WPA2 / 802.11i

Network Security - Lecture 4

Ruxandra F. Olimid

Faculty of Mathematics and Computer Science, University of Bucharest

*slides adapted from the course TTM4137 thought at NTNU

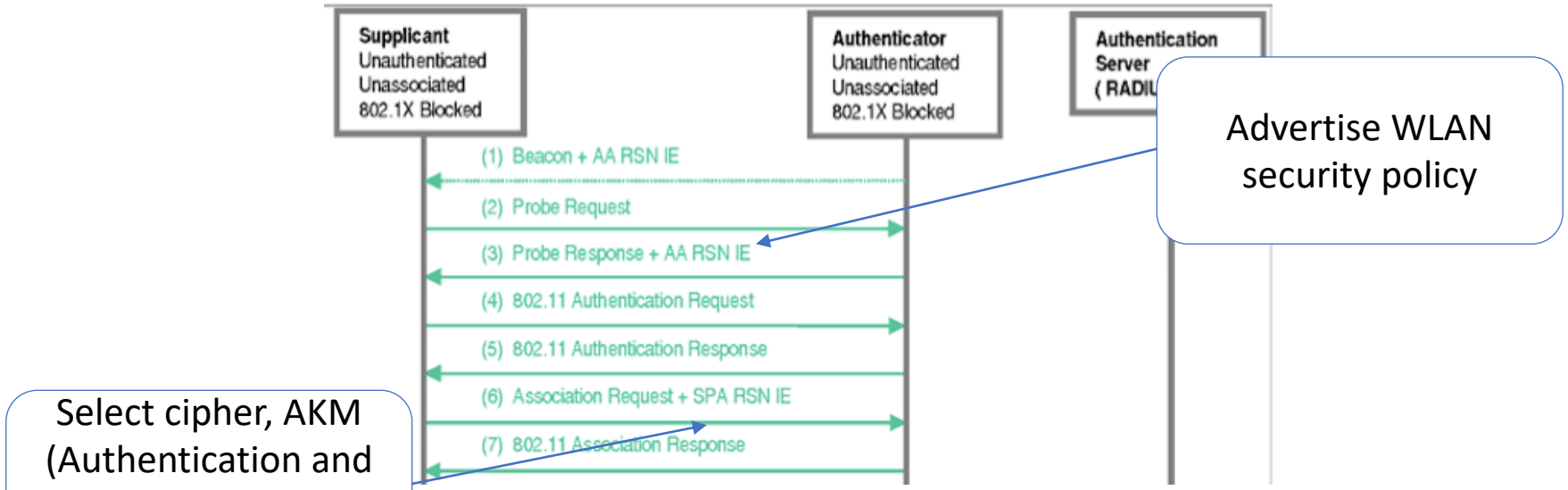
Outline

- RNS
- CCMP
- Key Hierarchy
- Security / Attacks

Robust Security Network (RSN)

RSN: a protocol for establishing a secure communication over 802.11 wireless networks

RSN Information Element (IE): data structure for advertising and negotiating security capabilities



[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i https://theory.stanford.edu/~jcm/papers/NDSS05.pdf]

Robust Security Network (RSN)

Backward compatibility with WEP!

If the cryptosystems are broken, easily change to new ones!

Defined Ciphersuites

- 00-0F-AC:1 WEP-40
- 00-0F-AC:2 TKIP
- 00-0F-AC:4 AES-CCMP (default)
- 00-0F-AC:5 WEP-104
- Vendor OUI:Any Vendor specific
- Other Reserved

Defined AKMs

- 00-0F-AC:1 802.1X Authentication + 4-Way Handshake
- 00-0F-AC:2 PSK + 4-Way Handshake
- Vendor OUI:Any Vendor specific
- Other Reserved

RSN IE

Element ID	Length	Version
Group Key Ciphersuite Selector		
Pairwise Ciphersuite Count	Pairwise Ciphersuite List	
Pairwise Ciphersuite List	AKM Count	
AKM List		
Capabilities	PMK ID Count	
PMK ID List		

[Source: 802.11i Overview doc.: IEEE 802.11-04/0123r1]

Security Goals

Tries to address all known WEP Problems

- Reply detection

  Packet Number (PN), replay counter

- Key management protocols

  Similar to WPA, discussed in more details

- Access control

  Uses **802.1X architecture**

Security Goals

Tries to address all known WEP Problems

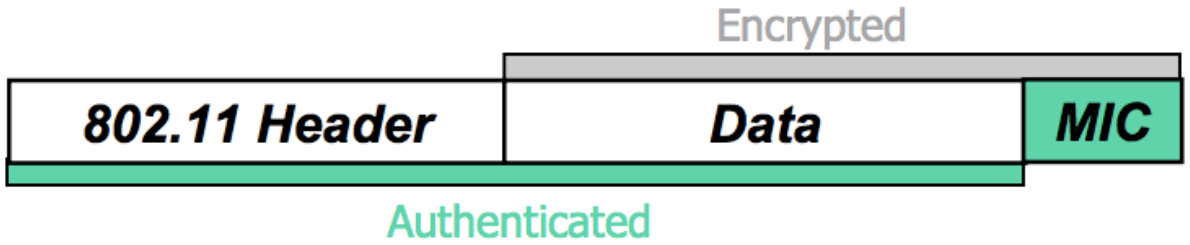
Authenticated encryption using CTR mode and CBC-MAC assumes 128-bit blocks and a single crypto key

- Confidentiality

  Uses **Advanced Encryption Standard (AES)**, instead of RC4

- Message integrity and authentication

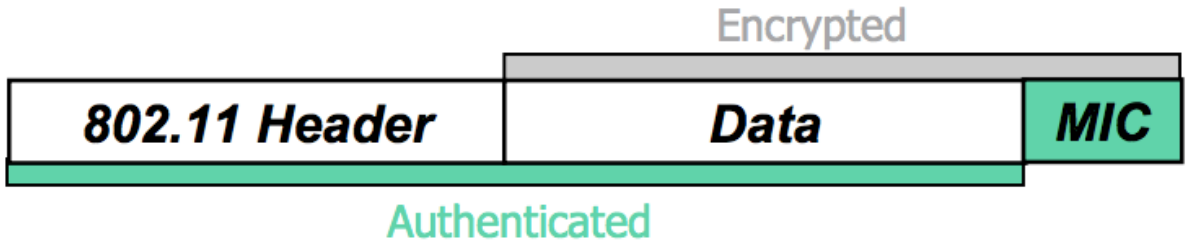
  Uses 128 bits **Counter Mode with CBC-MAC Protocol (CCMP)**



[Source: IEEE 802.11i Overview http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf]

