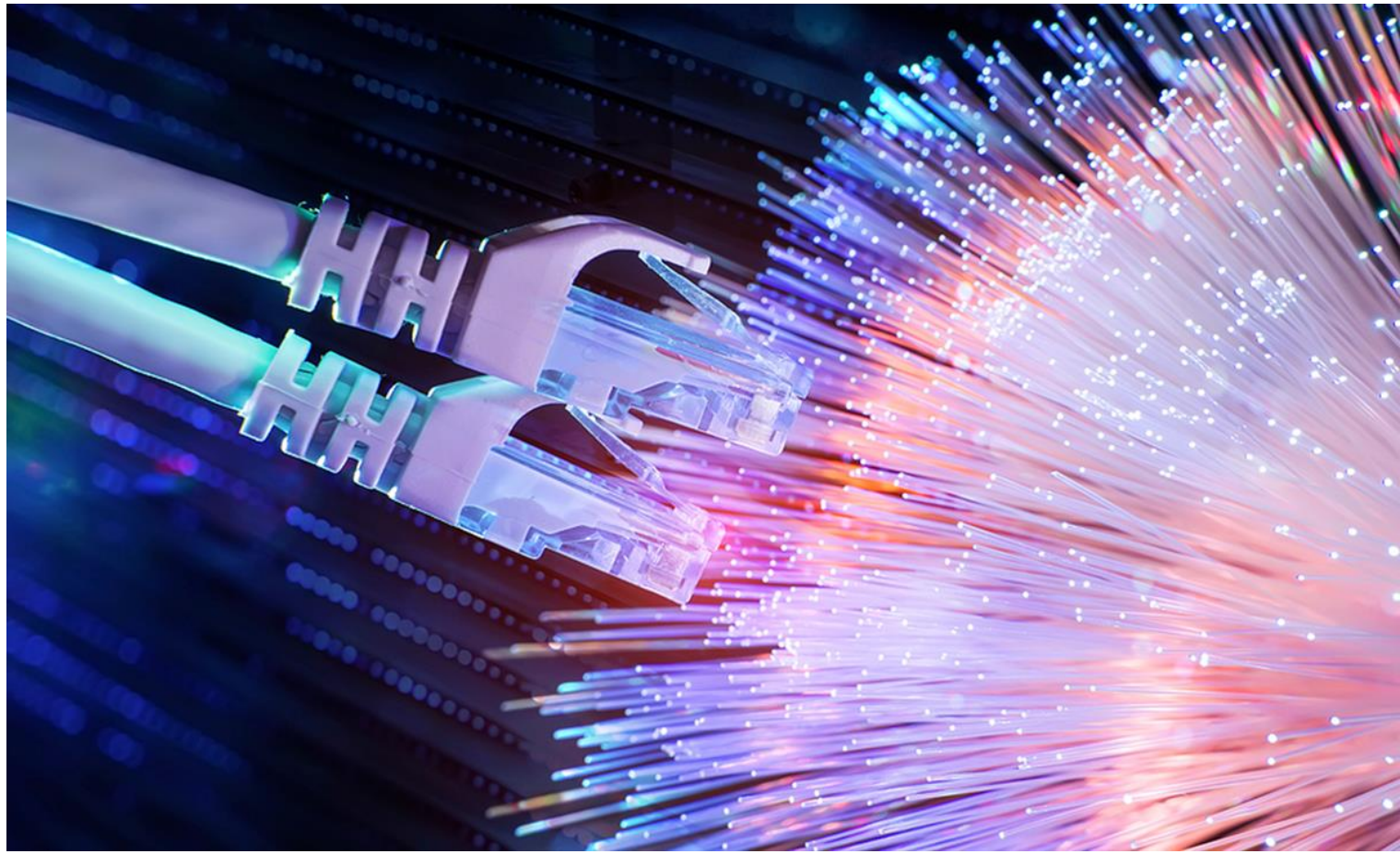
ARUP

Digital Technology

Professional Telecoms Services



Marc Winterton, **Paul Hales**

1st March 2023

Arup

Who are we?

ARUP

ARUP

Arup in the UK

Overview and offices

17 offices
across the UK

75 years
working in the region

ARUP

Key elements of an LTE Network.

