# LTE Security – Facts & Fictions

Joshua Franklin

BSIDES
Charlotte

# Introduction

- Cellular networks are a complicated subject
- 3GPP standards are confusing
- Cellular security claims are thrown around a lot
  - Hard to tell what is true
- We will discuss LTE networks/security
- We'll keep an eye on LTE standards
  - **Security claims based in reality**

# Agenda

- Who I am
- What is LTE
- Cellular standards
- Important cellular concepts
- Network architecture
  - Components and protocols
- Security architecture
  - Authentication, cryptography, etc.
- Further Reading / Release of Updated Material

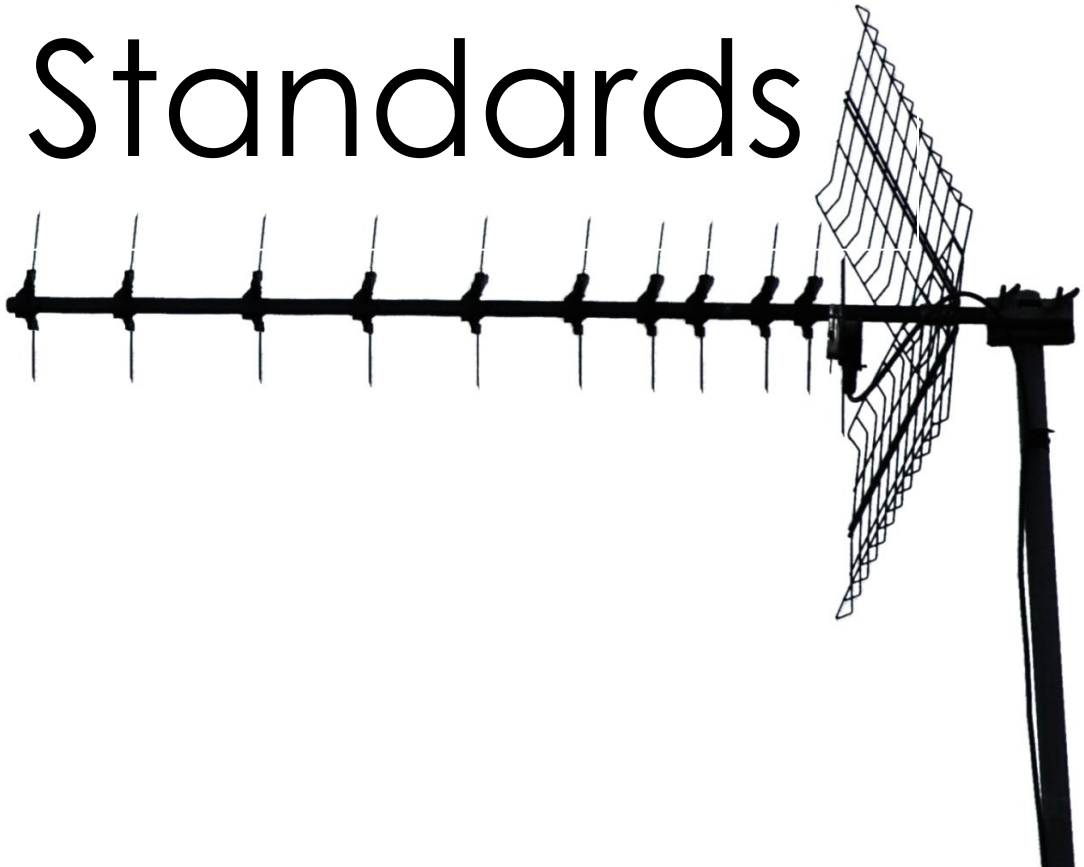
# Stats

- Subject: Joshua Franklin
- Location: Washington, DC
- Age: 27
- Height: 6’3
- Weight: ?
- Work: NIST, Computer Security Division
- Education: Masters in Information Security and Assurance from George Mason
- Focus on electronic voting and mobile security

# What is LTE

- LTE = Long Term Evolution
- Fourth generation cellular technology standard from the 3rd Generation Partnership Project (3GPP)
- Deployed worldwide and installations are increasing
- All implementations must meet baseline requirements
  - Increased Speed
  - Multiple Antennas (i.e., MIMO)
  - IP-based network (All circuits are gone/fried!)
  - New air interface: OFDMA (Orthogonal Frequency-Division Multiple Access)
  - Also includes duplexing, timing, carrier spacing, coding...
- LTE is always evolving and 3GPP often drops new "releases"
  - New releases are essentially a freeze of the body of LTE standards
  - Release 12 freezes December 2014
  - Let's take a look at the standards

# Cellular Standards



# What is 3GPP?

- An international standards body
- Standardizes GSM, UMTS, and LTE
- From their page:

*The 3rd Generation Partnership Project (3GPP) unites [Six] telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC), known as "Organizational Partners" and provides their members with a stable environment to produce the highly successful Reports and Specifications that define 3GPP technologies*

- Other cellular standards exist from other distinct standards bodies such as as 3GPP2 and the WiMax Forum
  - 3GPP2 CMDA family and the now deprecated UMB

# A Note on LTE and 3GPP

- 3GPP has Technical Reports (TR) and Technical Specifications (TS)
- Cellular standards use jargon and abbreviations frequently
  - LTE, EPS, BTS, K[ASME]
  - **Nested acronyms are common**
  - GERAN = GPRS Evolution Radio Access Network
  - LTE is often referred to as Evolved Packet System (EPS) in technical situations

# Packets and Circuits

- Pre-LTE, cellular networks used circuit switching technology for voice
  - For voice, LTE uses packet switching technologies
  - VoLTE is an example(VoIP over LTE [See the nested acronym!])
- Data traffic used to be sent over nearly distinct interconnected packet switched segments
  - GSM first used GPRS, then moved to EDGE
  - UMTS used HSPA technologies including HSPA+
- LTE is completely IP based; it does not use circuits

# Cellular Standards

| Generation | 3GPP Circuit Switched | 3GPP Packet Switched | 3GPP2 | Wimax Forum |
|---|---|---|---|---|
| 2G | GSM | | cdma One | |
| 2.5G | | GPRS | | |
| 2.75G | | EDGE | | |
| 3G | UMTS | | CDMA 2000 | |
| 3.5G | | HSPA/+ | CDMA EV-DO | |
| 4G | | LTE | ~~UMB~~ | WiMAX |

# Primary Standards Docs

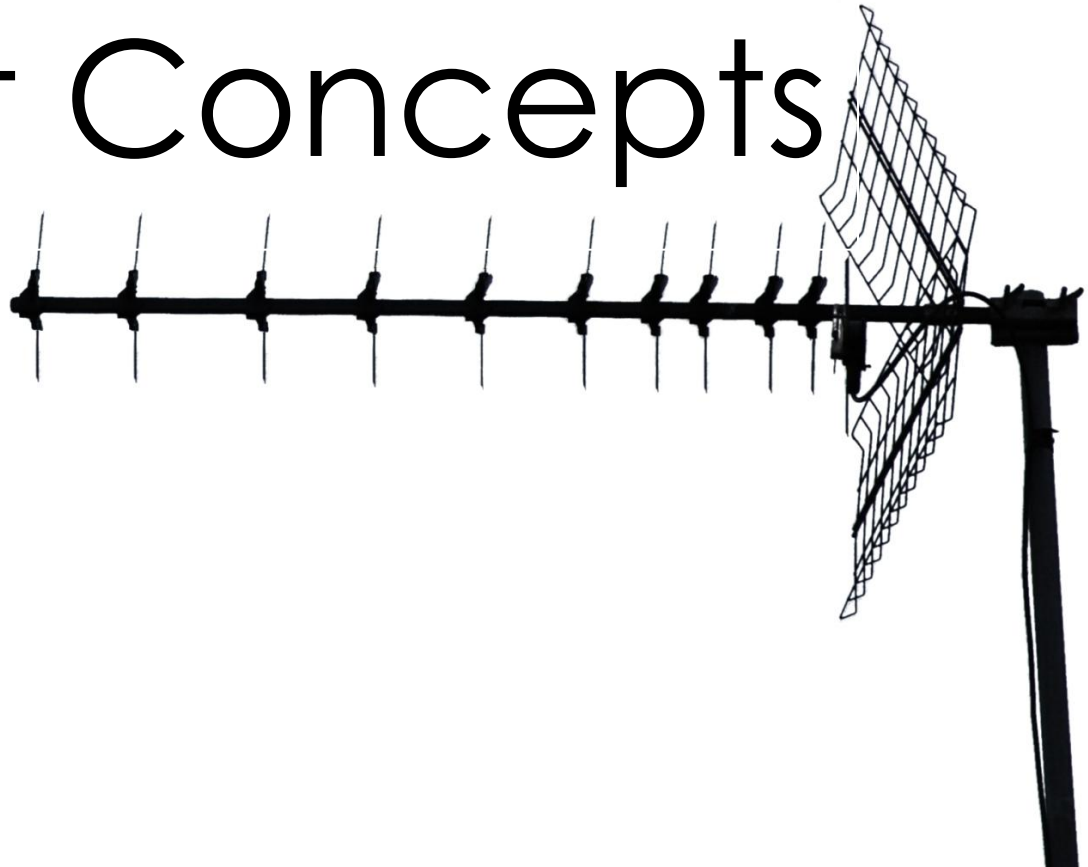
LTE standards you should be aware of:

- TS 36.300 – Overall description of E-UTRAN
- TS 33.401 – LTE Security Architecture
- TS 33.102 - 3G security; Security architecture
- TS 33.210 – Network Domain Security (NDS/IP)
- TS 35.206 – MILENAGE Algorithm
- TS 31.101 – UICC General
- TS 102.221 – UICC detailed specifications
- TS 31.102 – USIM specification

