Mobile Security

Network Security - Lecture 7

Ruxandra F. Olimid

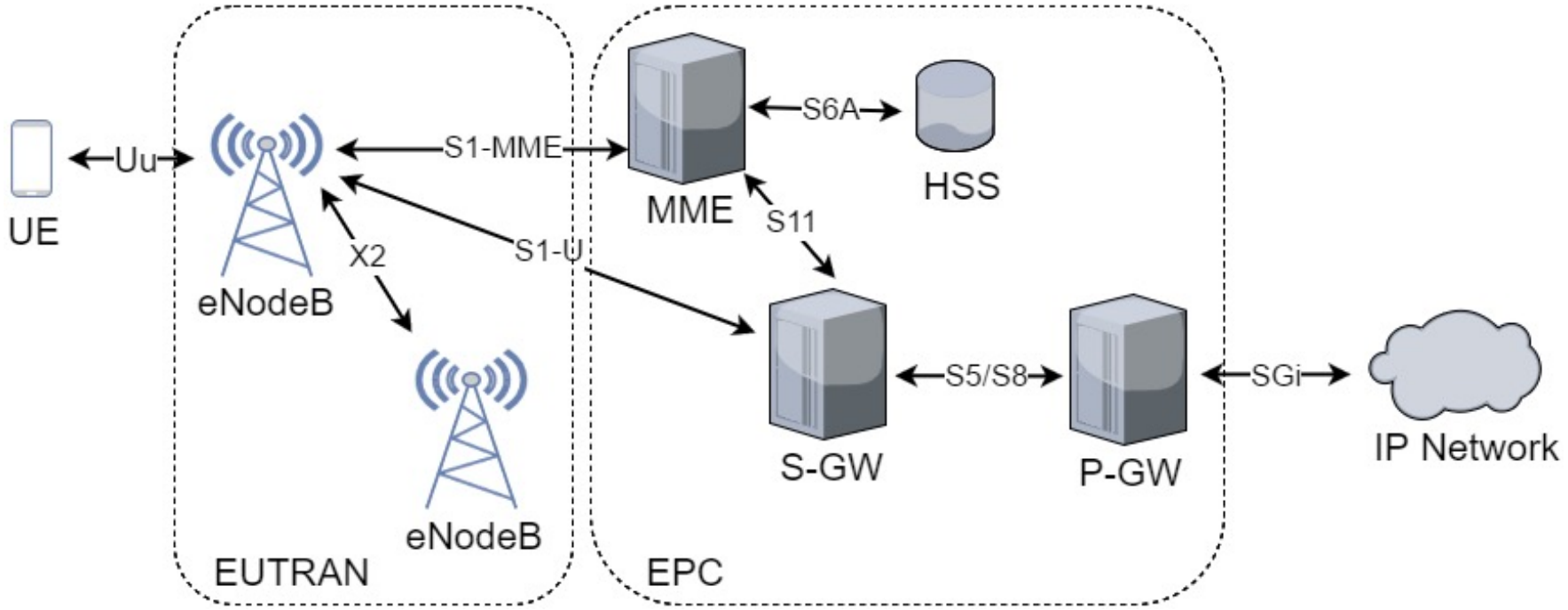
Faculty of Mathematics and Computer Science, University of Bucharest

*slides adapted from the course TTM4137 thought at NTNU

Outline

- LTE (Security) Architecture
- Security Requirements / Principles
- Vulnerabilities and Attacks

LTE - Architecture



UE: User Equipment
ME: Mobile Equipment
USIM: Universal SIM

EUTRAN: Evolved UTRAN
eNodeB: Evolved NodeB

EPC: Evolved Packet Core
MME: Mobility Management Entity
S-GW: Serving Gateway
P-GW: PDN (Packet Data Network) Gateway
HSS: Home Subscriber Server

LTE - Arhitecture

- UE (User Equipment):
  - Same as in UMTS: consists of the Mobile Equipment (ME) and the Universal Subscriber's Identity Module (USIM)
- EUTRAN (Evolved UTRAN):
  - Consists in several eNodeBs
  - A difference from UMTS is that the eNodeBs can communicate directly between themselves
- EPC (Evolved Packet Core):
  - UE is authenticated by the MME is responsible for selecting the SGSN at 2G/3G handovers, authentication and resources allocation to UEs. It manages the mobility of UEs in the network when eNodeBs cannot
  - S-GW is an interconnection point between EUTRAN and EPC, is responsible for packet routing and forwarding, buffering download packets, being a mobility anchor for inter-3GPP mobility
  - P-GW is a routing point to provide connectivity to the external PDN