CCM Mode

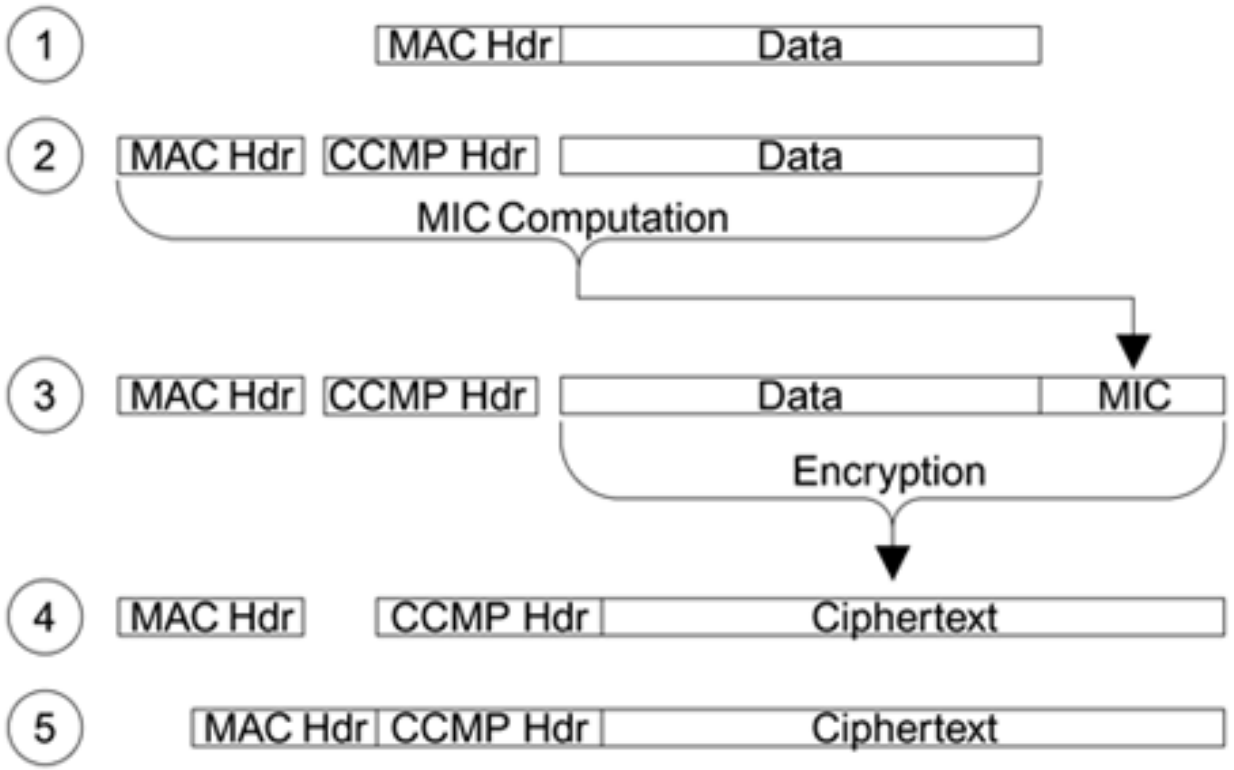
- Authenticated encryption (with associated data) combining CTR mode and CBC-MAC:
  - appends a CBC-MAC on the header, length of the header and plaintext
  - encrypts in CTR mode (plaintext blocks with 1,2,3… and MIC with counter value 0)
- Uses a single crypto key (temporal key shared by STA and AP) and assumes 128-bit blocks



[Source: IEEE 802.11i Overview http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf]

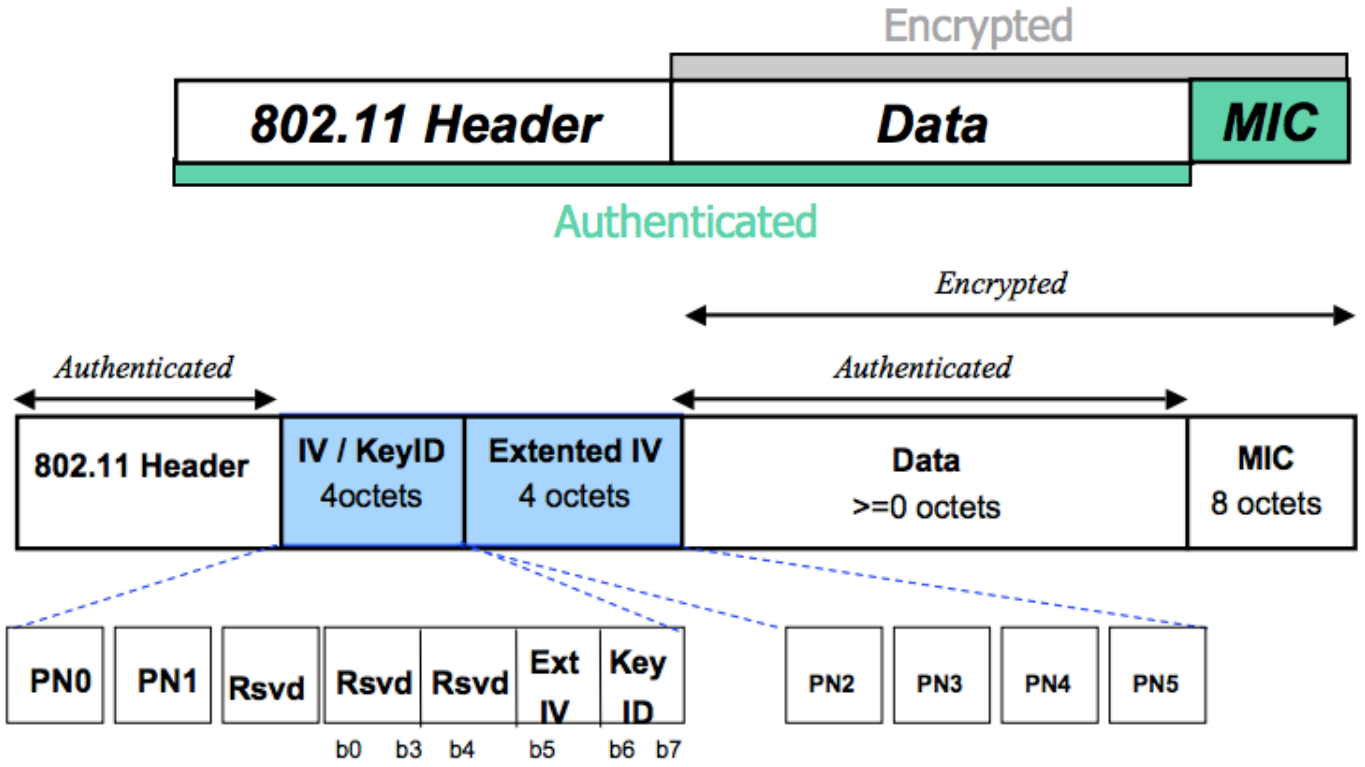
CCM Mode

1) Unencrypted MPDU; MAC header contains source and destination addresses;
2) CCMP header (32 bits) is constructed
3) MIC is computed to protect fields from the MAC header, the CCMP header and the data
4) Data and MIC are encrypted; CCMP header is pre-appended
5) MAC header is pre-appended



[Source: Course book, Edney &Arbaugh, Chapter 12]