# LTE Security Architecture

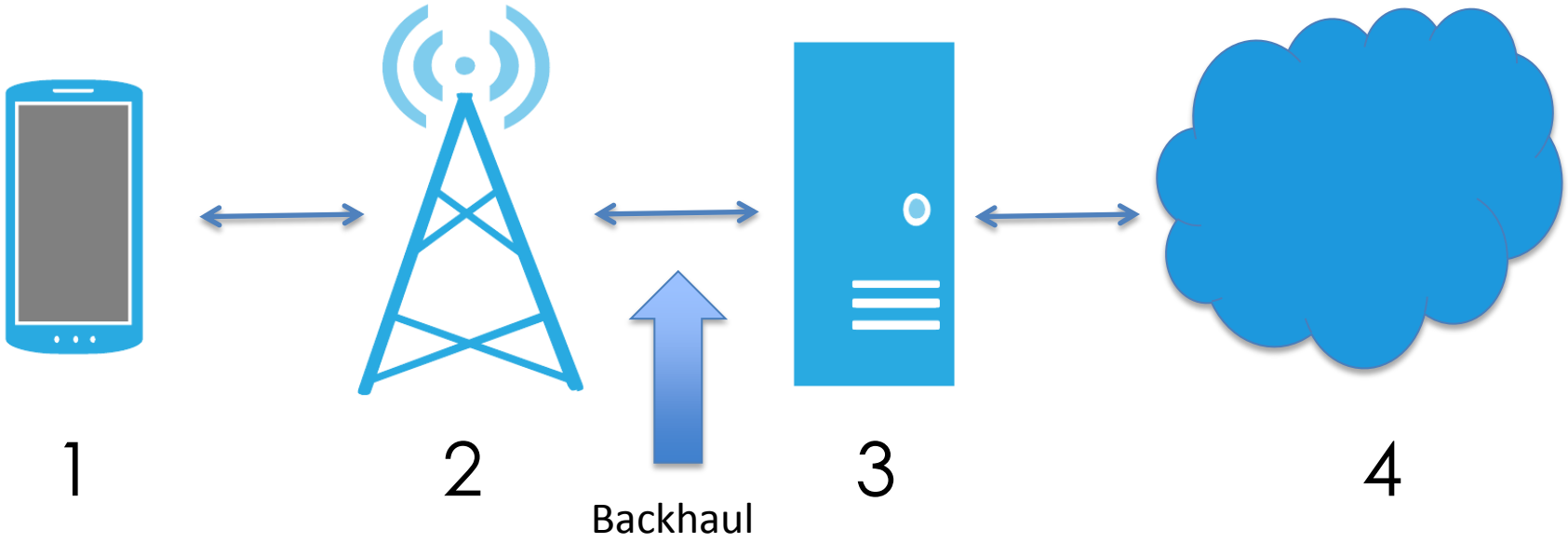
- The primary 3GPP standard governing LTE security is TS 33.401 (TS 33.401V12.10.0 2013-12)
- I link to the overarching page for the standard so the most recent version of the standard is attainable
  - Download and extract the zip for the word document

# Important Concepts



# Big Picture

Mobile devices (1) connect to a base station (2) which connects to a core network (3), which connects to the internet (4).



# Network Components

- The network between mobile devices and base stations is the Radio Access Network (RAN)
  - This name slightly changes with new standards such as GERAN, EUTRAN
- Base stations are permanent cellular sites housing antennas
- Base stations and the core network are run by telco, but there are interconnections and shared sites
  - AT&T customers need to be able to contact Verizon (vice versa)
- Base stations often connect to core via wired technologies (i.e., fiber)
  - Base stations often communicate with each other wirelessly

# Mobile Devices

- These are the devices with wireless radios that connect to cell towers
  - Radios are inside phones, tablets, laptops, etc. . .
- In LTE parlance, mobile device = User Equipment (UE)
- The parts of the UE we are concerned with today:
  - UICC and USIM (Universal SIM)
  - The UE sans USIM referred to as the ME (Mobile Equipment)

# Subscriber Identity

- LTE uses a unique ID for every subscriber
  - International Mobile Subscriber Identity (IMSI)
  - 15 digit number stored on the SIM
- Consists of 3 values: MCC, MNC, and MSIN
  - Possibly a software version (SV) appended (IMSI-SV)
- Temporary identities exist for authentication
  - Temporary Mobile Subscriber Identity (TMSI)
  - Globally Unique UE Identity (GUTI)
- This information is stored on the SIM/USIM
- Subscriber ID is distinct from the Mobile Subscriber ISDN Number (MSISDN)
  - This is the phone number

# IMSI Example

*The IMSI is divided into 3 parts*


*The MNC may be 2 or 3 digits, depending on region. 3 is common in the USA while 2 is common in Europe.*

Thanks to Wikipedia for the sample IMSI

# UE Identity

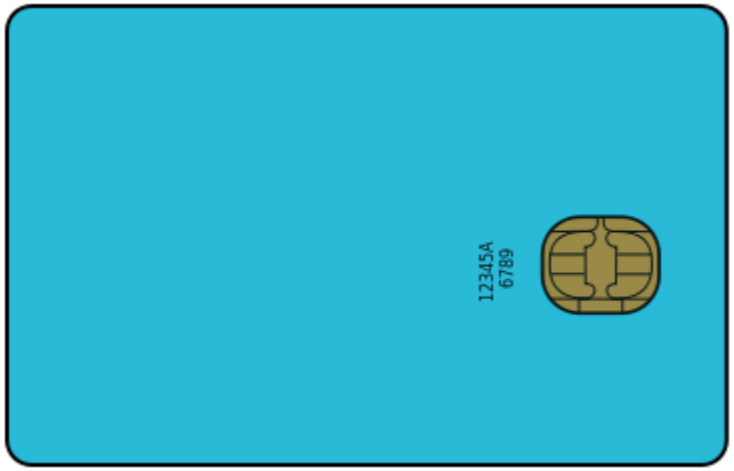
- LTE contains a unique ID for each UE
  - International Mobile Equipment Identity (IMEI)
- It is16 digits with the first 14 indicating equipment identity
  - The last 2 indicates software version (SV)
  - Referred to as IMEISV
- Dial *#06# to display your IMEI
- Used to blacklist phones from a network
- Illegal in some countries to change a phone's IMEI

# USIM Cards

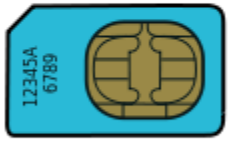
- USIMs are removable hardware tokens
  - Over 7 billion SIMs in circulation
- Stores cryptographic keys and sometimes SMSs and contacts
- Houses a processor and runs an OS
- Java Card runs atop the OS, which is a type of Java Virtual Machine (JVM) for applications
  - SIM application toolkit (STK) is used to create mobile applications
- SIMs are deprecated – the modern term is USIM
  - The USIM application runs atop the UICC (Universal Integrated Circuit Card) which is the physical card
  - Often used interchangeably

# USIM Card

Full-size SIM




Micro-SIM




Mini-SIM

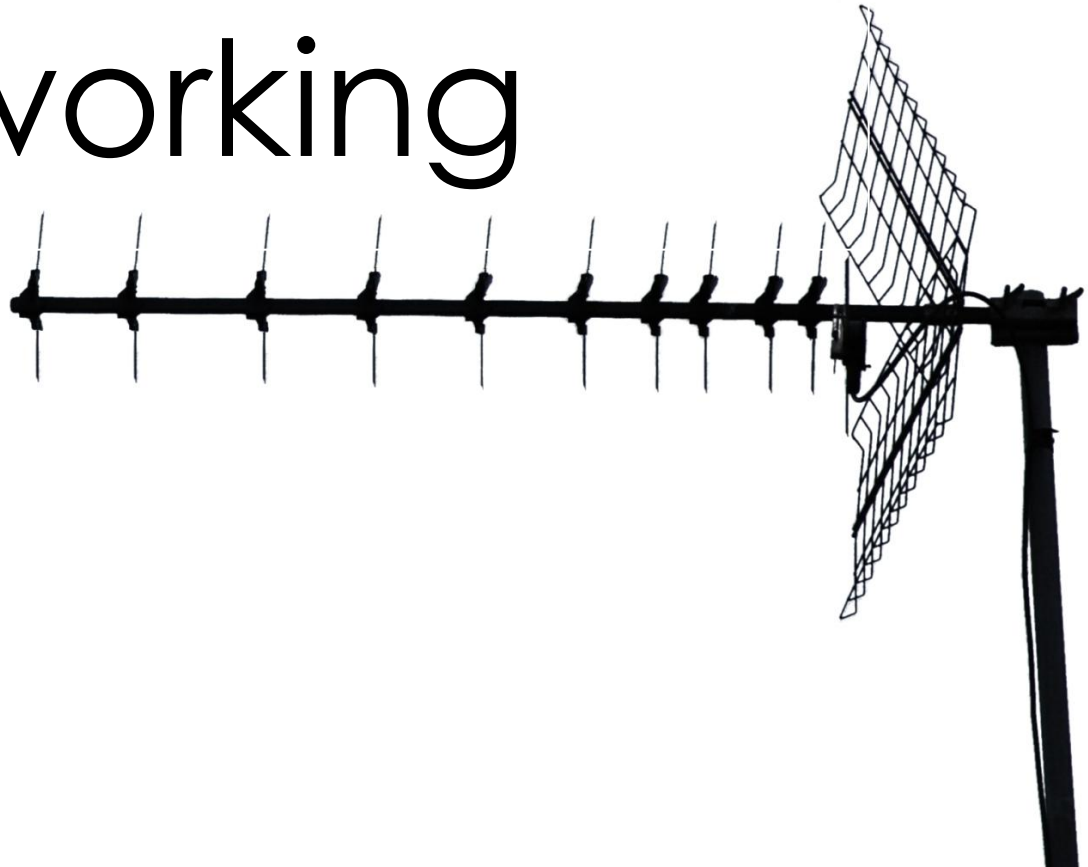
Nano-SIM

*From left to right, we are only removing plastic. The integrated circuit remains fairly static.*

Sims

Thanks to [Wikipedia]