Terminology

- LTE (Long Term Evolution):
  - The new radio technology
- SAE/LTE (System Architecture Evolution / LTE):
  - Stands for the entire system: LTE technology with access to previous technologies such as GSM and 3G
  - LTE includes the EUTRAN, while SAE includes the EPC
- EPS (Evolved Packet System):
  - The technical term for SAE/LTE, but the brand name of the new system has been chosen to be LTE

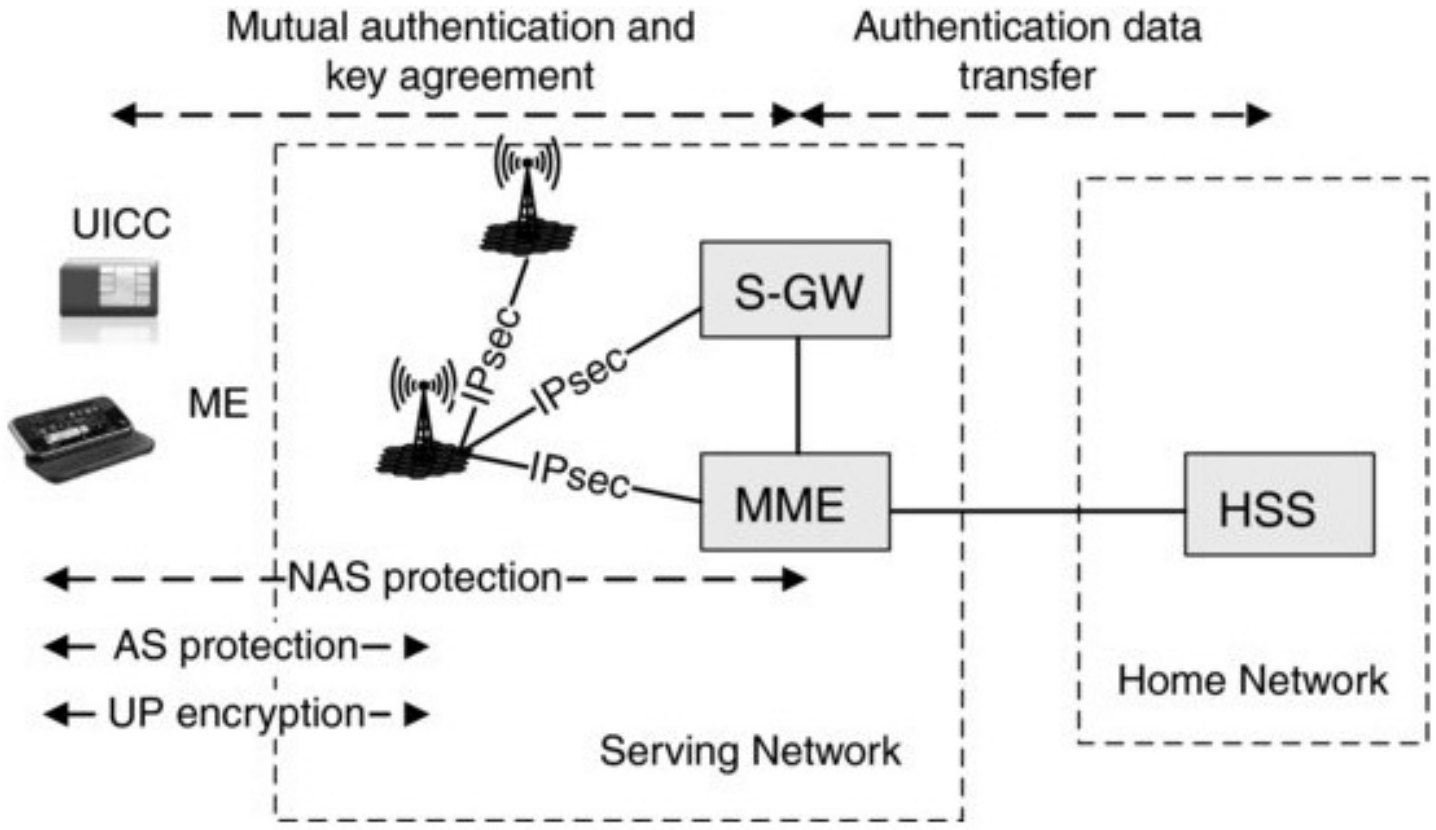
EPS Security Architecture