Paul Hales

01/03/2023

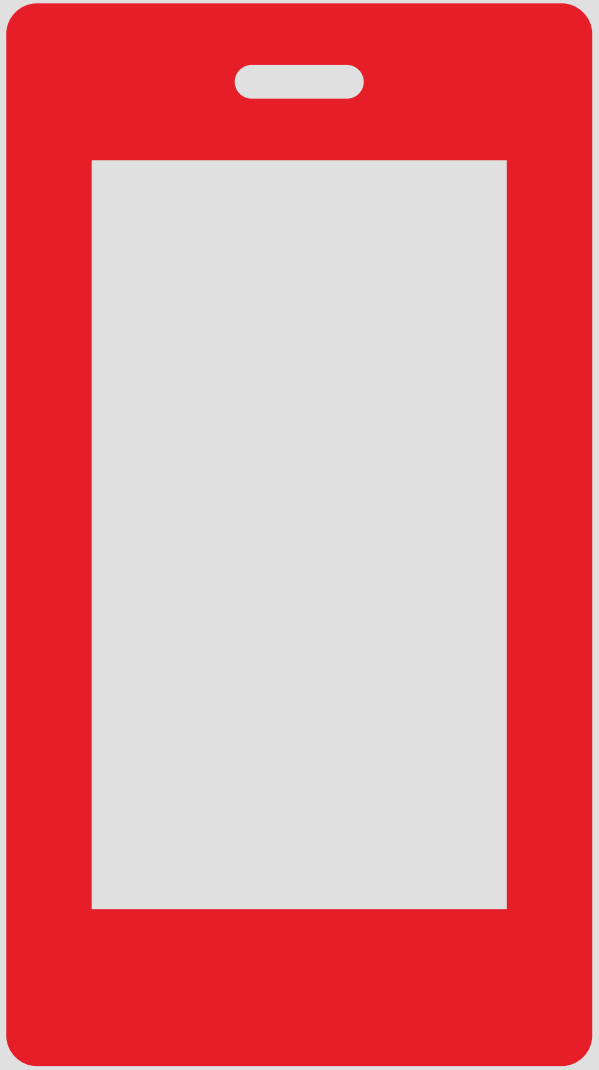
The need for orchestration and complexity of implementing large mission critical LTE networks

- Transition from a passive network to a dynamic network taking into account Distribute Energy Resources (DER) including renewables contributing into the supply.
- Net Zero, energy networks will need to be more flexible as renewable energy generation, energy storage systems, and millions of low carbon devices such as electric vehicles, heat pumps and micro-generation are connected across every tier of the network.
- Distribution Network Operators (DNOs) are being challenged as Distribution System Operators (DSOs) to use a broader range of tools to manage and operate networks as efficiently as possible.
- These tools include enhanced monitoring & planning; real-time network reconfiguration; actively managing system voltages; and using commercial arrangements to balance the electricity system generation with demand and to manage system constraints.
- These operations all have one thing in common: they require access to a resilient and reliable communications solution to plan, monitor, control and protect networks whilst addressing an increasingly complex and fragmented demand profile from consumers.

ARUP

LTE Architecture

Overview

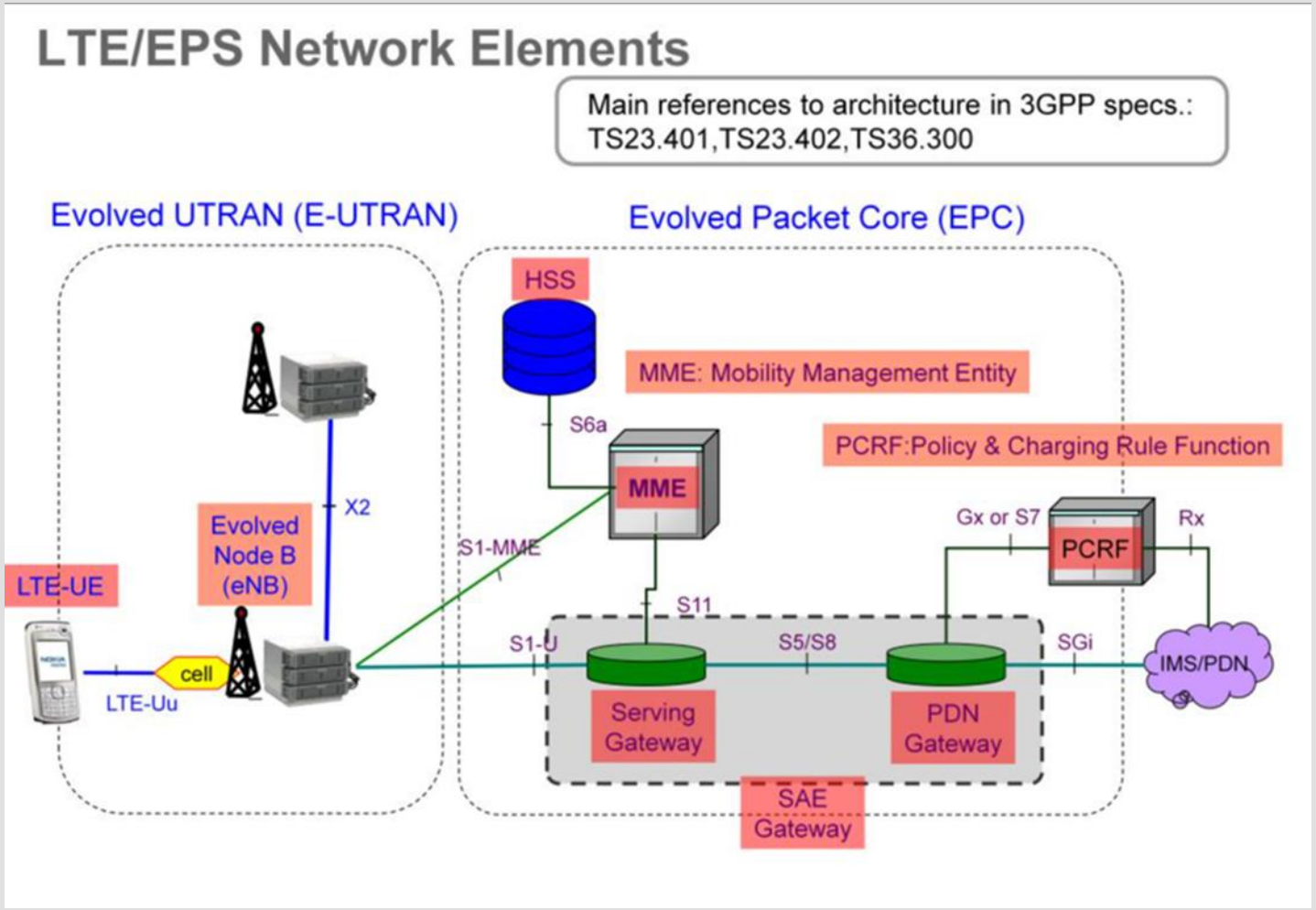


LTE?