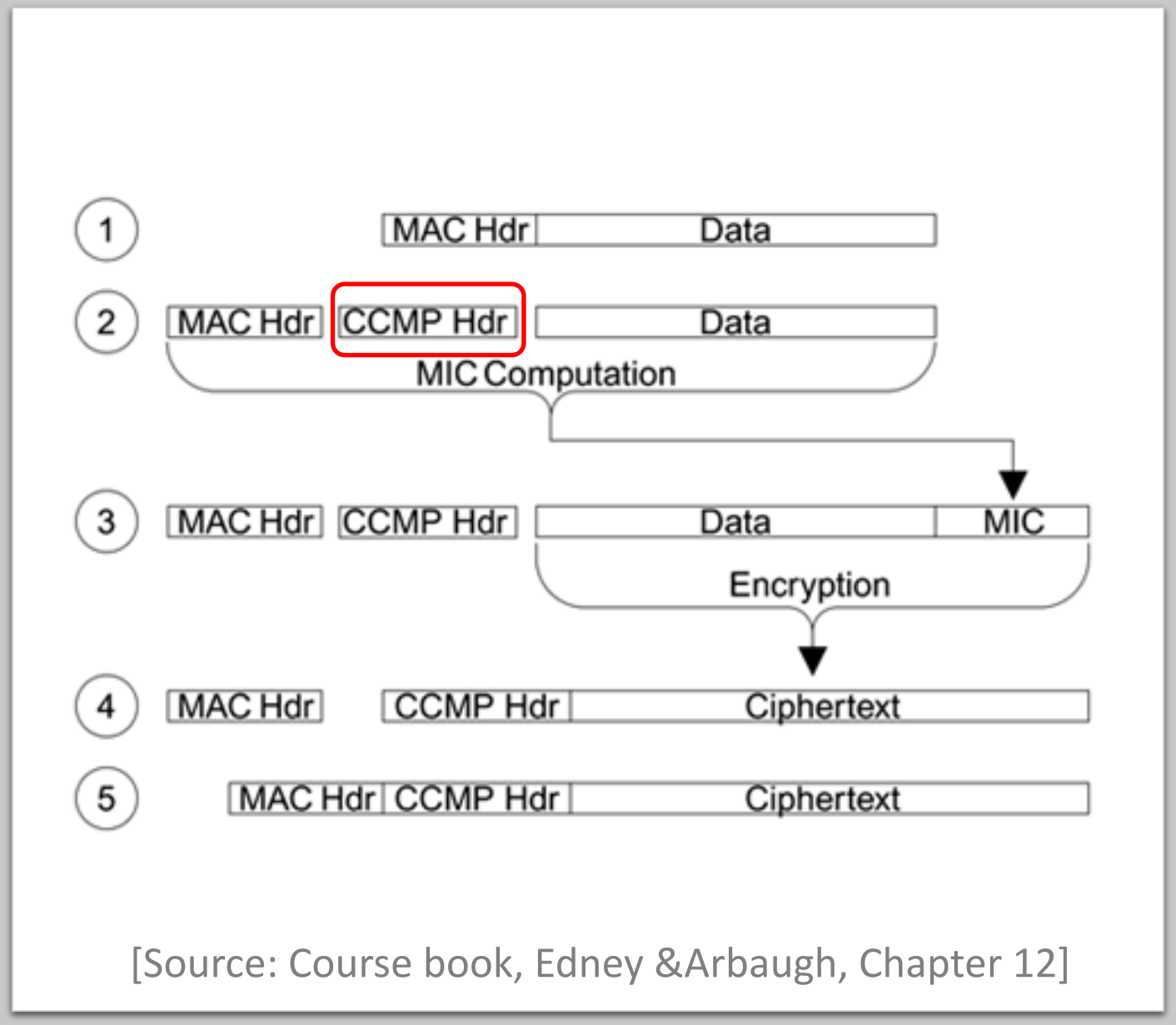
CCMP MPDU Format



[Source: IEEE 802.11i Overview http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf]

CCM Mode

1) Unencrypted MPDU; MAC header contains source and destination addresses;
2) CCMP header (32 bits) is constructed
3) MIC is computed to protect fields from the MAC header, the CCMP header and the data
4) Data and MIC are encrypted; CCMP header is pre-appended
5) MAC header is pre-appended



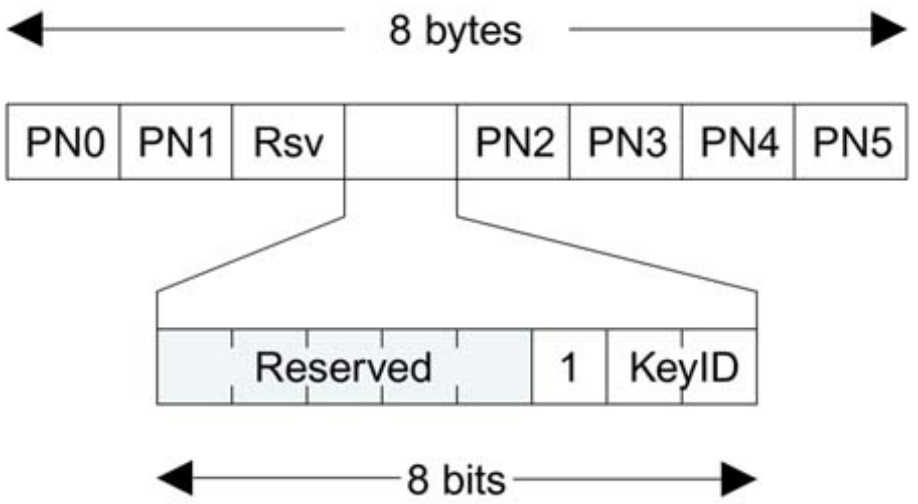
[Source: Course book, Edney &Arbaugh, Chapter 12]

CCMP Header

Purposes:

- Provides the Packet Number (PN) that provides replay protection and gives to the receiver the nonce required for decryption
- In case of multicast, it gives to the receiver the group key used for encryption