- GSM and UMTS security mechanisms are used as a basis, but adapted to the EPS architecture

- Protection is performed in both planes:
  - *Signalling plane*
  - *User plane*

- There exists both confidentiality and integrity protection mechanisms:
  - Confidentiality: **both signalling and user planes**
  - Integrity: **just signalling plane**

EPS Security Architecture



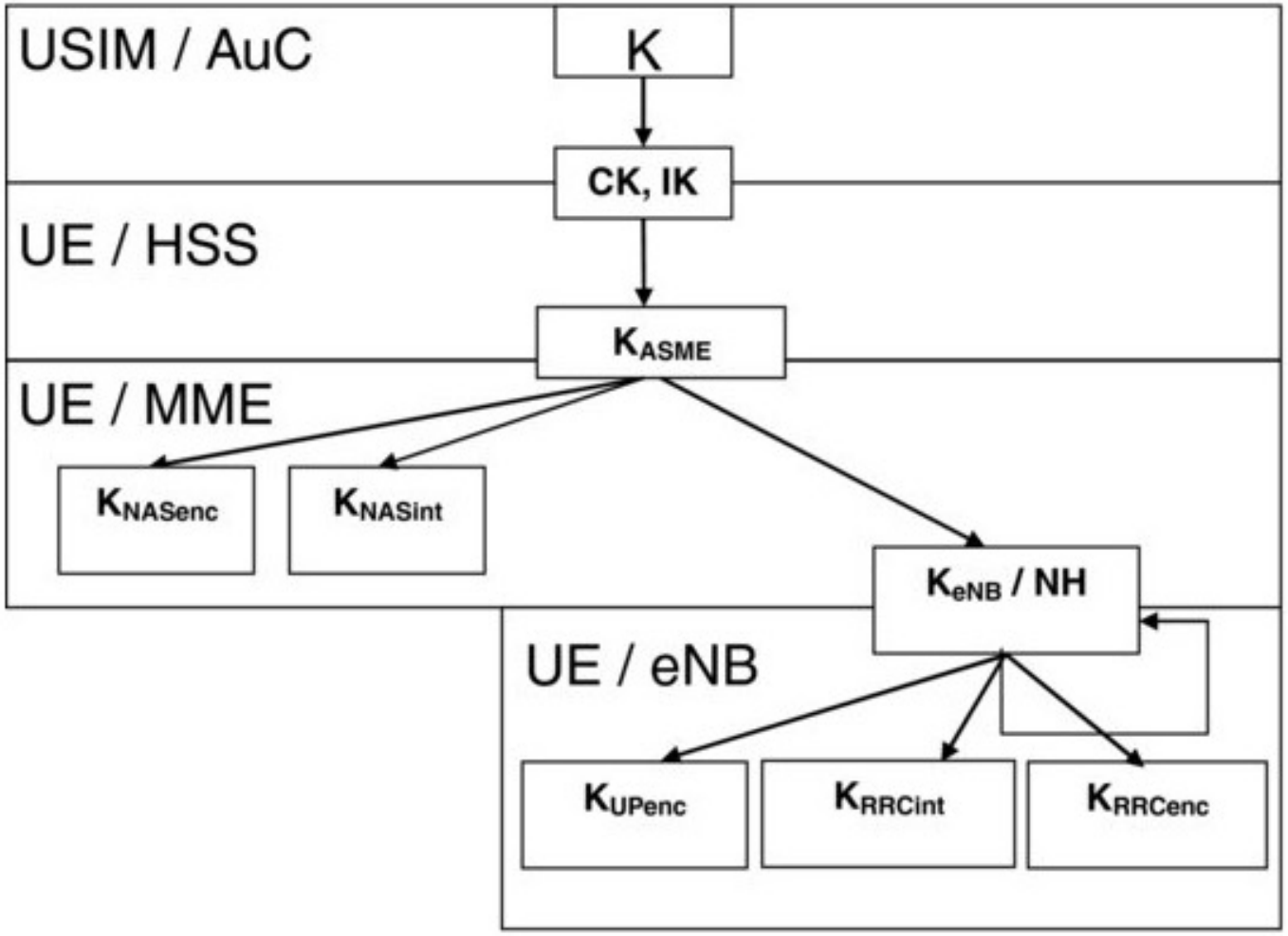
[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