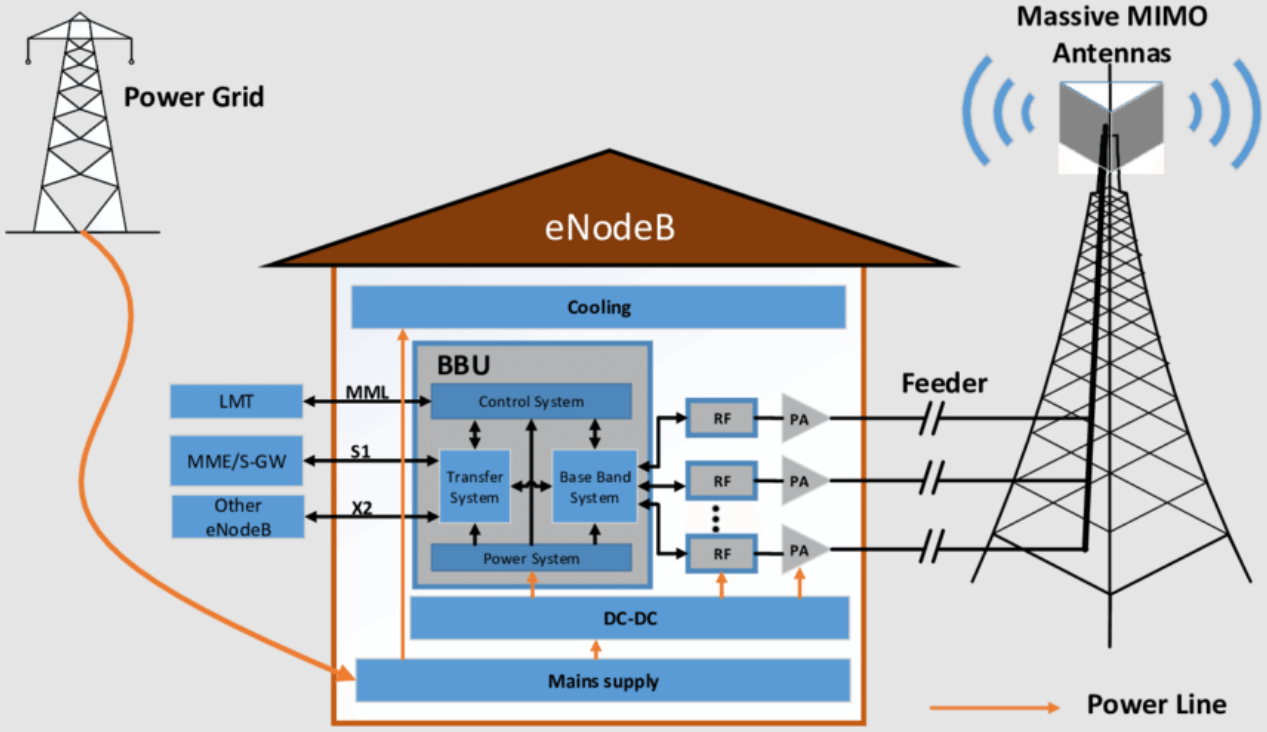
- Long Term Evolution (LTE), the 4th generation (4G) mobile broadband technology defined by 3GPP.
- High spectral efficiency with cutting edge digital communication techniques.
- Orthogonal Frequency-Division Multiple Access (OFDMA)
- Multiple-Input and Multiple-Output(MIMO)
- It can operate in numerous frequency bands and accommodate different channel size, catering to different spectrum availability situations and applications.

LTE Architecture

ARUP



eNode B



- Manages radio resources, including radio bearer control, radio admission control,
- Connection mobility control, resource scheduling and resource sharing.
- Routes user-plane and signaling-plane data towards a core network.
- Selects a core network.
- Schedules and transmits broadcast information and paging messages.
- Performs measurement and configures measurement reporting.

Mobility Management Entity (MME)

LTE MME is responsible for initiating paging and authentication of the mobile device.

The MME is in charge of all the Control plane functions related to subscriber and session management. From that perspective, the MME supports the following:

•Security procedures – this relates to end-user authentication as well as initiation and negotiation of ciphering and integrity protection algorithms.

•Terminal-to-network session handling – this relates to all the signaling procedures used to set up Packet Data context and negotiate associated parameters like the Quality of Service.

•Idle terminal location management – this relates to the tracking area update process used in order for the network to be able to join terminals in case of incoming sessions.