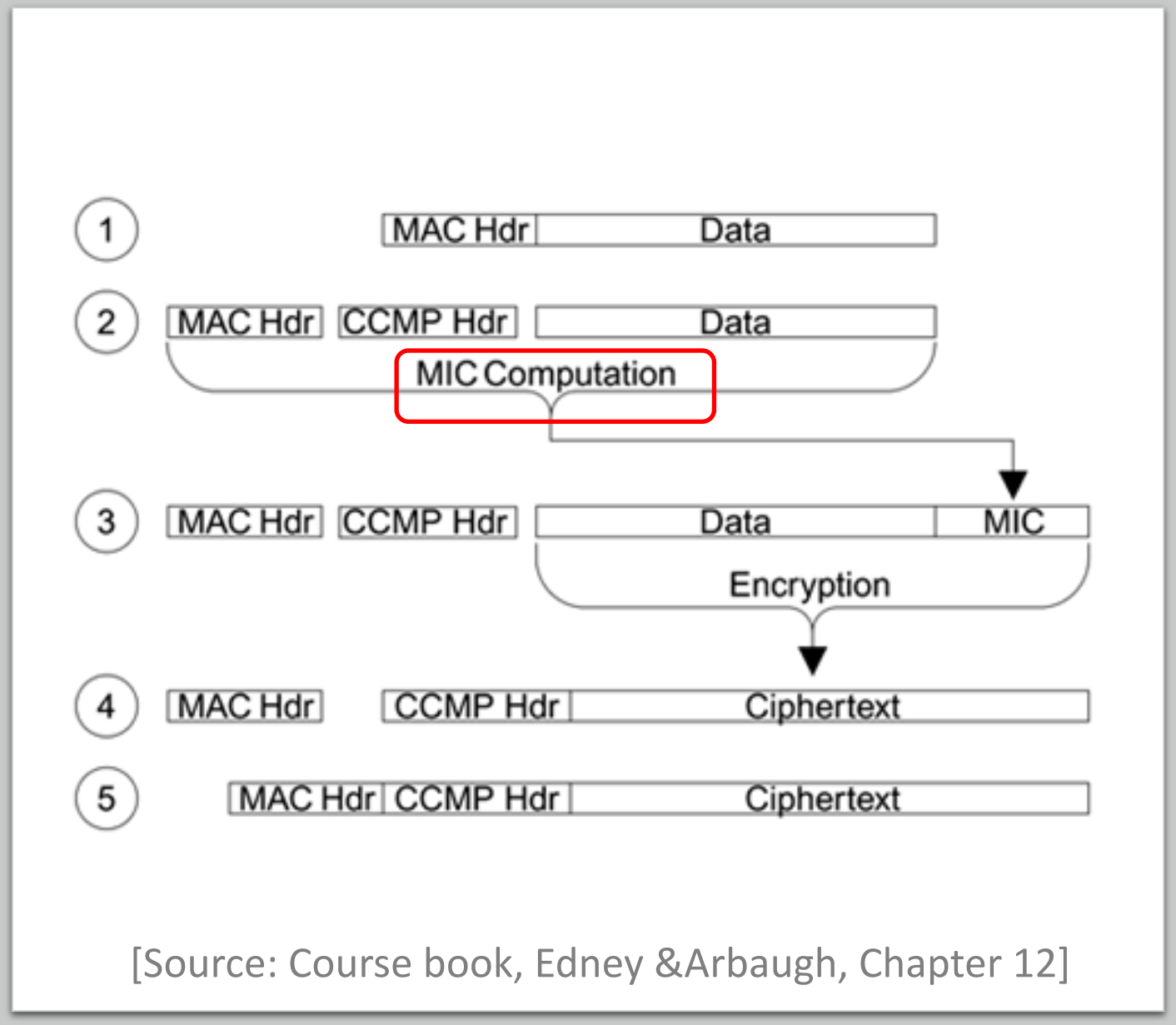
- Packet Number (PN): 48 bits (6 bytes)
- 1: indicates RSN
- KeyID: to select the group key id (from max.4 provisioned)



[Source: Course book, Edney &Arbaugh, Chapter 12]

CCM Mode

1) Unencrypted MPDU; MAC header contains source and destination addresses;
2) CCMP header (32 bits) is constructed
3) MIC is computed to protect fields from the MAC header, the CCMP header and the data
4) Data and MIC are encrypted; CCMP header is pre-appended
5) MAC header is pre-appended



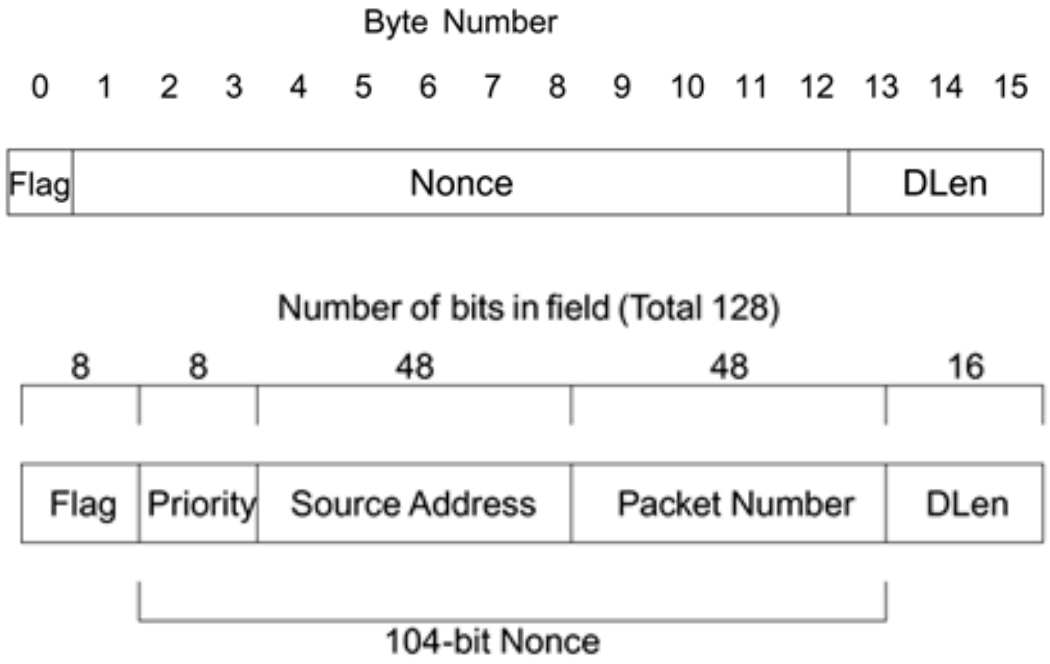
[Source: Course book, Edney &Arbaugh, Chapter 12]

MIC Computation

- Uses **CBC-MAC**, with a starting block – see CCMP Encapsulation slide
- 64-bit (8 bytes) MIC, so last 64 bits are discarded