NAS: Non-Access Stratum
AS: Access Stratum
UP: User Plane

EPS Security Architecture

- MME fetches authentication data from the HSS
- MME triggers the authentication and key agreement protocol with the UE, resulting a key $\mathbf{K_{ASME}}$
- 2 derived keys are used for confidentiality ($\mathbf{K_{NASenc}}$) and integrity ($\mathbf{K_{NASint}}$) protection of the signalling data between the MME and the UE - NAS protection
- One key is transported to the eNodeB ($\mathbf{K_{eNB}}$), from which 3 other keys are derived:
  - 2 derived keys are used for confidentiality ($\mathbf{K_{RRCenc}}$) and integrity ($\mathbf{K_{RRCint}}$) protection of the signalling data between the eNodeB and the UE - AS protection
  - 1 derived key ($\mathbf{K_{UPenc}}$) is used for confidentiality protection of the user plane data between the eNodeB and the UE

Key Hierarchy

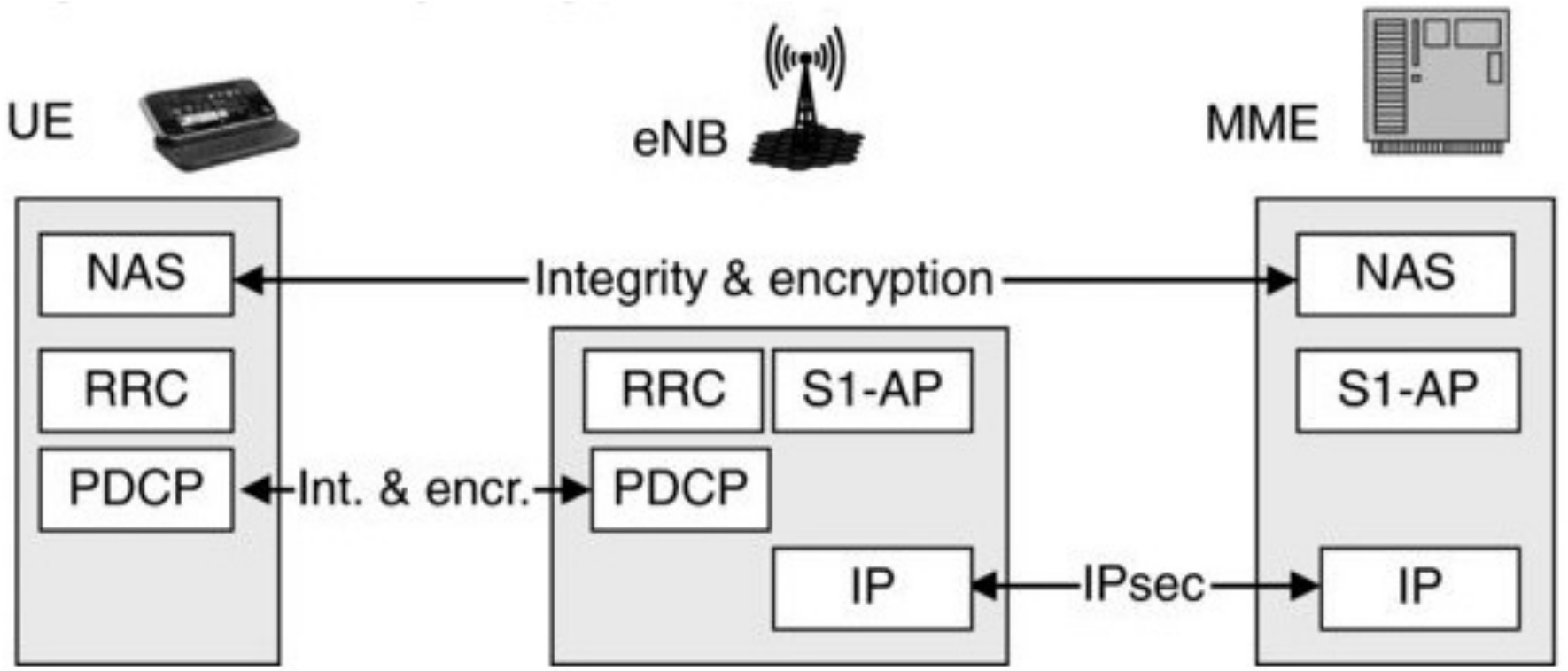


[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