The MME is linked through the S6 interface to the HSS which supports the database containing all the user subscription information.

Home Subscriber Server (HSS)

- The Home Subscribe Server is the main IMS database which also acts as database in EPC. The **HSS** is a super HLR that combined legacy HLR and AuC functions together for CS and PS domains
- User identification and addressing – this corresponds to the IMSI (International Mobile Subscriber Identity) and MSISDN (Mobile Subscriber ISDN Number) or mobile telephone number.
- User profile information – this includes service subscription states and user-subscribed Quality of Service information (such as maximum allowed bit rate or allowed traffic class).
- The AuC part of the HSS is in charge of generating security information from user identity keys. This security information is provided to the HLR and further communicated to other entities in the network. Security information is mainly used for:
- Mutual network-terminal authentication.
- Radio path ciphering and integrity protection, to ensure data and signaling transmitted between the network and the terminal is neither eavesdropped nor altered.

Serving GPRS Support Nobe (SGW)

- The **Serving GPRS Support Node** (**SGSN**) is a main component of the GPRS network, which handles all packet switched data within the network, e.g., the mobility management and authentication of the users. The **SGSN** performs the same functions as the MSC for voice traffic.
- From a functional perspective, the Serving GW is the termination point of the packet data interface towards E-UTRAN. When terminals move across eNodeB in E-UTRAN, the Serving GW serves as a local mobility anchor, meaning that packets are routed through this point for intra E-UTRAN mobility and mobility with other 3GPP technologies, such as 2G/GSM and 3G/UMTS.

Packet Data Network Gateway (PGW)

- Packet Data Network Gateway (PGW) is a critical network function for the 4G mobile core network, known as the evolved packet core (EPC). The PGW acts as the interface between the LTE network and other packet data networks, such as the Internet or SIP-based IMS networks

- The Packet Data Network (PDN) Gateway (P-GW) communicates with the outside world ie. packet data networks PDN, using SGi interface. Each packet data network is identified by an access point name (APN)
- Similarly, to the Serving GW, the PDN gateway is the termination point of the packet data interface towards the Packet Data Network. As an anchor point for sessions towards the external Packet Data Networks, the PDN GW also supports Policy Enforcement features (which apply operator-defined rules for resource allocation and usage) as well as packet filtering (like deep packet inspection for virus signature detection) and evolved charging support (like per URL charging).

.

Policy and Charging Rules Function Server (PCRF)

The PCRF (Policy and Charging Rules Function) Server

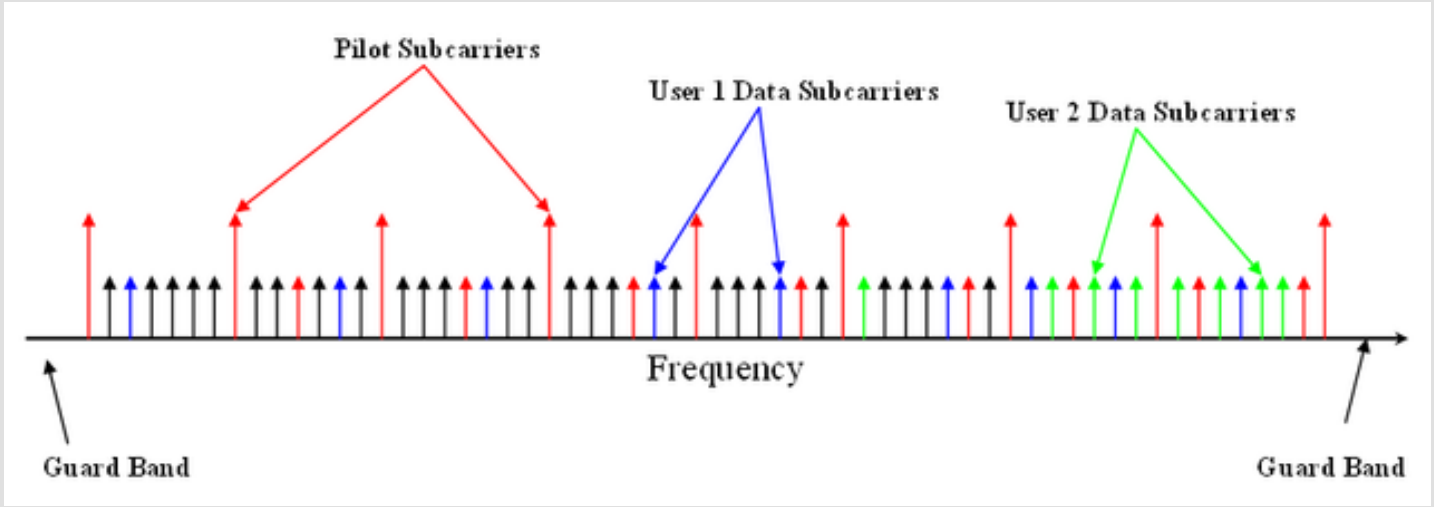
- The PCRF server manages the service policy and sends QoS setting information for each user session and accounting rule information. The PCRF Server combines functionalities for the following two UMTS nodes:
- The Policy Decision Function (PDF)
- The Charging Rules Function (CRF)
- Allowing or rejecting the media request..
- Checking the allocation of new resources against the maximum authorized.