Staring block (IV) is formed in a special way**:**

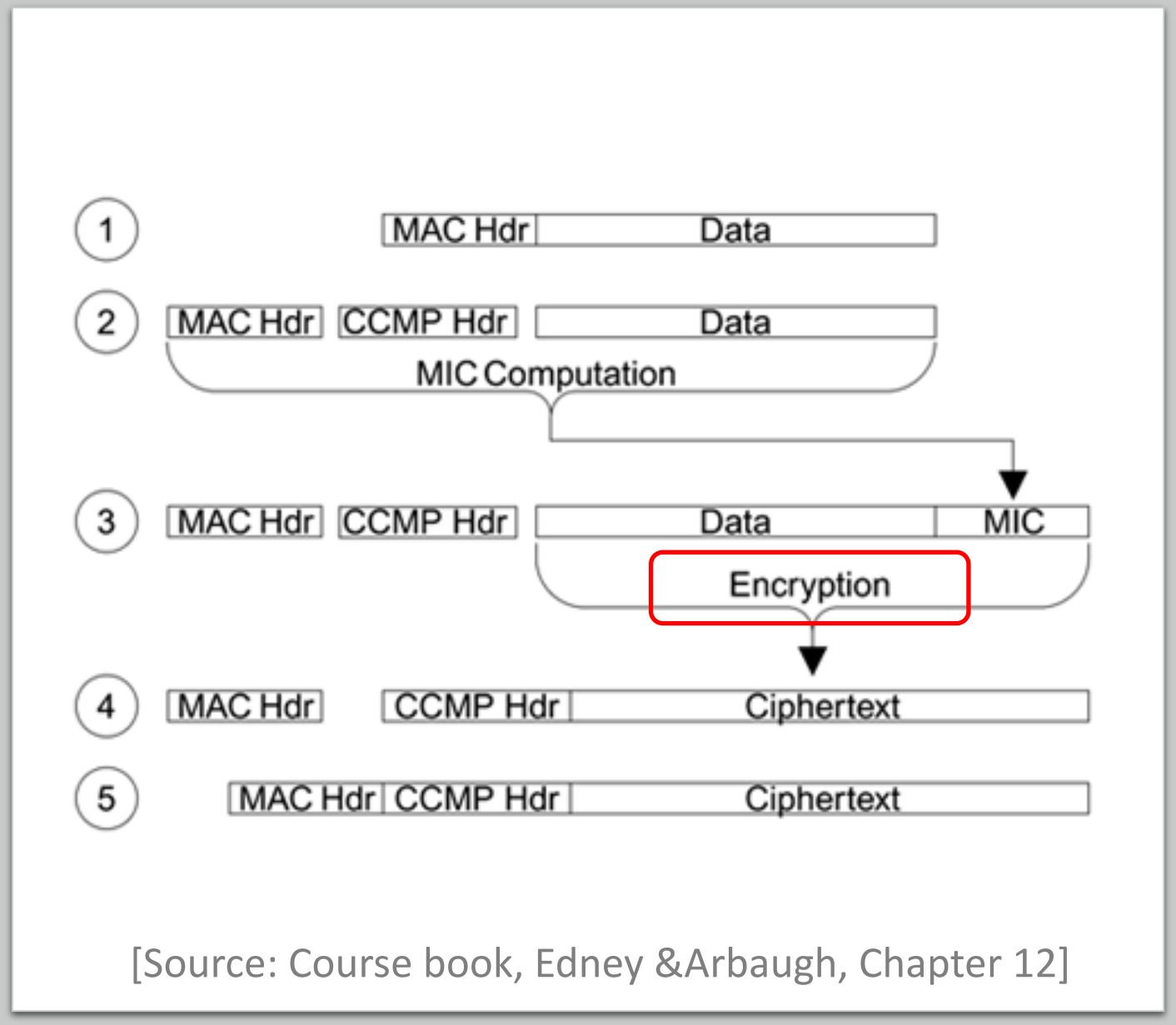
- **Flag: 01011001** (fixed)
- **Nonce:** contains both the PN and the source address to assure uniqueness (the PN could have been already used by one of the two communicating parties in another conversation); priority might refer to different streams (audio, video, etc.);
- **DLen**: length of the data



[Source: Course book, Edney &Arbaugh, Chapter 12]

CCM Mode

1) Unencrypted MPDU; MAC header contains source and destination addresses;
2) CCMP header (32 bits) is constructed
3) MIC is computed to protect fields from the MAC header, the CCMP header and the data
4) Data and MIC are encrypted; CCMP header is pre-appended
5) MAC header is pre-appended



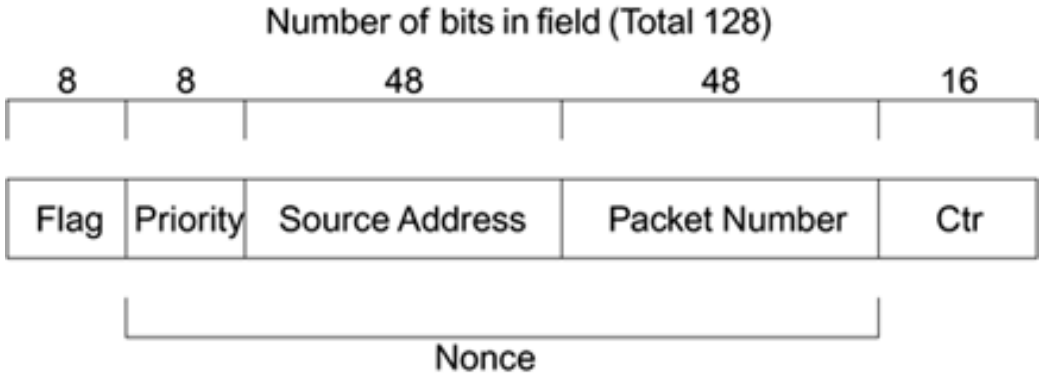
[Source: Course book, Edney &Arbaugh, Chapter 12]

Encryption

- Uses **CTR-AES**

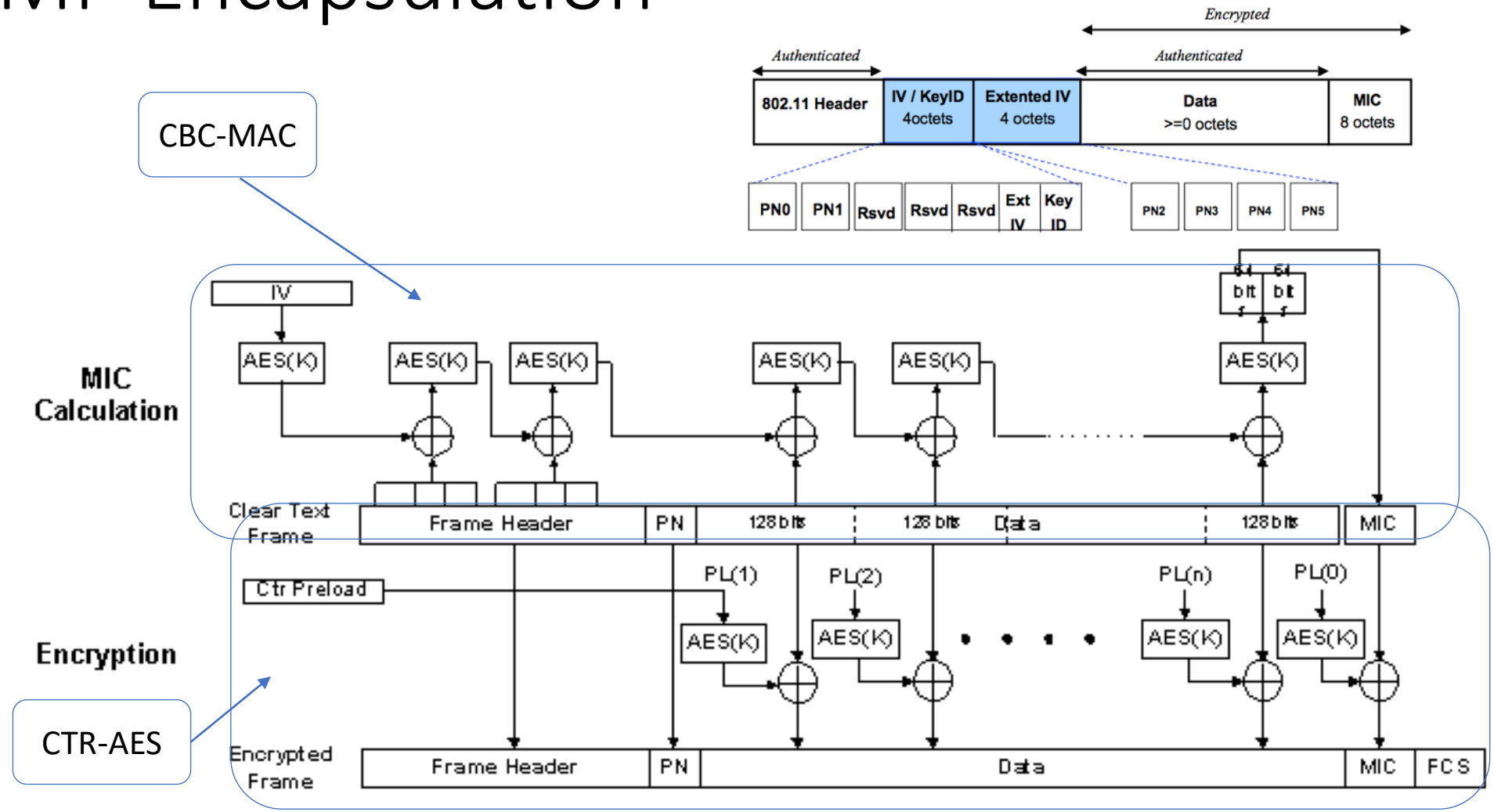
Counter block (PL0,PL1…):