# LTE Networking



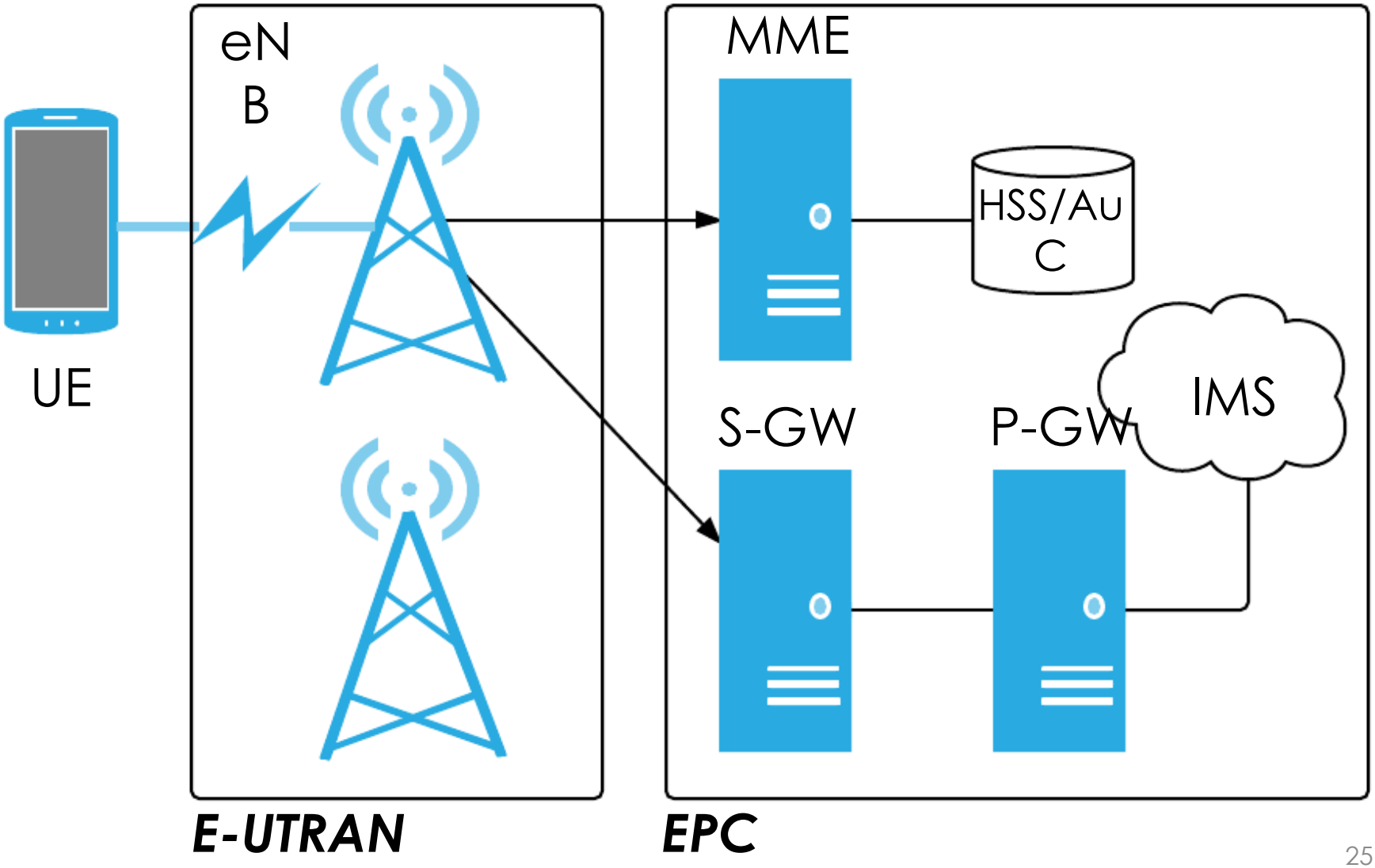
# LTE Network Intro

- **4G data and voice technology**
- 3 main components:
  - Evolved U-TRAN (E-UTRAN) - Radio Network
  - Evolved Packet Core (EPC) – Core Network
  - IP Multimedia Subsystem (IMS) - Extended core functionality
- The following is primarily focusing on the interactions between a UE and an eNB

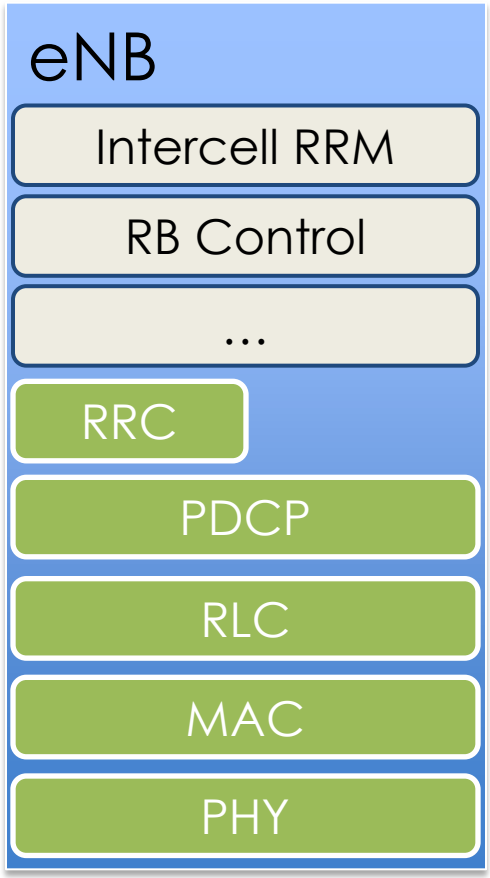
# Component Descriptions

- **User equipment (UE)** – The LTE device
- **Evolved Node B (eNodeB or eNB)** – An evolved Node B (aka base station)
- **Mobility Management Entity (MME)** – Primary signaling node (no user traffic). Large variation in functionality including managing/storing UE contexts, creating temporary IDs, sending pages, controlling authentication functions, and selecting the S-GW and P-GWs
- **Serving Gateway (S-GW)**- Carries user plane data, anchors UEs for intra-eNB handoffs, and routes information between the P-GW and the E-UTRAN
- **Packet Data Network Gateway (P-GW)** – Allocates IP addresses, routes packets, and interconnects with non 3GPP networks
- **Home Subscriber Server (HSS)** - This is the master database with the subscriber data
- **Authentication Center (AuC)** - Resides within the HSS, maps an IMSI to K, performs cryptographic calculations during AKA
- **IP Multimedia Subsystem (IMS)** – Paging, connections to the PSTN, and other functions.

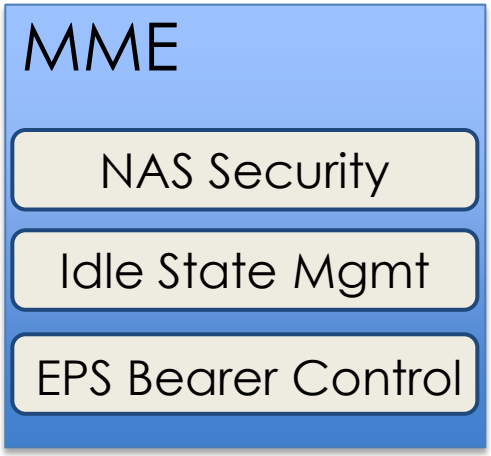
# LTE/EPS Architecture Diagram

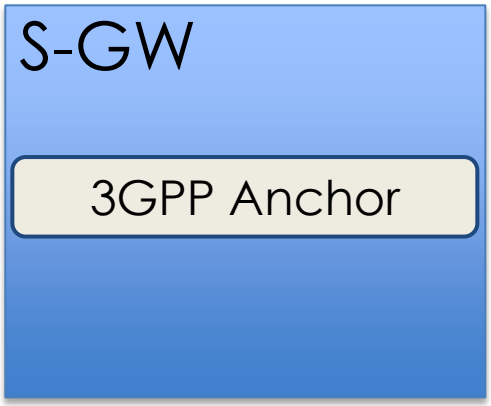


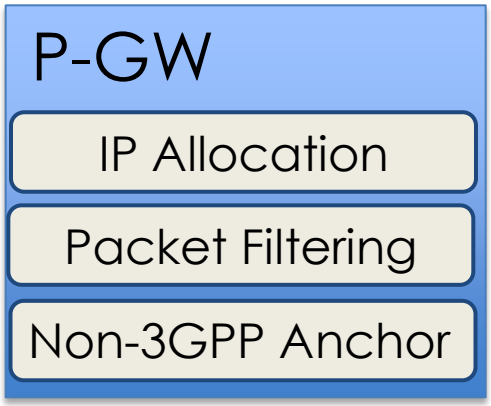
# E-UTRAN & EPC Protocols




*E-UTRAN*



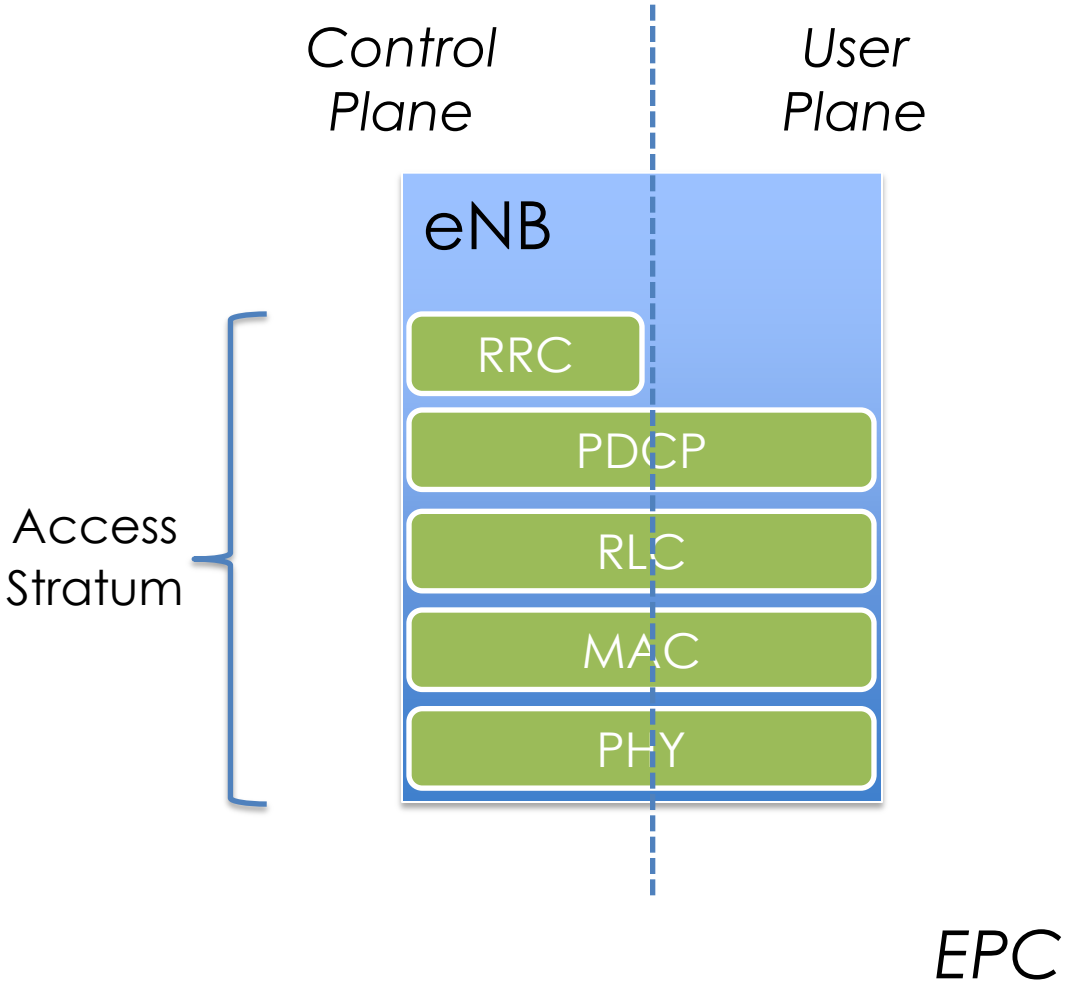




*EPC*

*Green boxes depict the radio protocol layers. White boxes depict the functional entities of the control plane*