OFDMA

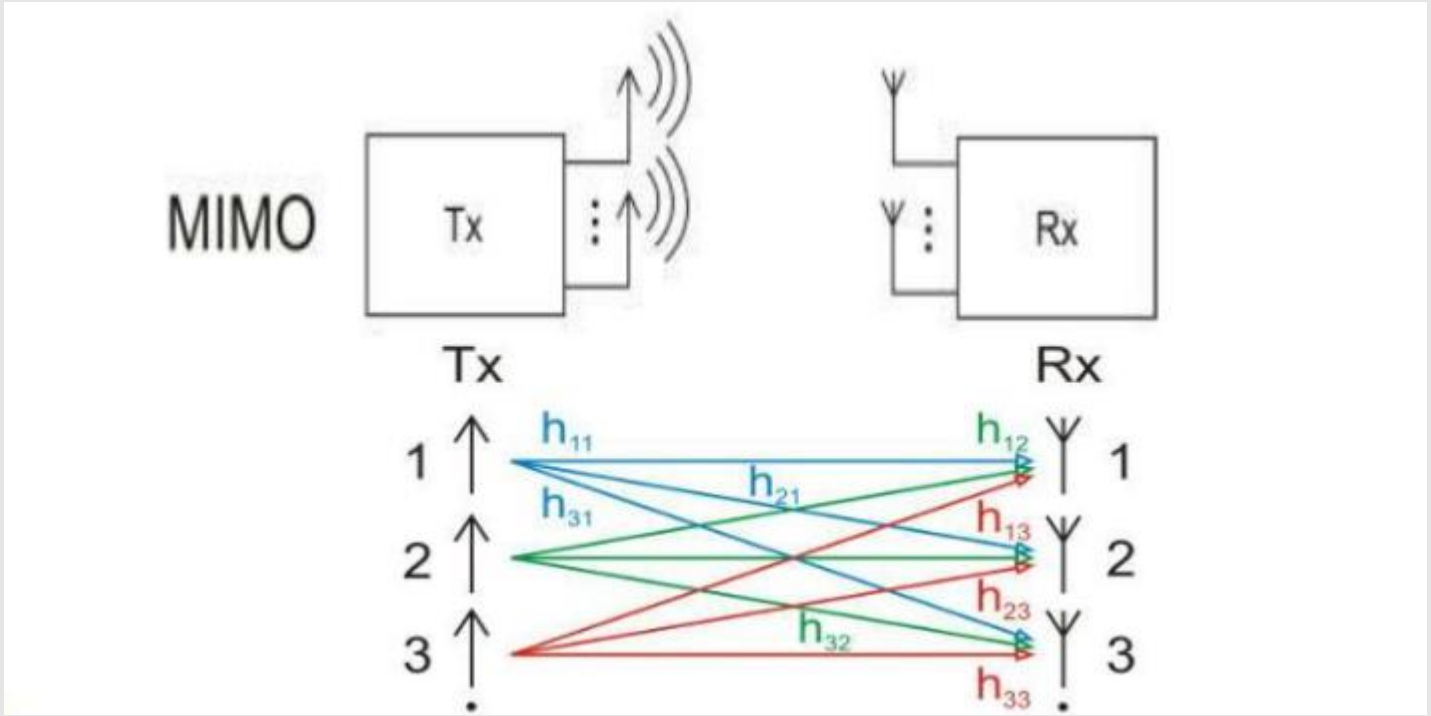
Orthogonal Frequency Division Multiple Access

ARUP

Orthogonal frequency-division multiple access



MIMO



MIMO (multiple input, multiple output) is an antenna technology for wireless communications in which multiple antennas are used at both the source (transmitter) and the destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed

Quality of Service (QoS)

- To ensure that carrier traffic in LTE networks is appropriately handled, a mechanism is needed to classify the different types of carriers into different classes, with each class having appropriate QoS parameters for the traffic type.
- Examples of the QoS parameters include Guaranteed Bit Rate (GBR) or non-Guaranteed Bit Rate (non-GBR), Priority Handling, Packet Delay Budget and Packet Error Loss rate. This overall mechanism is called QCI(Quality of Service Class Identifier)

Encryption and Security

2.1 Scope and Concept of LTE Security

Figure 1 below shows the scope and overall concept of the LTE Security documents. The scope of these documents will include the following three areas:

1. LTE Authentication: performs mutual authentication between a UE and a network.
2. NAS Security: performs integrity protection/verification and ciphering (encryption/decryption) of NAS signaling between a UE and an MME.
3. AS Security
   - performs integrity protection/verification and ciphering of RRC signaling between a UE and an eNB.
   - performs ciphering of user traffic between a UE and an eNB.