Key Hierarchy

Key	Length	Info
K	128 bits	Key shared between the subscriber and the network operator, stored in the USIM and AuC; permanent key of the subscriber
CK, IK	128 bits	Ciphering key CK and integrity key IK are for UMTS interconnection
K_{ASME}	256 bits	A local master key of the subscriber from which all other keys will be derived; Shared between the UE and the MME
K_{NASenc}, K_{NASint}	128 / 256 bits	Ciphering key K_{NASenc} and integrity key K_{NASint} for NAS protection
K_{eNB} / NH	256 bits	Intermediate key stored in the eNodeB NH (Next Hop) is used in handover
K_{RRCenc}, K_{RRCint}	128 / 256 bits	Ciphering key K_{RRCenc} and integrity key K_{RRCint} for AS protection
K_{UPenc}	128 / 256 bits	Ciphering key K_{UPenc} for user data

EPS Signalling Plane Protection



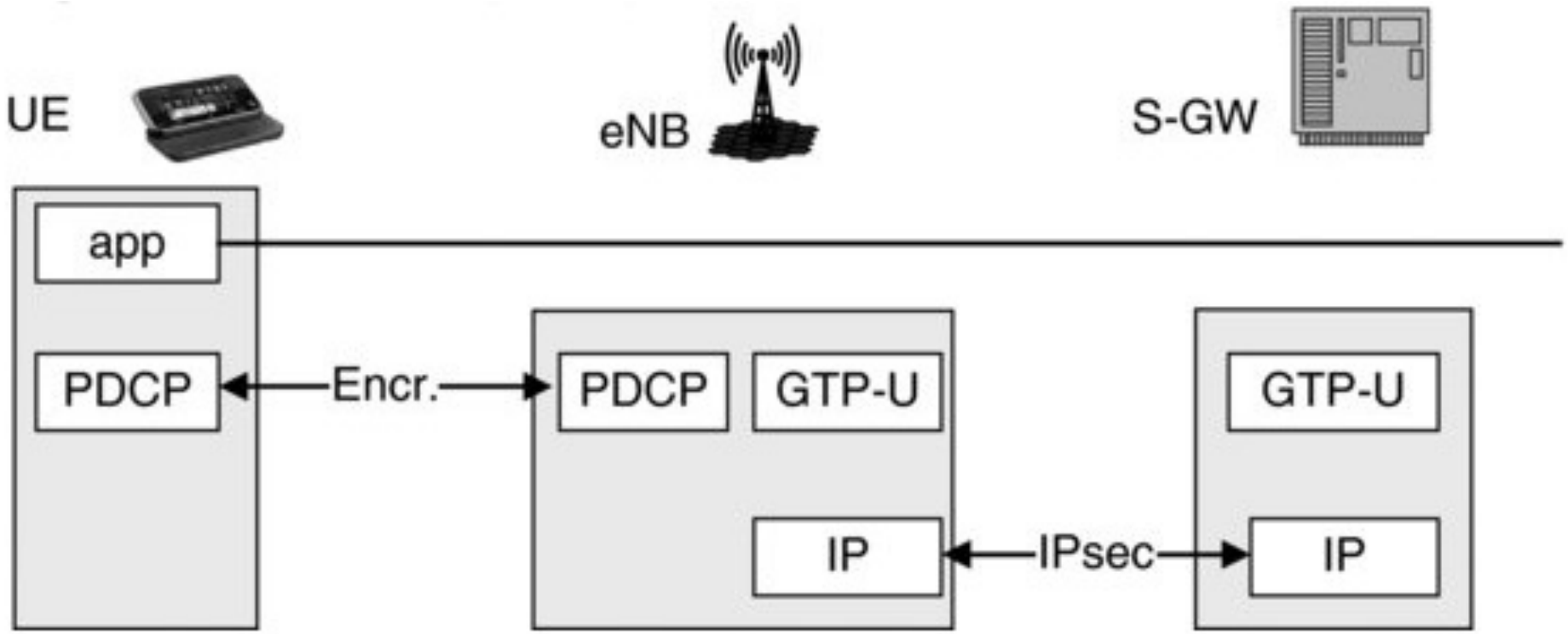
NAS: Non-Access Stratum
RRC: Radio Resource Control
PDCP: Packet Data Convergence Protocol
IP: Internet Protocol