Adapted from 3GPP TS 36.300

# LTE Communication Planes

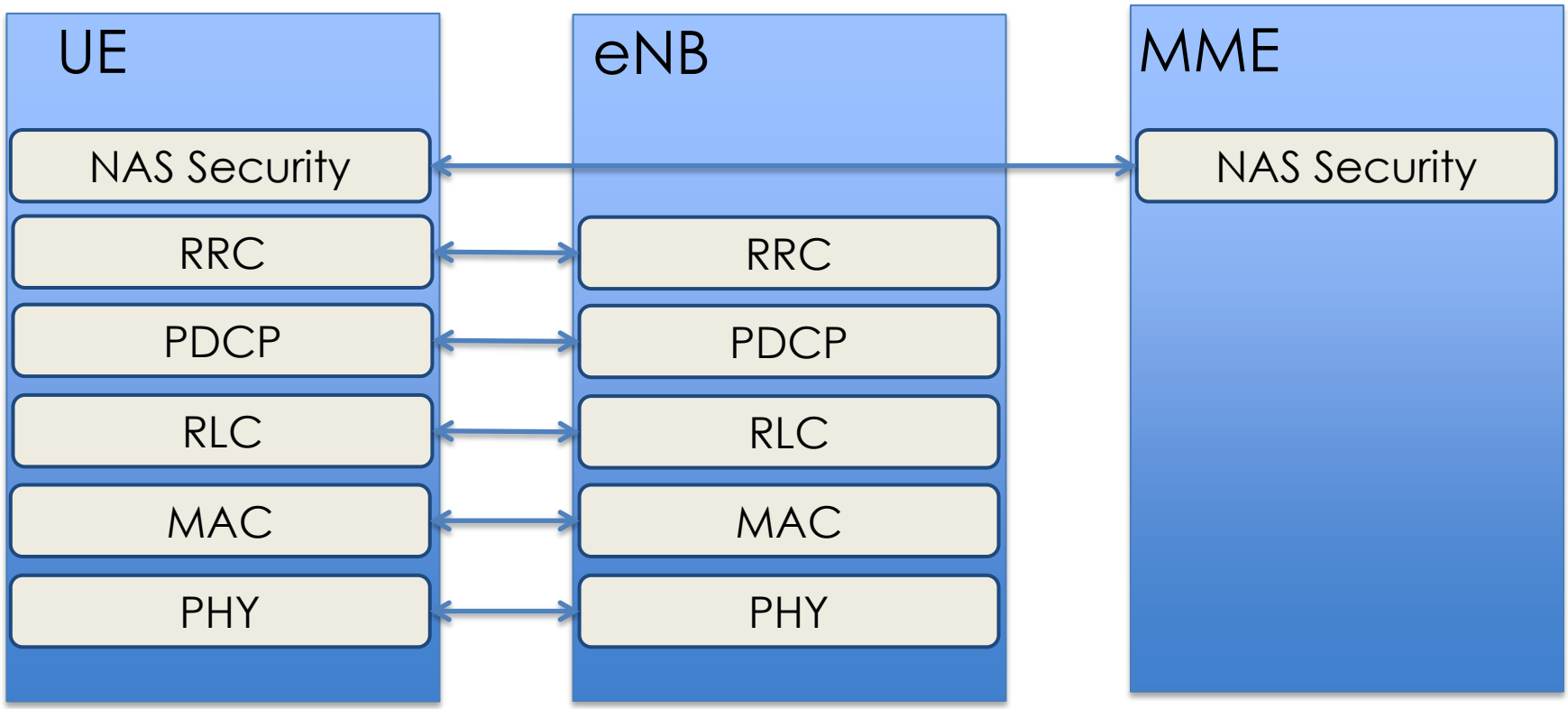



Adapted from 3GPP TS 36.300

# Protocol Discussion

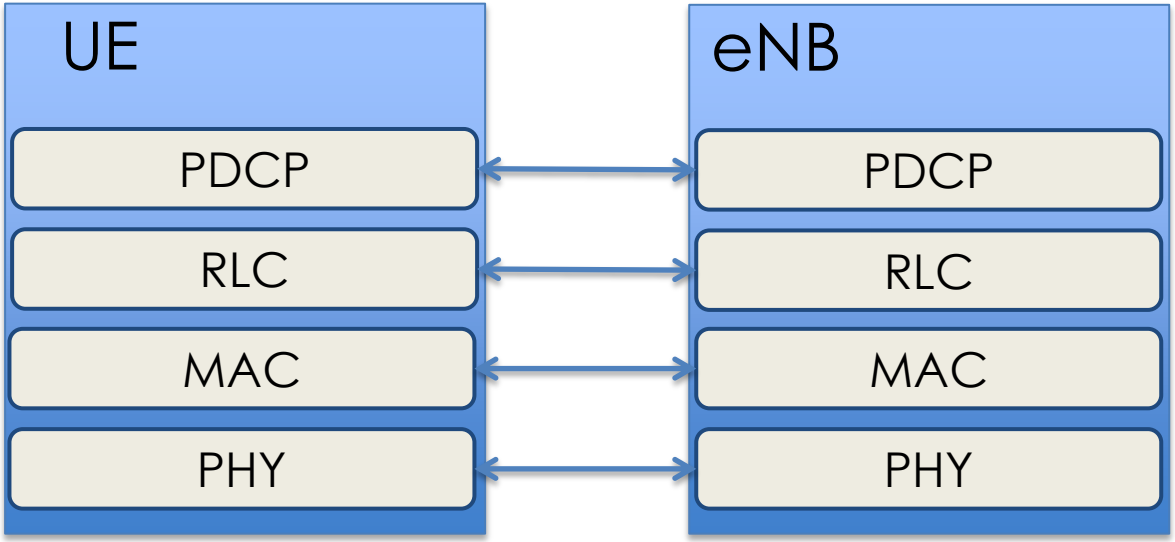
- There are a number of additional capabilities provided by the eNB
  - IP header compression of user data stream
  - Selection of an MME at UE attachment when no routing to an MME can be determined from the information provided by the UE
  - Routing of User Plane data towards Serving Gateway
- **Radio Resource Control (RRC)** – Transfers NAS messages, AS information may be included, signaling, and ECM
- **Packet Data Convergence Protocol (PDCP)** – header compression, radio encryption
- **Radio Link Control (RLC)** – Readies packets to be transferred over the air interface
- **Medium Access Control (MAC)** – Multiplexing, QoS