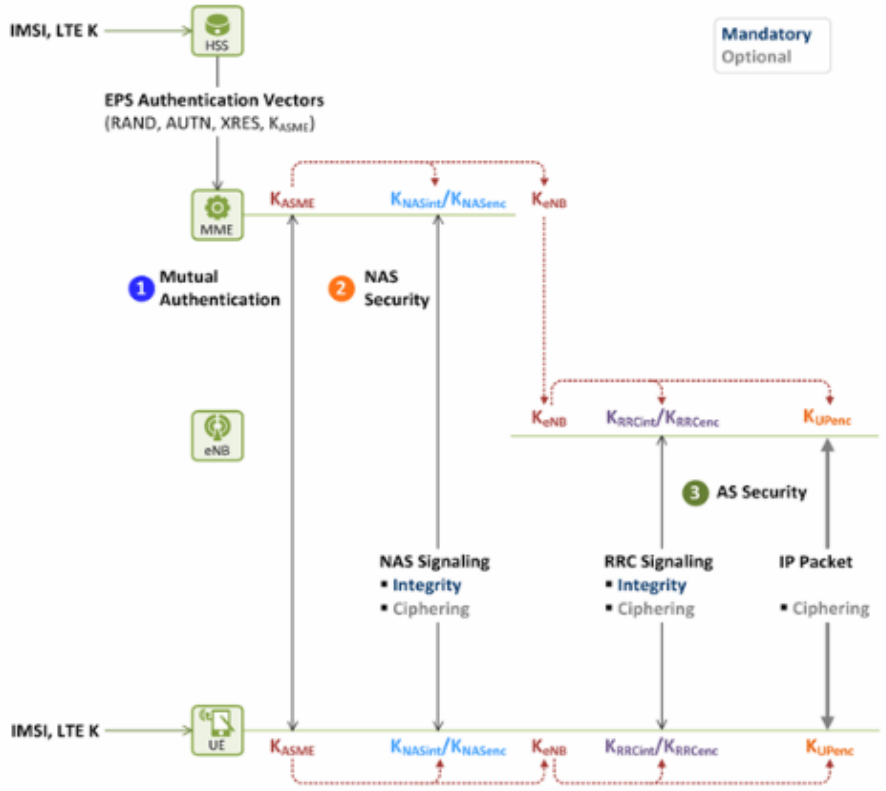
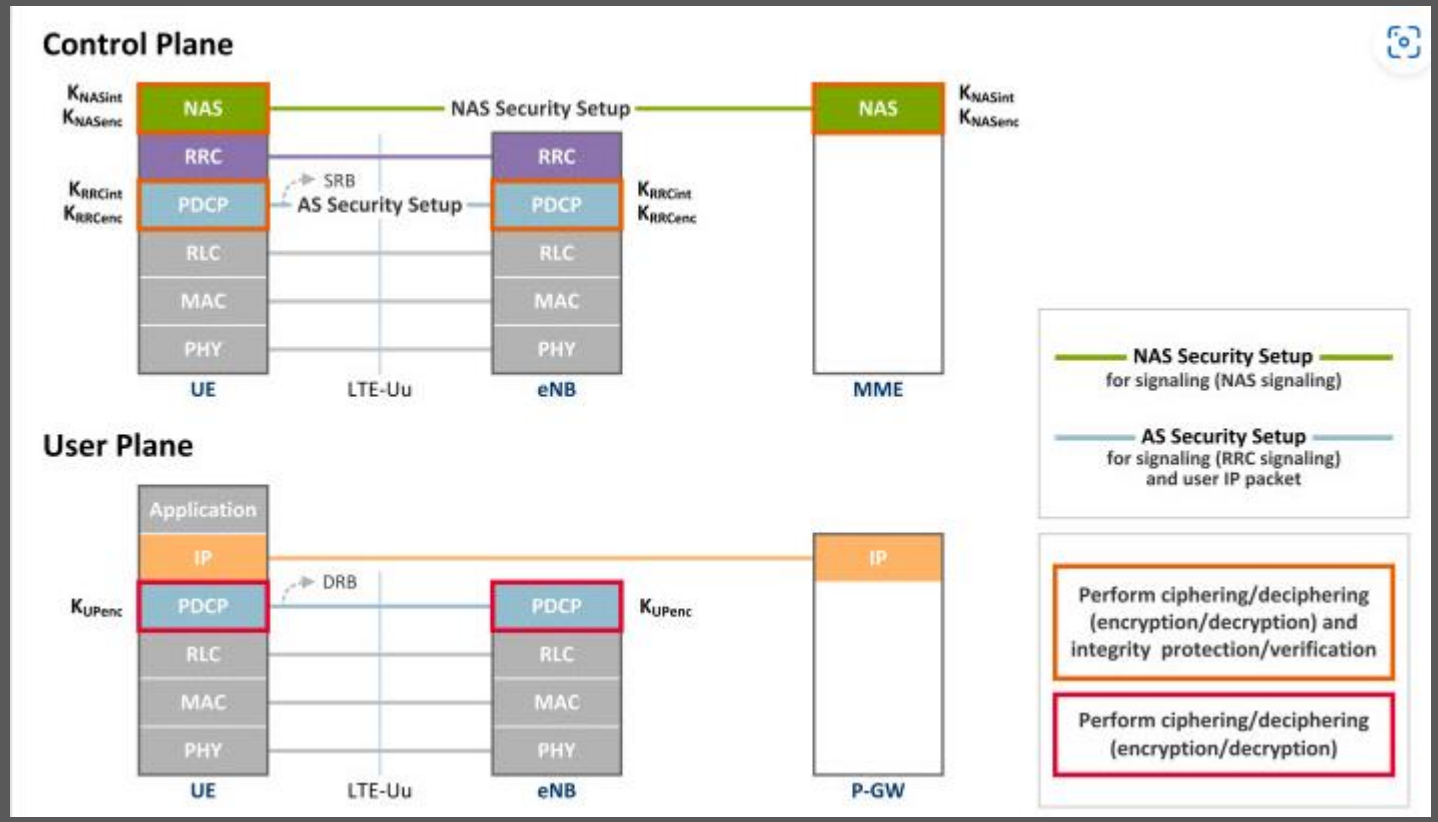