- **Flag: 01011001** (fixed)
- **Nonce:** contains both the PN and the source address to assure uniqueness (the PN could have been already used by one of the two communicating parties in another conversation); priority might refer to different streams (audio, video, etc.);
- **Ctr**: starts at 1 and increases



[Source: Course book, Edney &Arbaugh, Chapter 12]

CCMP Encapsulation

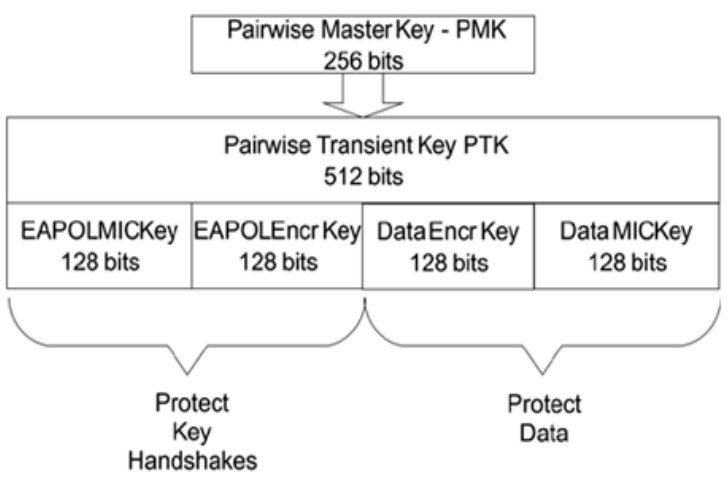


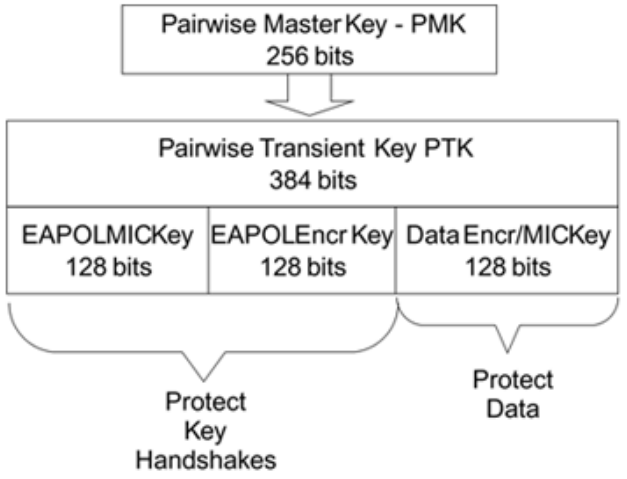
More details in the course book – Edney & Arbaugh, Chapter 12

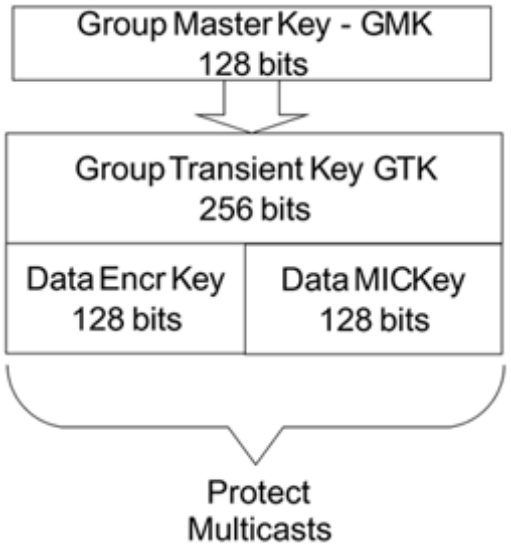
Key hierarchy (TKIP vs CCMP)

Pairwise

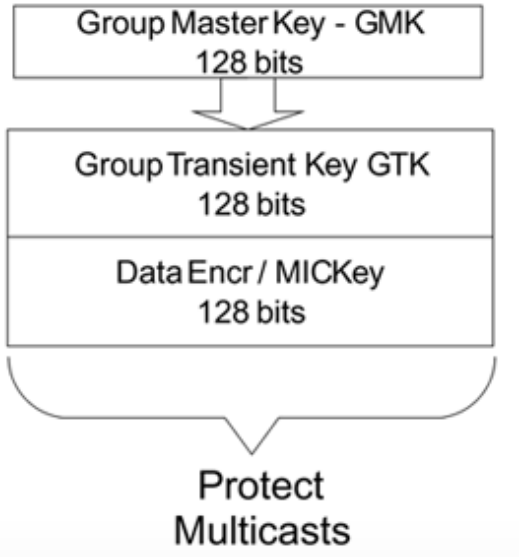
Group







TKIP

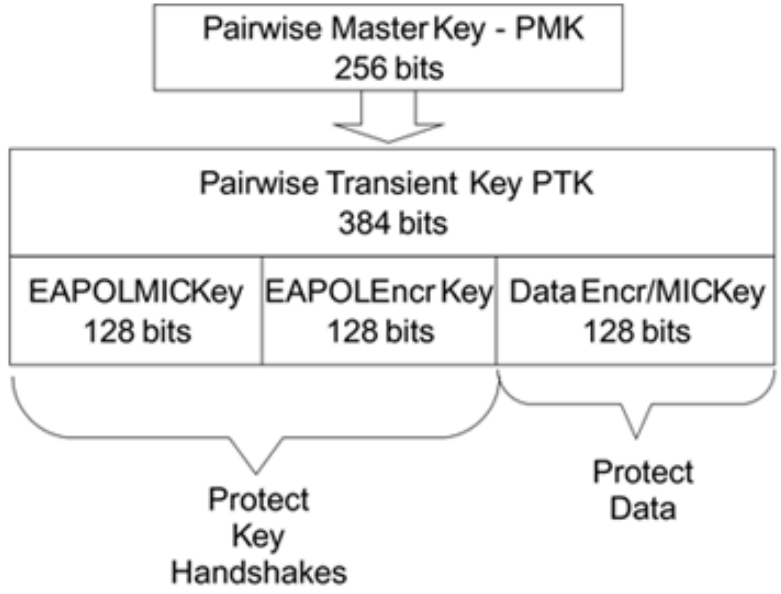


CCMP

[Source: Course book, Edney &Arbaugh, Chapter 10]