# CP Protocols




Adapted from 3GPP TS 36.300

# UP Protocols

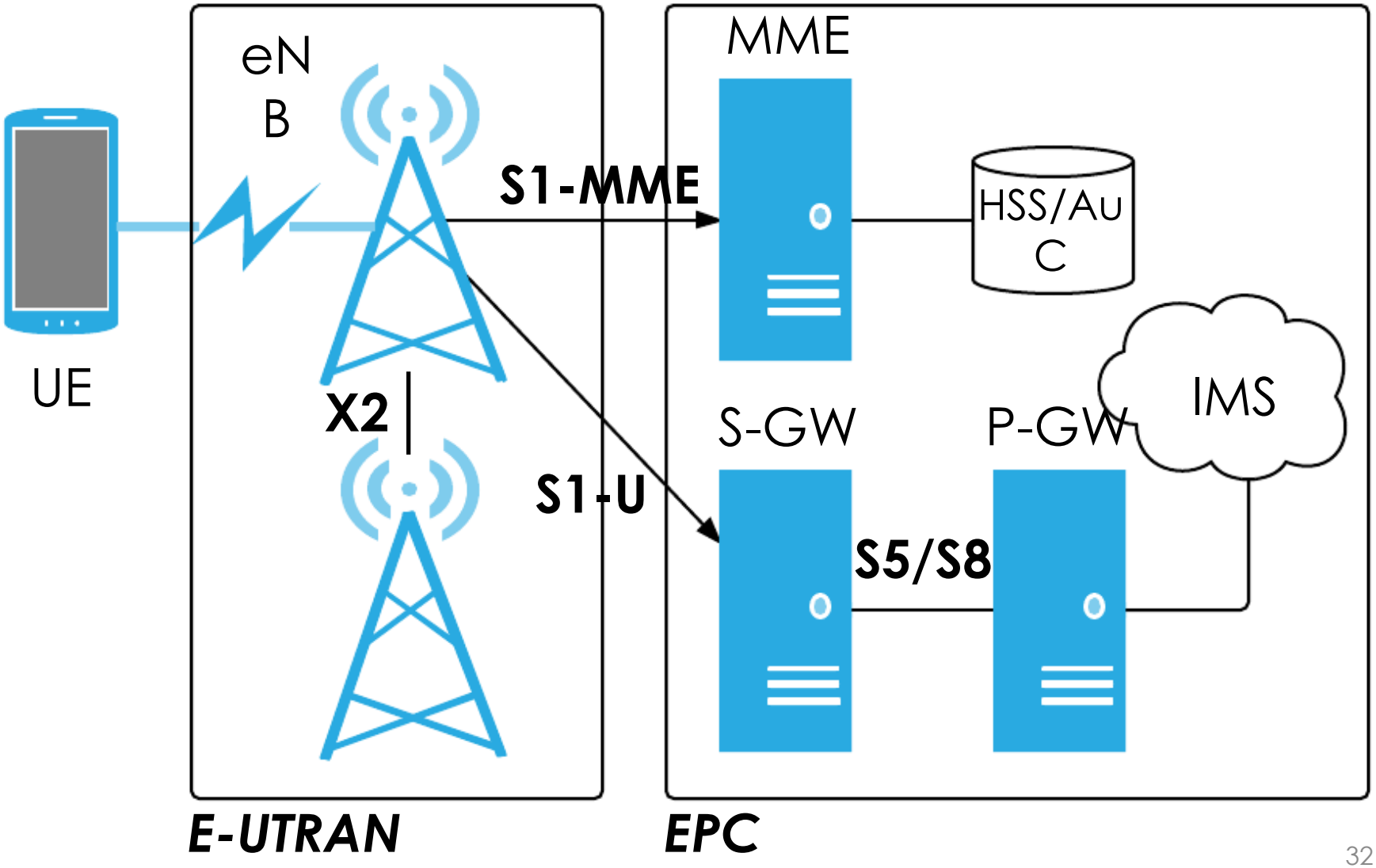



Adapted from 3GPP TS 36.300

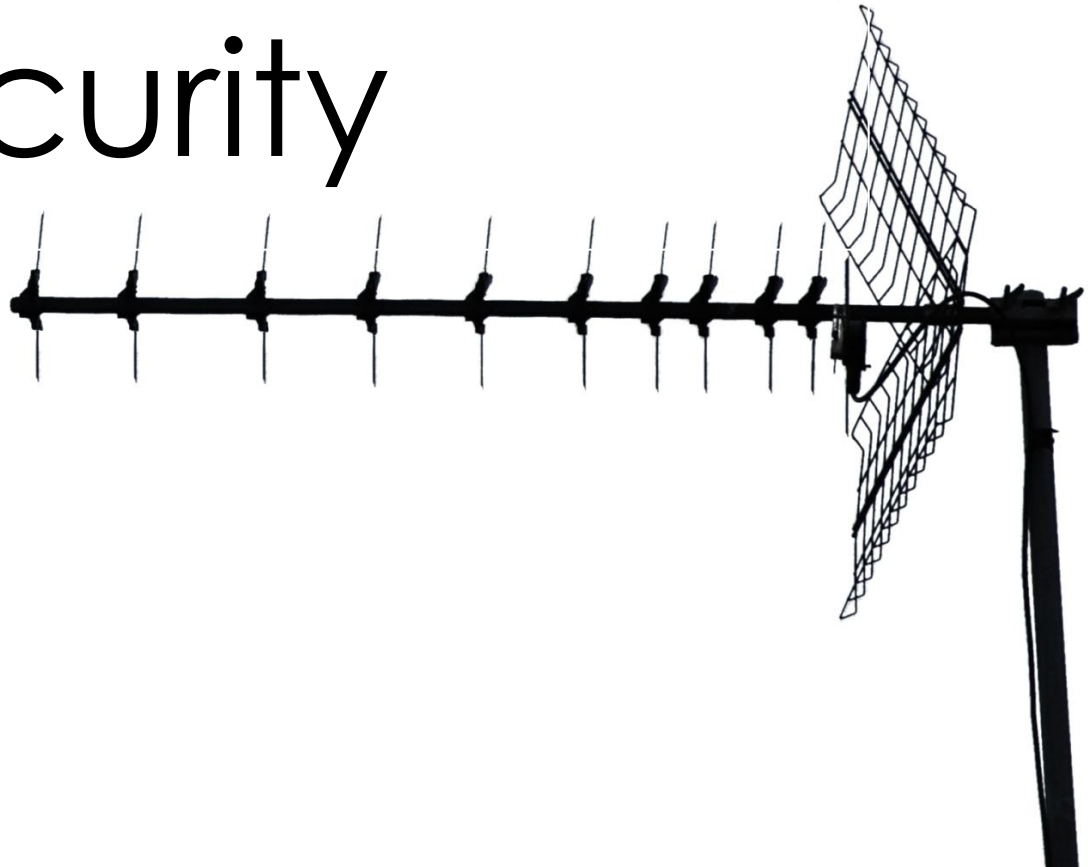
# Interfaces

- Interfaces are the communications paths LTE components use to communicate
- Each one is provided with its own label
  - There may be unique protocols between various interfaces
- There are many interfaces - we are discussing a subset
  - X2 - eNB to eNB
  - S1-U - eNB to S-GW
  - S1-MME (sometimes S1-C) - eNB to MME
  - S5/S8 - S-GW to P-GW

# LTE/EPS Interface Diagram



# LTE Security



# LTE Security Mechanisms

- USIM hardware token
- Subscriber and network authentication via Authentication and Key Agreement (AKA)
- Cryptography
  - Algorithms
  - Key hierarchy
  - Protected Interfaces
  - Independent Domains
    - Non-access Stratum (NAS)
    - Access Stratum (AS)

# High-Level Threats to LTE

- Tracking identity or devices (privacy)
- Physical attacks on base stations or network equipment
- Manipulating control plane or user plane data
- Threats related to interaction between base stations, or dropping to older standards or other networks
- Jamming handsets or network equipment or other attacks on availability
  - *Jamming attacks are not within the threat model of LTE*

# Low-Level Threats

- The communication medium(air interface) is open and accessible by all
  - Vulnerable to confidentiality (sniffing) and availability (jamming) attacks
- SIM cloning
  - Copying a phone's unique information to steal another customer's service (not as common today)
- Threats to privacy
  - By design cellular networks must quickly locate a device's location all times
- Battery life
  - Pay phones don't need to be charged once a day
- Modern mobile network operators have a large and complex public facing TCP/IP-based network to defend

# Hardware Token

- The physical USIM/UICC is identical in UMTS
  - Points to the same standard
- LTE uses a new hardware protected 128-bit key: K
  - Keys are derived from K as needed
  - K never moves from UICC and HSS/AuC

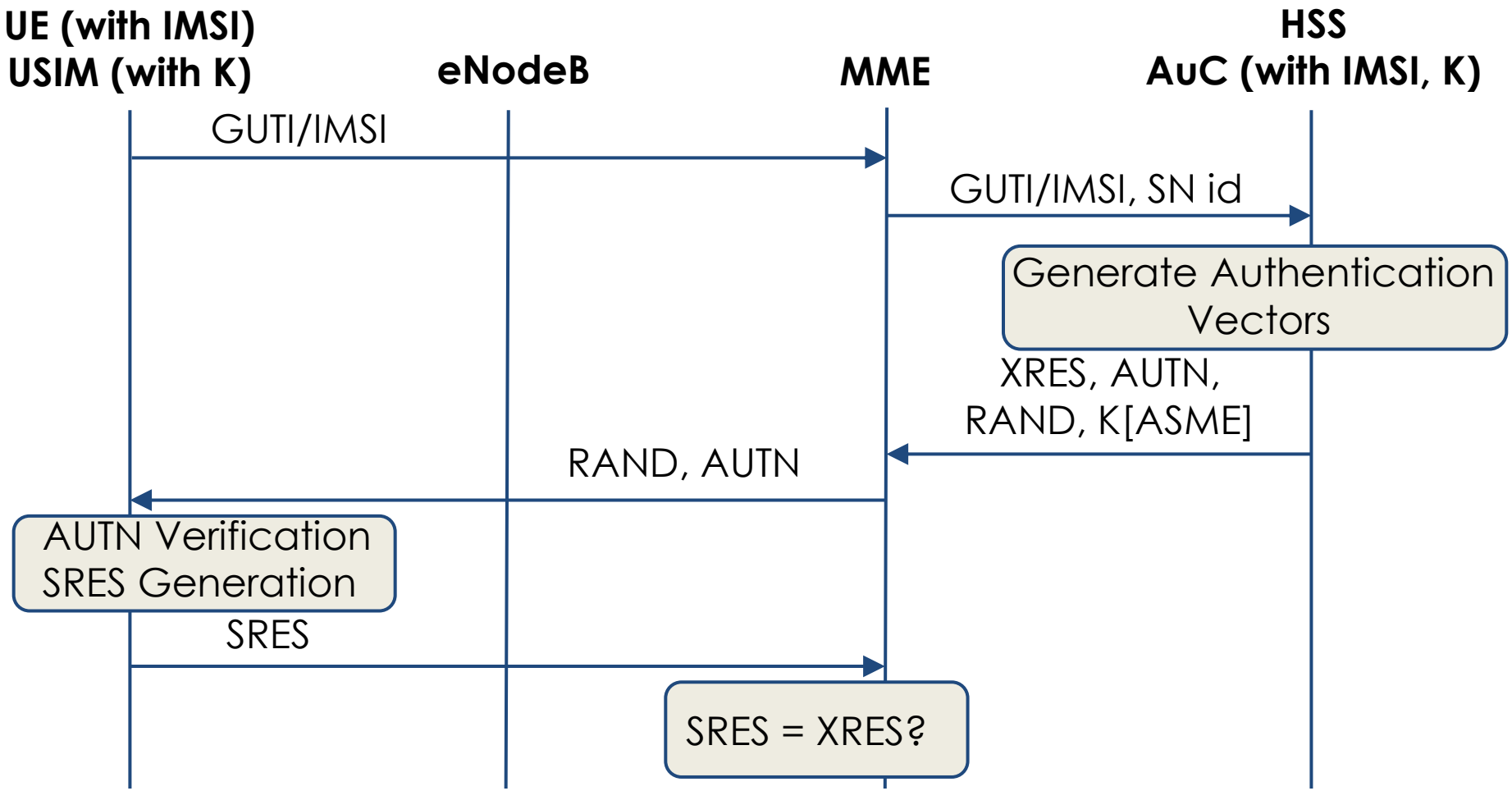
# LTE AKA Discussion

- Authentication and Key Agreement (AKA)
- UMTS AKA and LTE AKA are extremely similar
  - Originally specified in TS 33.102
  - The LTE security standard doesn't even fully describe it (TS 33.401)
- The big update for LTE AKA?
  - network separation
- This prevents a breach on one telco's network to spill into another's
  - Network identity is bound to certain keys
- LTE AKA directly authenticates network identity
  - Mutual authentication

# AVs Generation

- Authentication Vectors (AVs) are a main AKA concept
  - Requested by the MME and generated by HSS/AuC
- **LTE AV = (XRES || AUTN || RAND || K[ASME])**
- AK = Anonymity key
- AUTN = (SQN xor AK || AMF || MAC)
  - MAC = Message authenticate code in this instance
- AMF = Authentication Management Field
- CK = Cipher key
- IK = Integrity key
- KDF = Key derivation function
- MAC = A message authentication function
- SQN = Sequence Number
- XRES = Expected response
- SRES = Signed response