Figure 1. Scope and concept of LTE security

LTE Authentication

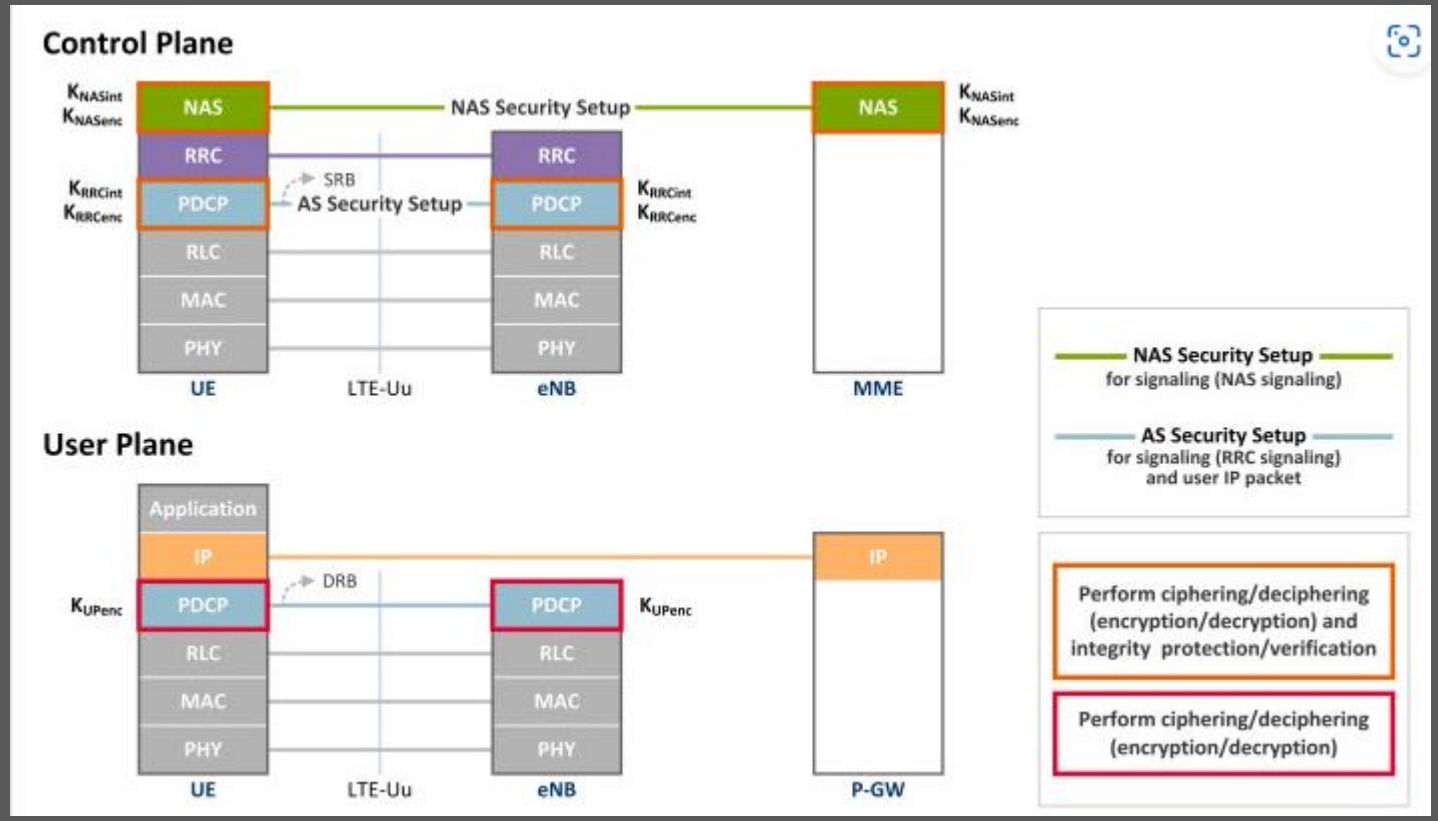
In mobile communication networks, authentication refers to the process of determining whether a user is an authorized subscriber to the network that he/she is trying to access. Among various authentication procedures available in such networks, EPS AKA (Authentication and Key Agreement) procedure is used in LTE networks for mutual authentication between users and networks.