Pairwise CCMP Key Hierarchy

- Pairwise Master Key (PMK):
  - 256 bits, symmetric key
  - Preshared or server supplied by upper layers (e.g.: authentication server sends to AP)



[Source: Course book, Edney &Arbaugh, Chapter 10]

- Pairwise Transient Key (PTK):

$$PTK = f(PMK, NonceA, NonceB, A, B)$$

- Temporal Keys:
  - Up to 3 keys (128 bits):
    - EAPOL-keys: encryption key, integrity key
    - Data encryption and data integrity key (**a single key!**)

Group CCMP Key Hierarchy

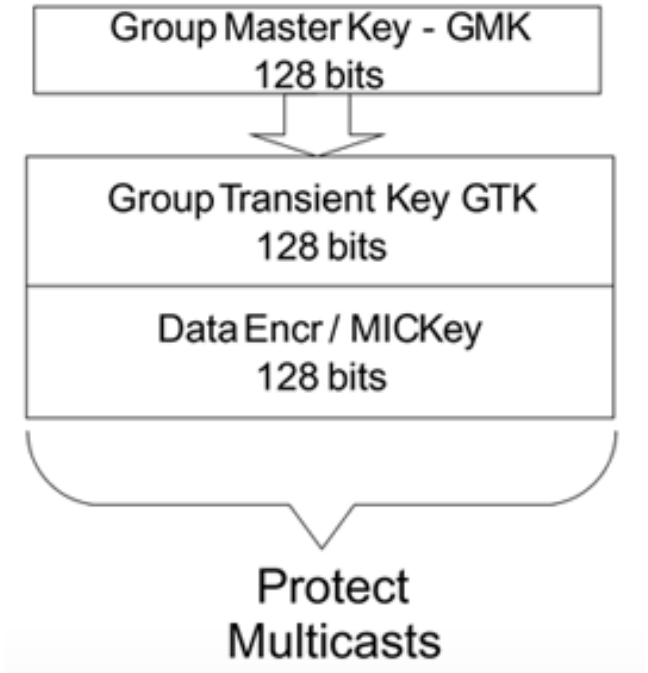
- Used for multi- and broadcast communication

- Group Master Key (GMK):
  - 256 bits, symmetric key
  - Generated by the AP

- Group Transient Keys (GTK):

$$GTK = f(GMK, Nonce, AP)$$

- Temporal Key:
  - Encryption and integrity key 128 bits (**a single key!**)



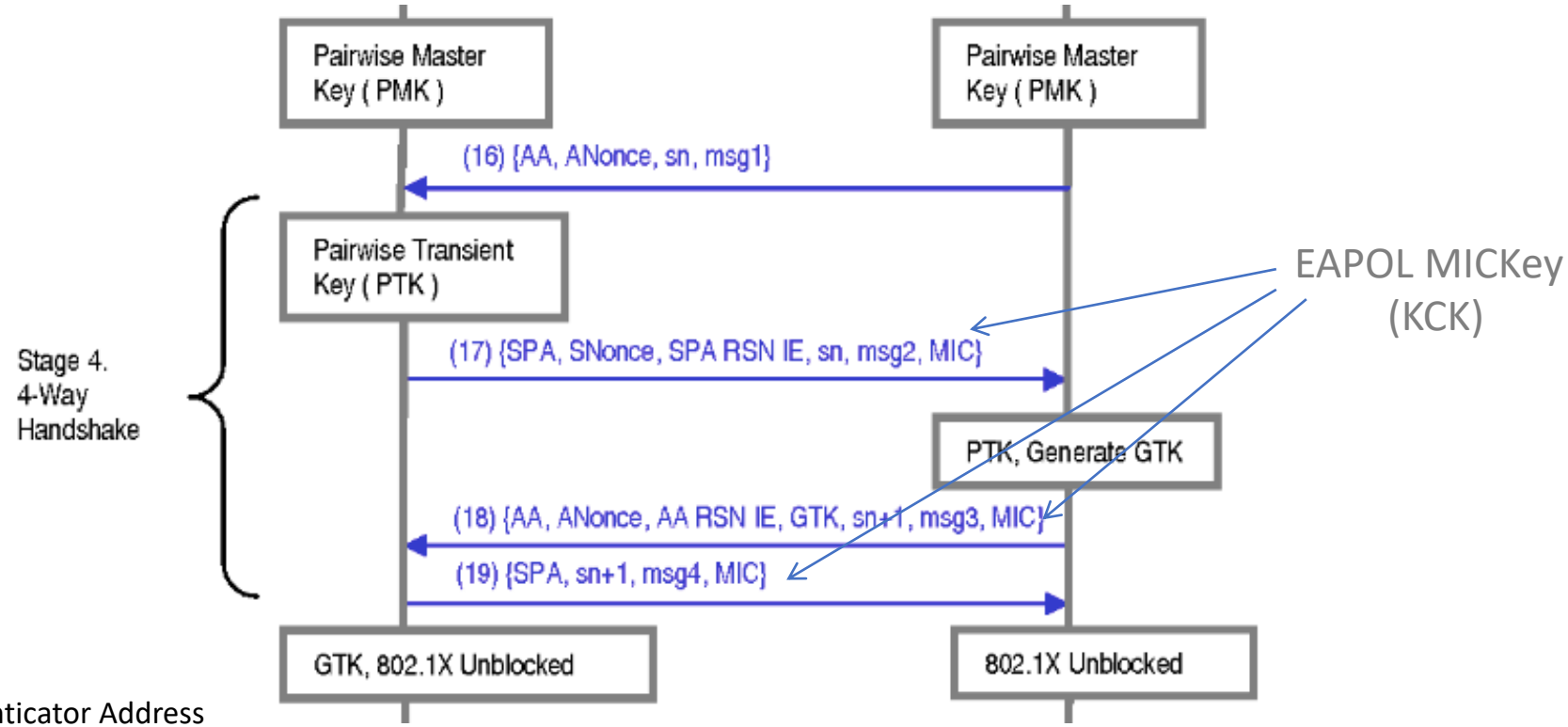
[Source: Course book, Edney &Arbaugh, Chapter 10]

802.11 Key Derivation Function (KDF)

$$\text{PTK} \leftarrow \text{KDF}(\text{PMK}, \min\{Addr_{AP}, Addr_{STA}\} \,||\, \max\{Addr_{AP}, Addr_{STA}\}, \max\{N_{AP}, N_{STA}\}))$$