[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

EPS Signalling Plane Protection

- NAS (Non-Access Stratum): network layer communication between the UE and the core network
- RRC (Radio Resource Control): layer 3 protocol in the AS (Access Stratum) protocol stack that provides communication between the UE and the eNodeB (the AS level signalling protocol)
- PDCP (Packet Data Convergence Protocol): both RRC signalling and user data are carried by the PDCP, and here is where security is implemented
- S1-AP: signalling service between the E-UTRAN and the EPC

EPS User Plane Protection



PDCP: Packet Data Convergence Protocol
GTP: GPRS Tunneling Protocol

[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

EPS User Plane Protection

- PDCP (Packet Data Convergence Protocol): if for signalling data both confidentiality and integrity are supported, user plane protection does not consider integrity

- GTP-U: is used for carrying data from the access network to the core network

Confidentiality is optional for both signalling and user plane!

EPS Security Requirements

- High level and service-related security requirements:
  - EPS should provide authenticity of information between the terminal and the network
  - EPS shall ensure that unauthorized users cannot establish communication through the system
  - EPS shall allow the network to hide its internal structure from the terminal
  - Security policies should be under home operator control
  - EPS shall provide support for lawful interception
  - EPS shall support emergency calls
  - Rel-99 or newer USIM is required for authentication

EPS Security Requirements

- Privacy related security requirements:
  - *EPS shall provide several appropriate levels of user privacy for communication, location and identity*
  - *Communication content, origin and destination shall be protected against disclosure to unauthorized parties*
  - *EPS shall be able to hide user identities from unauthorized parties*
  - *EPS shall be able to hide user location from unauthorized parties*

EPS Security Features

- Features that are carried over from GSM and UMTS:
  - Subscriber authentication, usage of USIM (IMEI stored in the ME and IMSI stored in the UICC)
  - Mutual authentication (from UMTS)
  - Encryption on the radio interface (for *confidentiality*), which remains optional to the network operator
  - Usage of temporary identities (for *privacy of subscribers*)
  - Visibility and configurability of security at the UE (e.g. ciphering indicator) is optional
  - Lawful interception

EPS Security Features

- New features in EPS to overcome the shortcomings in GSM/UMTS:
  - The endpoint for encryption in the network side remains the eNodeB, but physical security requirements are introduced for eNodeB (in UMTS is the RNC, but in GSM is the BTS)
  - No integrity mechanism for the user data (reason: risk to tamper the user data is considered too low to introduce significant overhead by integrity protection, especially for voice)
  - New key hierarchy, more elaborated
  - Improvements on crypto algorithms and protocols

EPS Security Standards

- TS 33.401: *3GPP System Architecture Evolution (SAE); Security architecture* / ETSI 133 401
  - EPS security architecture
  - EPS security features, procedures, mechanisms
  - Main reference

- TS 33.402: *Security aspects of non-3GPP accesses* / ETSI 133.402
- TS 33.320: *Security of Home evolved Node B (HeNB)* / ETSI 133.320

- TS 36.331: *Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification* / ETSI 136 331
- TS 24.301: *Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)* / ETSI 124 301
- …

3GPP: The 3rd Generation Partnership Project
ETSI: European Telecommunications Standards Institute

To remember!

1. LTE (security) architecture
2. Security mechanisms on both the signalling and the user plane
3. Security features (build on previous generations' features)