NAS Security



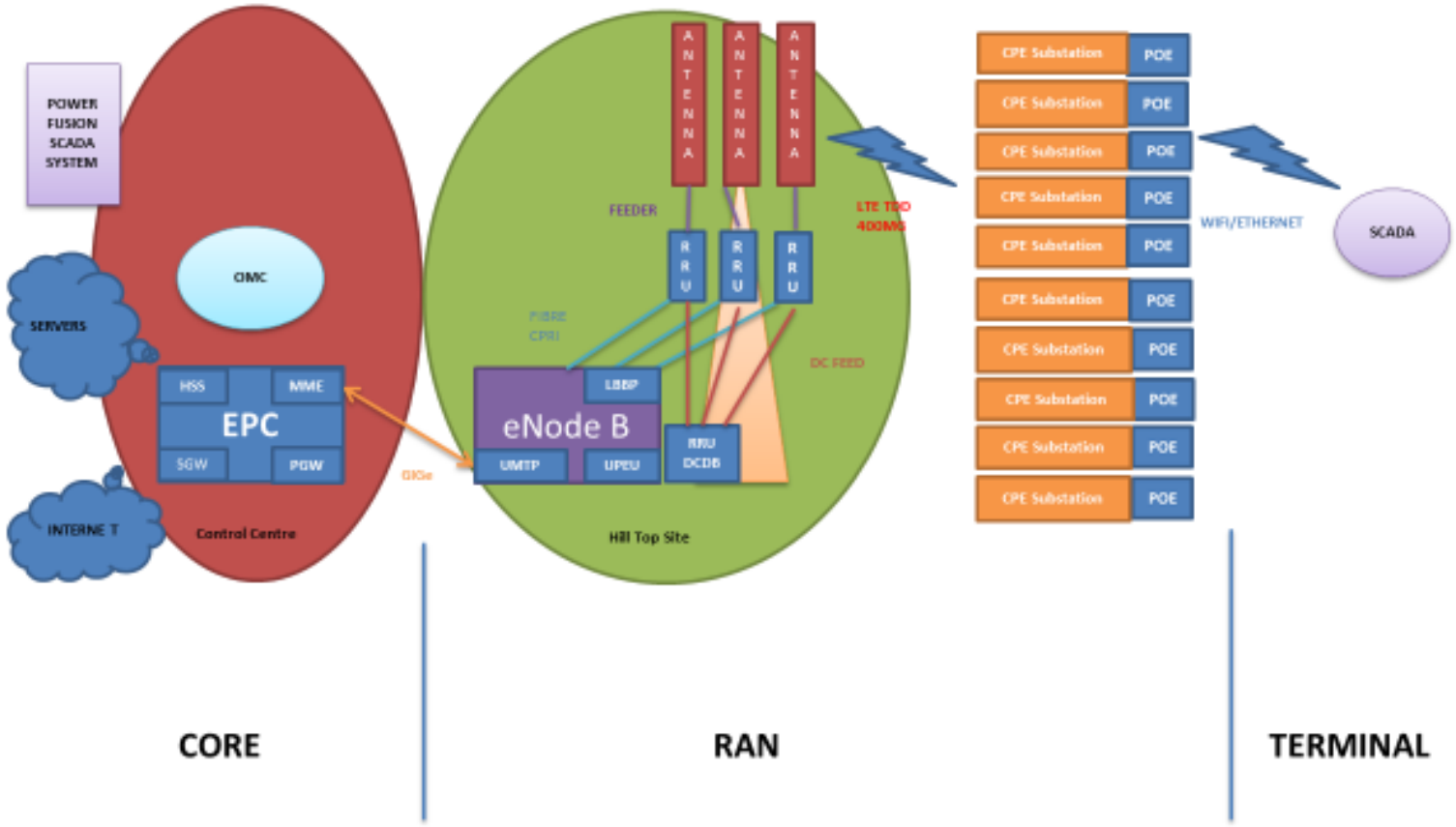
NAS security, designed to securely deliver signalling messages between UEs and MMEs over radio links, performs integrity check (i.e., integrity protection/verification) and ciphering of NAS signalling messages. Different keys are used for integrity check and for ciphering. While integrity check is a mandatory function, ciphering is an optional function.

AS Security



AS security is purposed to ensure secure delivery of data between a UE and an eNB over radio links. It conducts both integrity check and ciphering of RRC signalling messages in control plane, and only ciphering of IP packets in user plane. Different keys are used for integrity check/ciphering of RRC signalling messages and ciphering of IP packets. Integrity check is mandatory, but ciphering is optional.

LTE for a DNO


POWER FUSION SCADA SYSTEM
OMC
SERVERS
HSS
MME
EPC
SGW
PGW
INTERNE T
Control Centre
FEEDER
ANTENNA
ANTENNA
ANTENNA
RRU
RRU
RRU
LTE TDD 400MG
DC FEED
LBBP
eNode B
UMTP
UPEU
RRU DCDB
HBI Top Site
CPE Substation
POE
WIFI/ETHERNET
SCADA
CORE
RAN
TERMINAL

Questions

Contact Details

ARUP

Marc Winterton

Associate Director | UKIMEA Head of Rail Telecommunications

10th Floor The Plaza

100 Old Hall Street

Liverpool L3 9QJ

United Kingdom

t: +44161 228 2331

d: +44161 602 9009

m: +44 7799 773789

Paul Hales

Senior Consultant, Digital Services Portfolio

10th Floor The Plaza

100 Old Hall Street

Liverpool L3 9QJ

United Kingdom

d: +44 161 602 9681

m:+044 7799 909302

www.arup.com

Connect with Arup on LinkedIn

Follow @ArupUKIMEA

ARUP