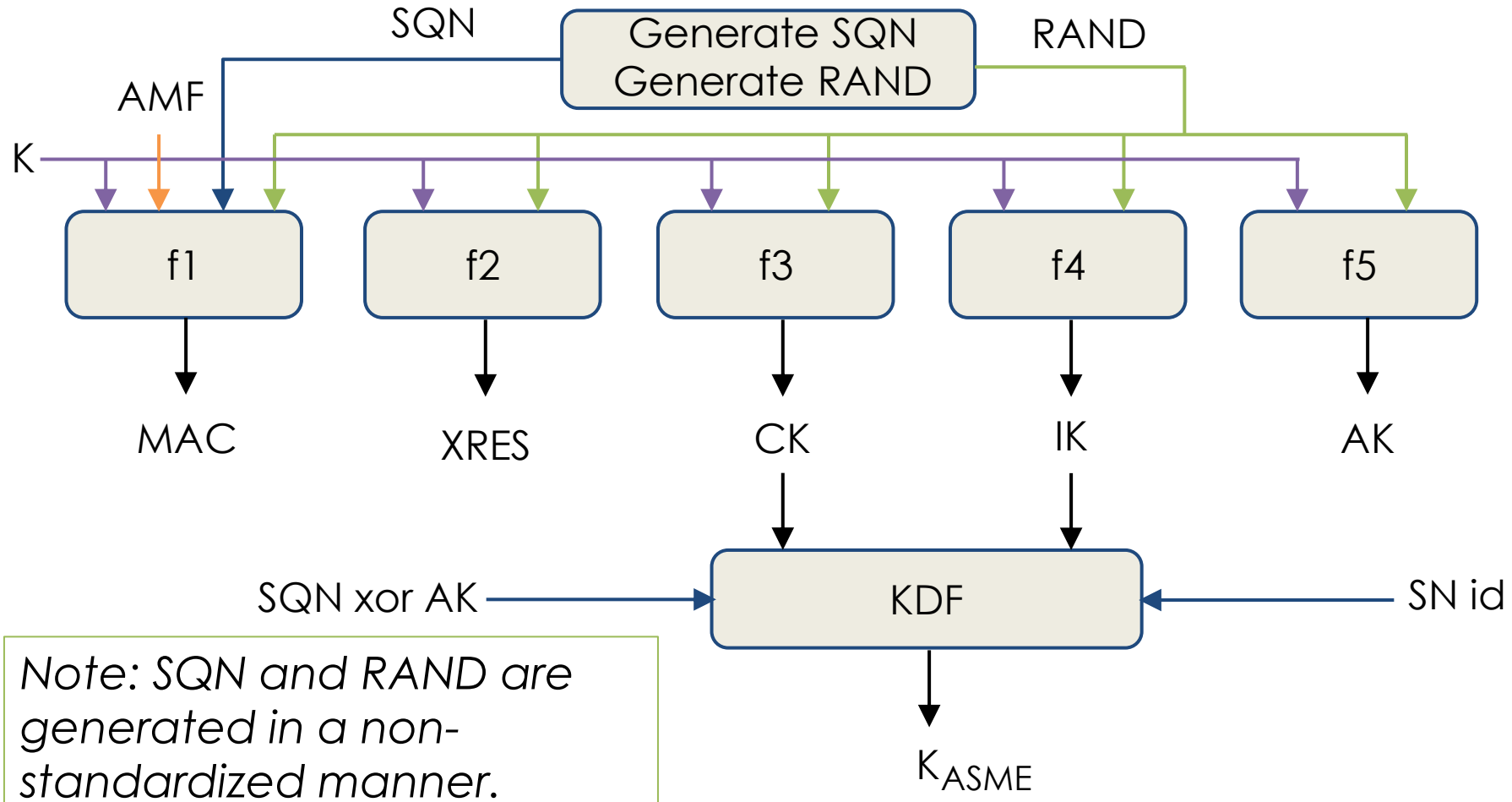
# LTE AKA Ladder Diagram




GUTI = Globally Unique Temporary Identity

Adatpted from 3GPP TS 33.102

# AVs Generation Diagram



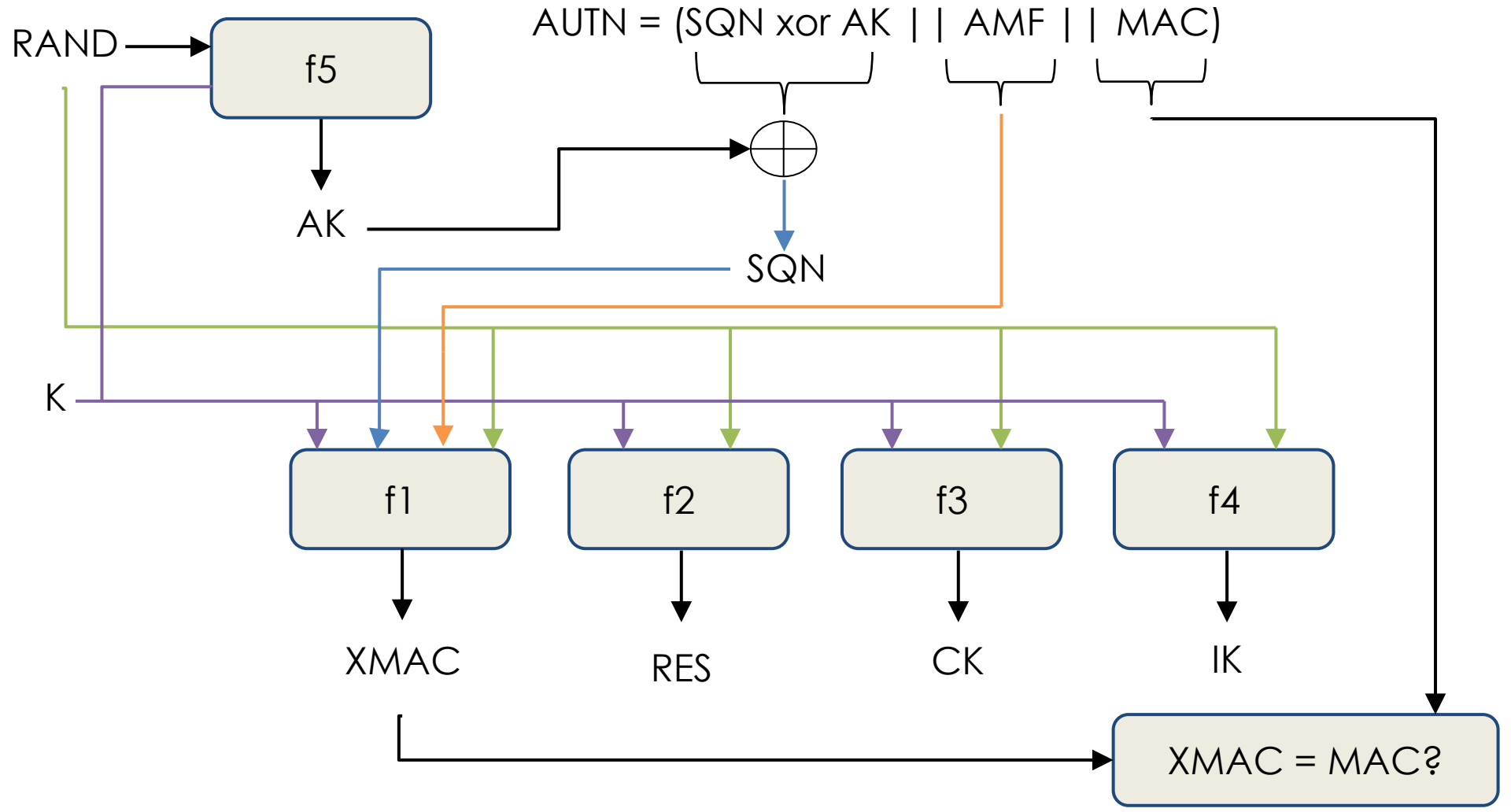

*Note: SQN and RAND are generated in a non-standardized manner.*

Adatpted from [3GPP TS 33.401]

# USIM Verification

- To verify the AVs in the USIM, the authentication process is reversed
- A standardized algorithm called MILENAGE may be used
  - Voluntary: telcos can roll their own
- If XMAC != MAC then an authentication failure occurs
  - There is a distinct process for this

# USIM Verification Diagram




Adatpted from [3GPP TS 33.401]

# LTE Crypto Algorithms

- New algorithms and cryptographic key structure
  - Introduced a new set of intermediate keys
  - Unique keys for each connection/bearer - large complicated hierarchy
- 3 sets of algorithms for confidentiality and integrity
  - EEA1/EIA1 - based on SNOW 3G
    - Similar to UMTS
  - EEA2/EIA2 - AES CTR and AES-CBC-MAC (USA)
  - EEA3/EIA3 - based on ZUC (China)
- CP and UP may use different algorithms
- Most keys in LTE are 256-bits long, but in many cases only the 128 least significant bits are used
  - Upgrade to 256-bit keys underway

# Standardized Algorithms

**33.401 – 5.1.3.2**
Currently, the following values have been defined:

- "$0000_2$" EIA0 Null Integrity Protection algorithm
- "$0001_2$" 128-EEA1 SNOW 3G based algorithm
- "$0010_2$" 128-EEA2 AES based algorithm
- "$0011_2$" 128-EEA3 ZUC based algorithm

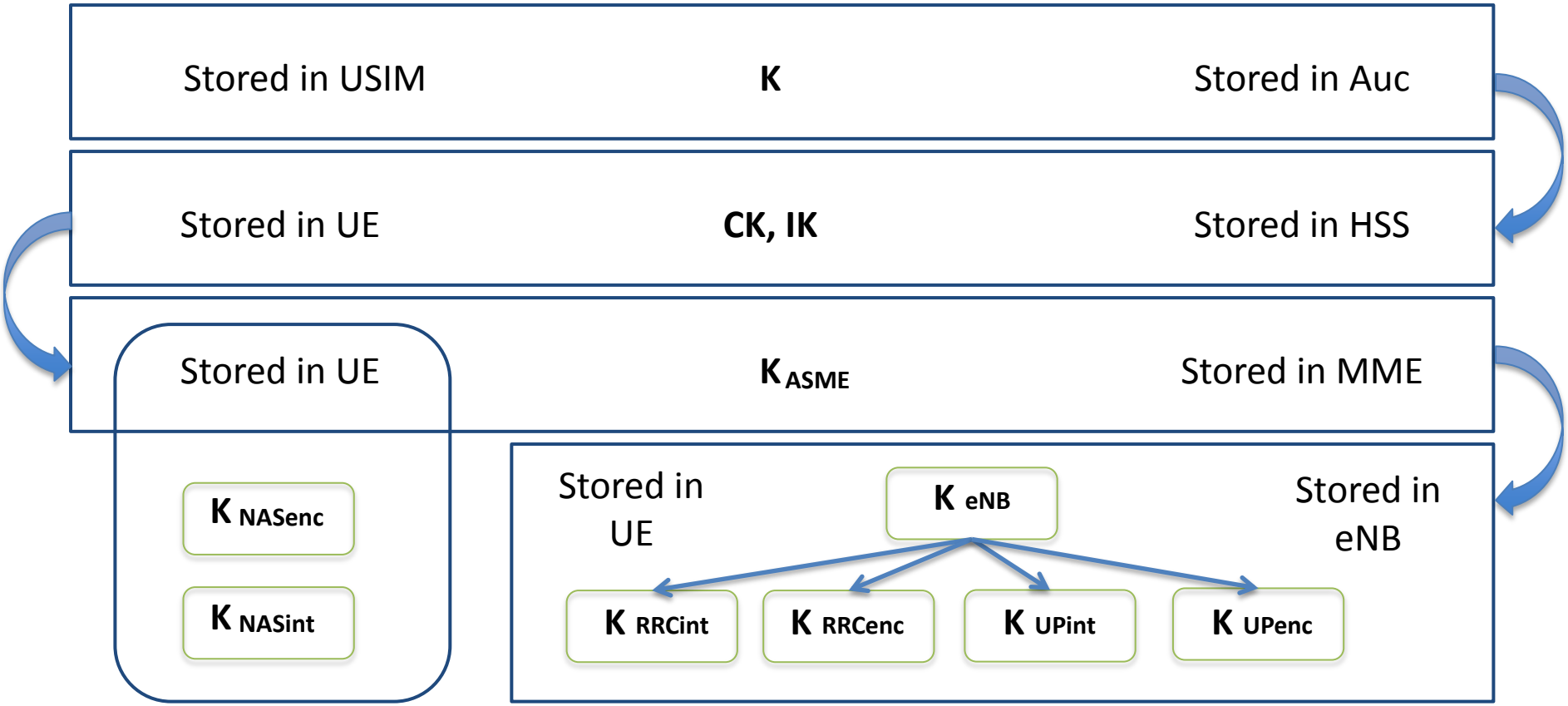
UEs and eNBs shall implement EEA0, 128-EEA1 and 128-EEA2 for both RRC signalling ciphering and UP ciphering. **UEs and eNBs may implement 128-EEA3** for both RRC signalling ciphering and UP ciphering.

UEs and MMEs shall implement EEA0, 128-EEA1 and 128-EEA2 for NAS signalling ciphering. **UEs and MMEs may implement 128-EEA3** for NAS signalling ciphering.

# Key Discussion

- K – The master key. Permanent pre-shared key stored in hardware. Located on USIM and HSS/AuC.
- CK and IK – Cipher key and Integrity key.
- K[ASME] – Local master. The serving network ID (SN id) is used to derive this key in addition to CK and IK.
- K[eNB] – Used to derive additional keys used in handoff.
- K[eNB*] – Intermediate eNB handover key.
- NH – Next Hop. Intermediate key used to provide forward secrecy.
- K[NASenc] & K[NASint]- Protection of NAS traffic.
- K[RRCenc] & K[RRCint] - Protection of RRC traffic.
- K[UPenc] & K[UPint] - Protection of UP traffic.

# Key Hierarchy




Adatpted from 3GPP TS 33.401

# Key Discussion

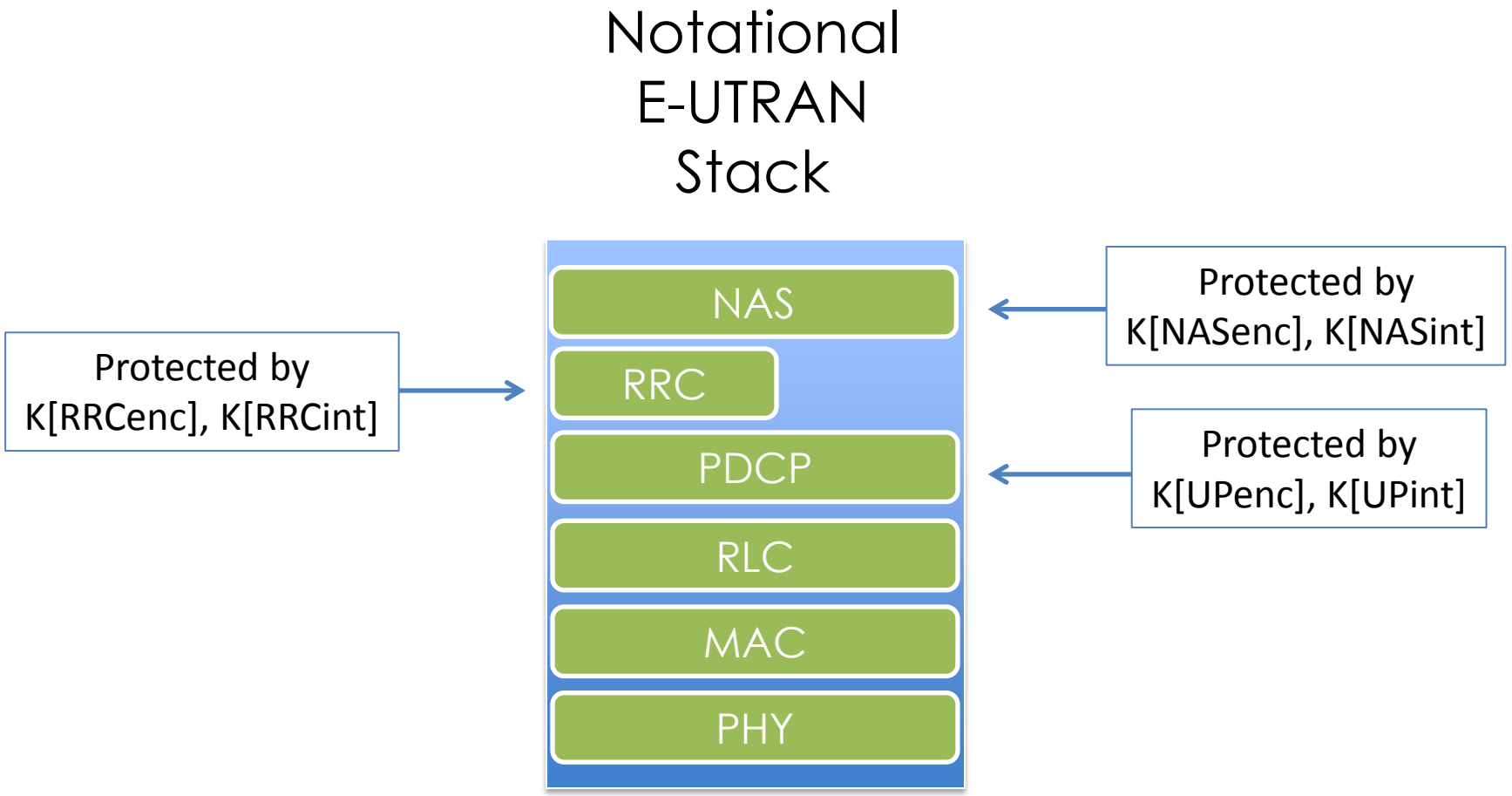
| Key | Name | Length | Derived From |
|---|---|---|---|
| K | Master Key | 128 | ----- |
| CK, IK | Cipher Key, Integrity Key | 128 | K |
| K[ASME] | MME Base Key | 256 | CK, IK |
| K[eNB*] | eNB Handover Key | 256 | K[ASME], K[eNB*] |
| K[eNB] | eNB Base Key | 256 | NH, K[eNB] |
| NH | Next Hop | 256 | K[eNB] |
| K[NASenc/NASint] | NAS cipher and integrity keys | 128 / 256 | K[ASME] |
| K[RRCenc/RRCint] | RRC cipher and integrity keys | 128 / 256 | K[eNB] |
| K[UPenc/UPint] | UP cipher and integrity keys | 128 / 256 | K[eNB] |

Adapted from Agilent Security in the LTE-SAE Network

# Signaling Protection

- Network components create protected channels for each device it communicates with, for example:
  - UE and eNB communicate with a unique key
  - UE and MME communicate with a unique key
  - eNB and S-GW communicate with a unique key
- NAS security is always setup if a UE is registered to the network
- AS security is setup as needed
- A common claim is that LTE is "fully encrypted"
  - Initial radio access and signaling is not, but no data is being transmitted at that point

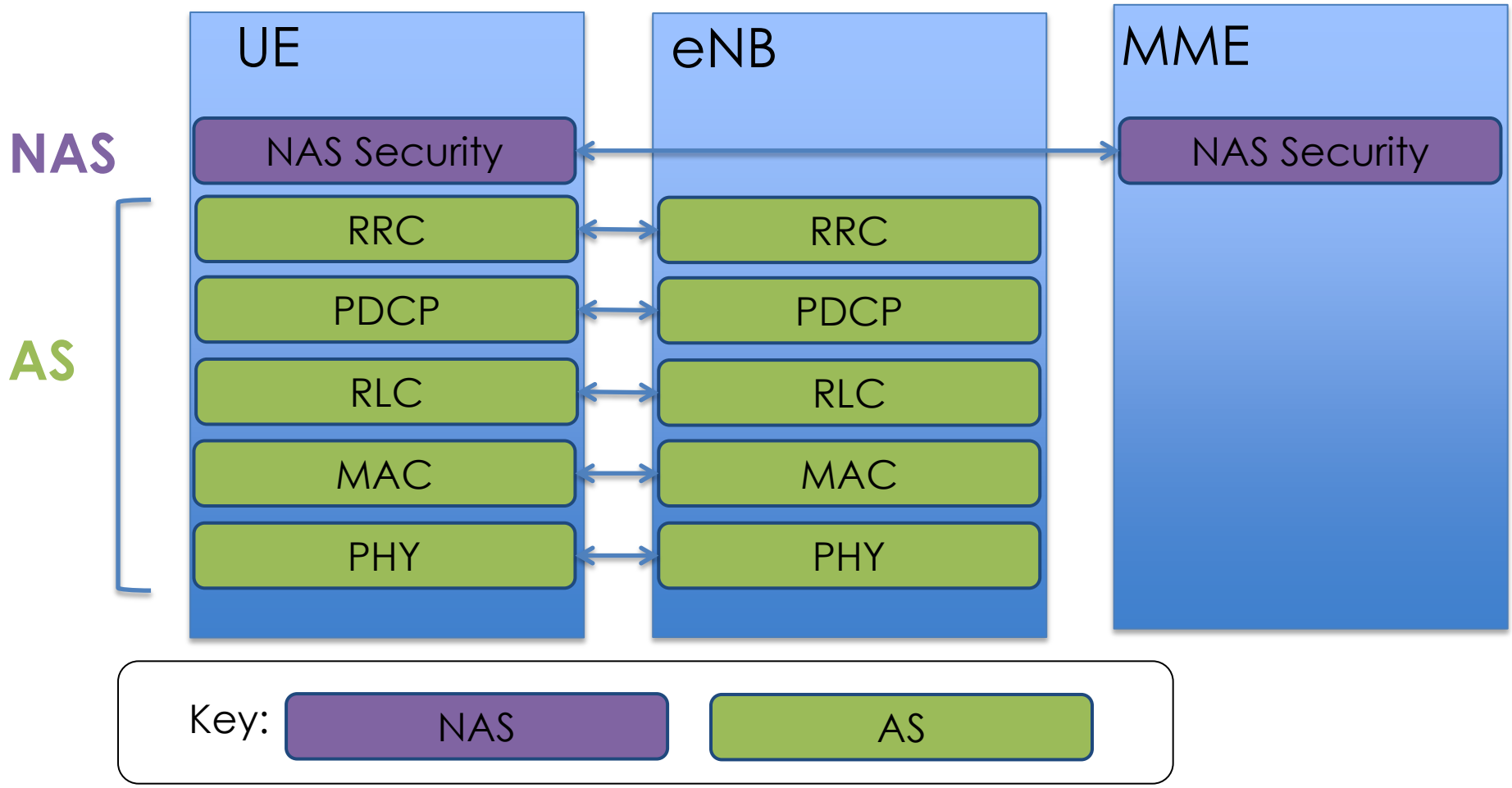
# Signaling Protection in Action



# Non-Access Stratum (NAS)

- Signaling between UE and the core (MME)
  - NAS independently applies integrity protection and ciphering to core network signaling
  - MME contains a list of confidentiality and integrity algorithms in a prioritized order
- Negotiation begins when an MME sends an integrity protected Security Mode Command to UE
  - Contains evolved key set identifier (eKSI), list of security capabilities and algorithms, IMSI request, and additional cryptographic information
- The UE responds with an integrity protected encrypted message called the NAS Security Mode Complete containing its IMEI and a MAC of the message

# NAS versus AS




Adapted from 3GPP TS 36.300

# Access Stratum (AS)

- Signaling between UE and eNB
  - Algorithm selection occurs between these components
  - eNB contains a list of confidentiality and integrity algorithms in a priority order
- AS and RRC communication occur on the Packet Data Convergence Protocol (PDCP)
- AS protection is optional (look ahead for proof)

# NDS/IP

- Network Domain Security / Internet Protocol
  - Defined by TS 33.210 and IPsec defined by IETF RFC-4301and RFC-2401
- Provides confidentiality protection, including authentication and anti-replay capabilities to traffic running over backhaul and core network
  - May not apply to user plane traffic
- Mobile network operator's network is divided into different security domains
- Hardware security appliances are used to implement this standard
  - Security Gateways (SEG)
  - Beware of the term/name collision of *Security Gateway* used for HeNBs
- SEG are placed in front of important network elements, such as the MME
  - 33.210 does not dictate where the SEG should be placed within the network (operator option)
- If interfaces are physically protected, cryptographic protection is not required.

# NAS Requirements

**33.401 – 5.1.1**

The UE shall not send IMEI or IMEISV to the network on a network request before the NAS security has been activated.

From subscriber's privacy point of view, the MSIN, the IMEI, and the IMEISV should be confidentiality protected.

The NAS signalling may be confidentiality protected. **NAS signalling confidentiality is an operator option.**

NOTE 1: RRC and NAS signalling confidentiality protection is recommended to be used.

# User Data Confidentiality

**33.401 – 5.1.3.1**

Ciphering **may** be provided to RRC-signalling to prevent UE tracking based on cell level measurement reports, handover message mapping, or cell level identity chaining. **RRC signalling confidentiality is an operator option.**

User plane confidentiality protection shall be done at PDCP layer and **is an operator option.**

**NOTE 2: User plane confidentiality protection is recommended to be used.**

# User Data Integrity

**33.401 – 5.1.4.1**

Synchronization of the input parameters for integrity protection shall be ensured for the protocols involved in the integrity protection.

**Integrity protection, and replay protection, shall be provided to NAS and RRC-signalling.**

All NAS signaling messages **except those explicitly listed in TS 24.301** [9] as exceptions shall be integrity-protected. All RRC signaling messages **except those explicitly listed in TS 36.331** [21] as exceptions shall be integrity-protected.

# MIN(confidentialityProtection)

Assuming physical protection: Encryption really isn't required

- NAS = 33.401 – 5.1.3.1
- RRC / UP = 33.401 – 5.1.3.1
- S1 – Control = 33.401 - 11
- S1-User = 33.401 – 12

# HeNB

- Home eNode Bs (HeNBs) connect to the core via a distinct Security Gateway (SeGW)
  - Tunnel is protected with Ipsec
  - Formal name for a femtocell in LTE
- IMSI-catcher is a femtocell that is configured to look like a real base station to steal IMSIs from nearby devices
  - Often used by law enforcement
  - IMSIs are important for device/subscriber tracking and call interception
- A hardware root of trust is included in modern HeNBs
  - Used to assist in secure boot and integrity checks
  - Ensures that upon boot, key firmware and other sensitive security parameters are not modified
- The status of integrity checks are communicated to the SeGW

# Lawful Interception

- Lawful interception mechanisms are built into 3GPP standards
- Call/message content and related data provided from certain network elements to the law enforcement side
- Assumes typically that the content appears in clear in the network element
- End-to-end encryption is still possible if keys are provided
- No weak algorithms introduced for LI purposes
  - All 3GPP algorithms are publicly known
- National variations exist
- Check TS 33.106, 33.107, and 33.108 more additional information

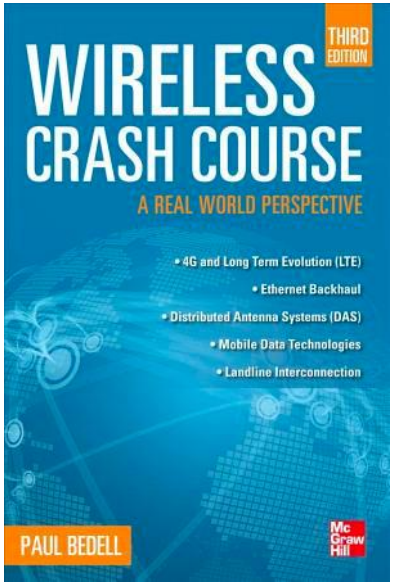
# Conclusions

- LTE security is imperfect and complicated
- In general, integrity and replay protection are mandated - not confidentiality protection
- Standards provide the bare minimum level of security that must be achieved
  - Telcos may voluntarily raise the security of their networks beyond what is required…it's hard to tell
- Thanks for having me!

Joshua Franklin
www.jfranklin.me
– @thejoshpit

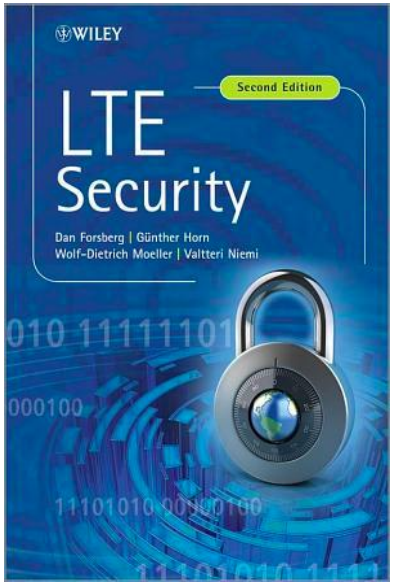
# Further Reading

**Wireless Crash Course**
**3rd edition**



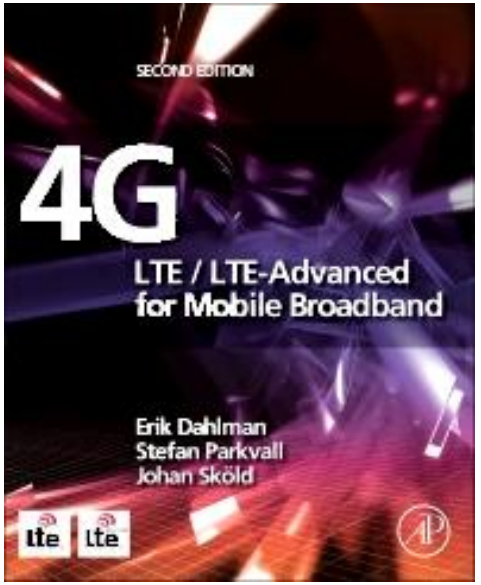

Easy Mode

**LTE Security**
**2nd edition**



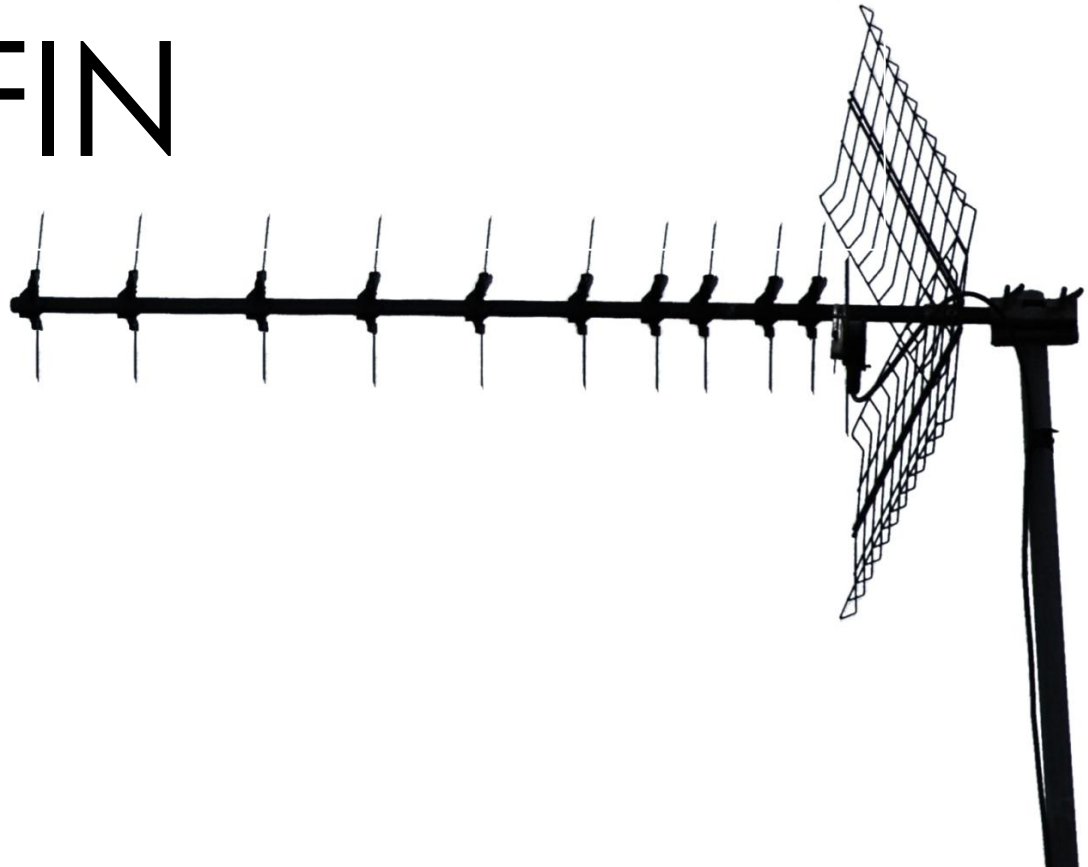

Intermediate

**LTE-Advanced for Mobile Broadband - 2nd edition**




God Mode

# FIN



# Intro to Cellular Security

- An 8 hour intro to cellular security is available at opensecuritytraining.info