- KDF is based on **HMAC-SHA-1**

4-Way Handshake protocol



Encrypted data communication follows

AA: Authenticator Address
SA: Supplicant Address
ANonce: nonce generated by the Authenticator (AP)
SNonce: nonce generated by the Supplicant (STA)
sn: sequence number

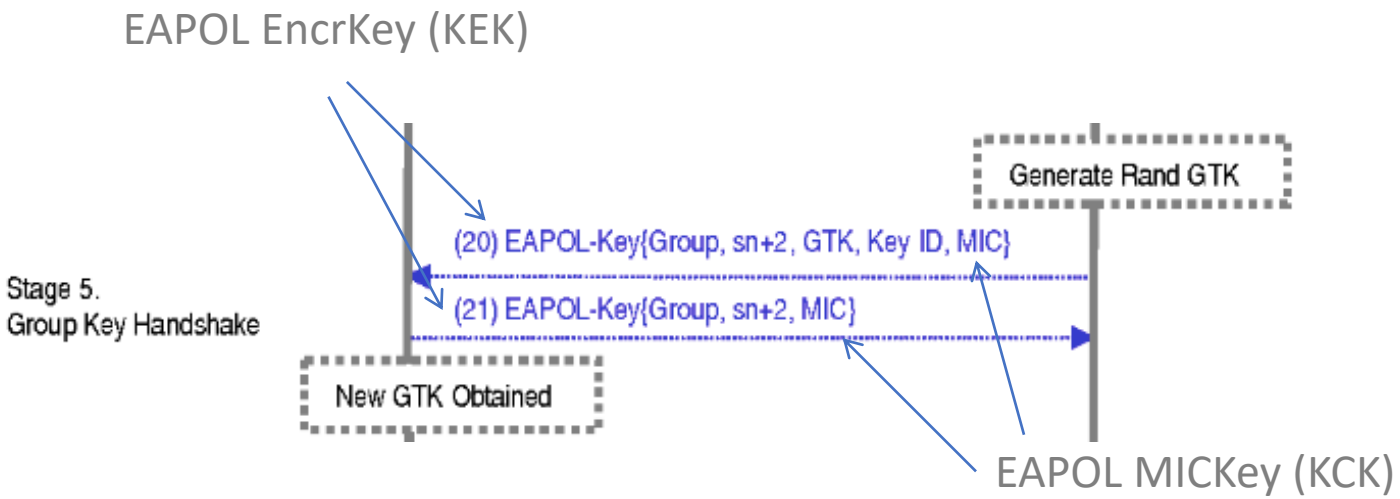
[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i https://theory.stanford.edu/~jcm/papers/NDSS05.pdf]

4WHS properties

- No forward secrecy
  - PMK + MACs + Nonces enough to derive PTK
  - Can decrypt old recorded communication sessions

- Vulnerable to dictionary attacks
  - If PMK derived from weak password
  - Capture MACs + Nonces → guess password → derive PMK

Group Key Generation and Distribution



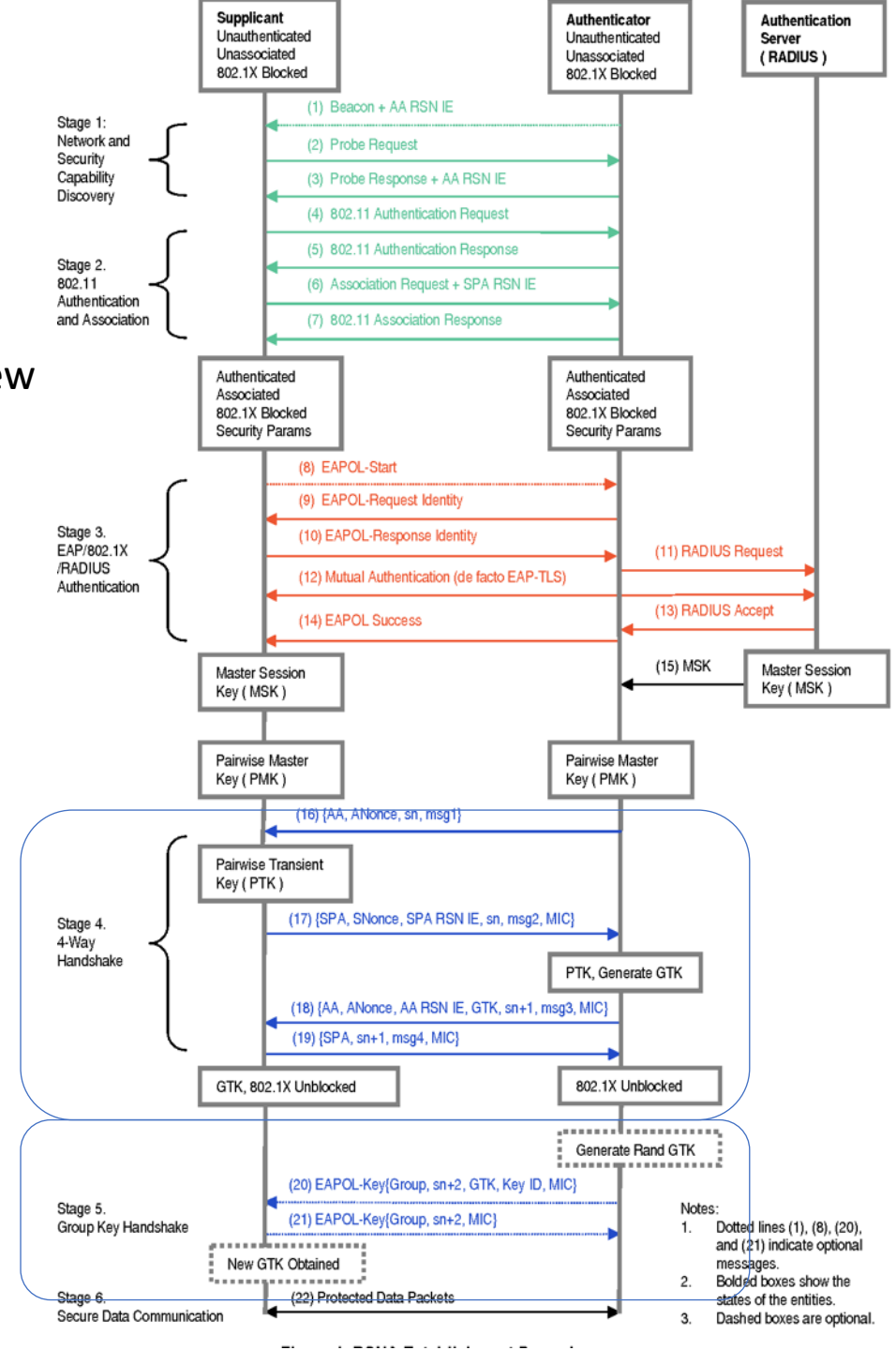
Encryption data communication follows

AA: Authenticator Address
SA: Supplicant Address
ANonce: nonce generated by the Authenticator (AP)
SNonce: nonce generated by the Supplicant (STA)
sn: sequence number

[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i https://theory.stanford.edu/~jcm/papers/NDSS05.pdf]

RSN/WPA2

Association Overview

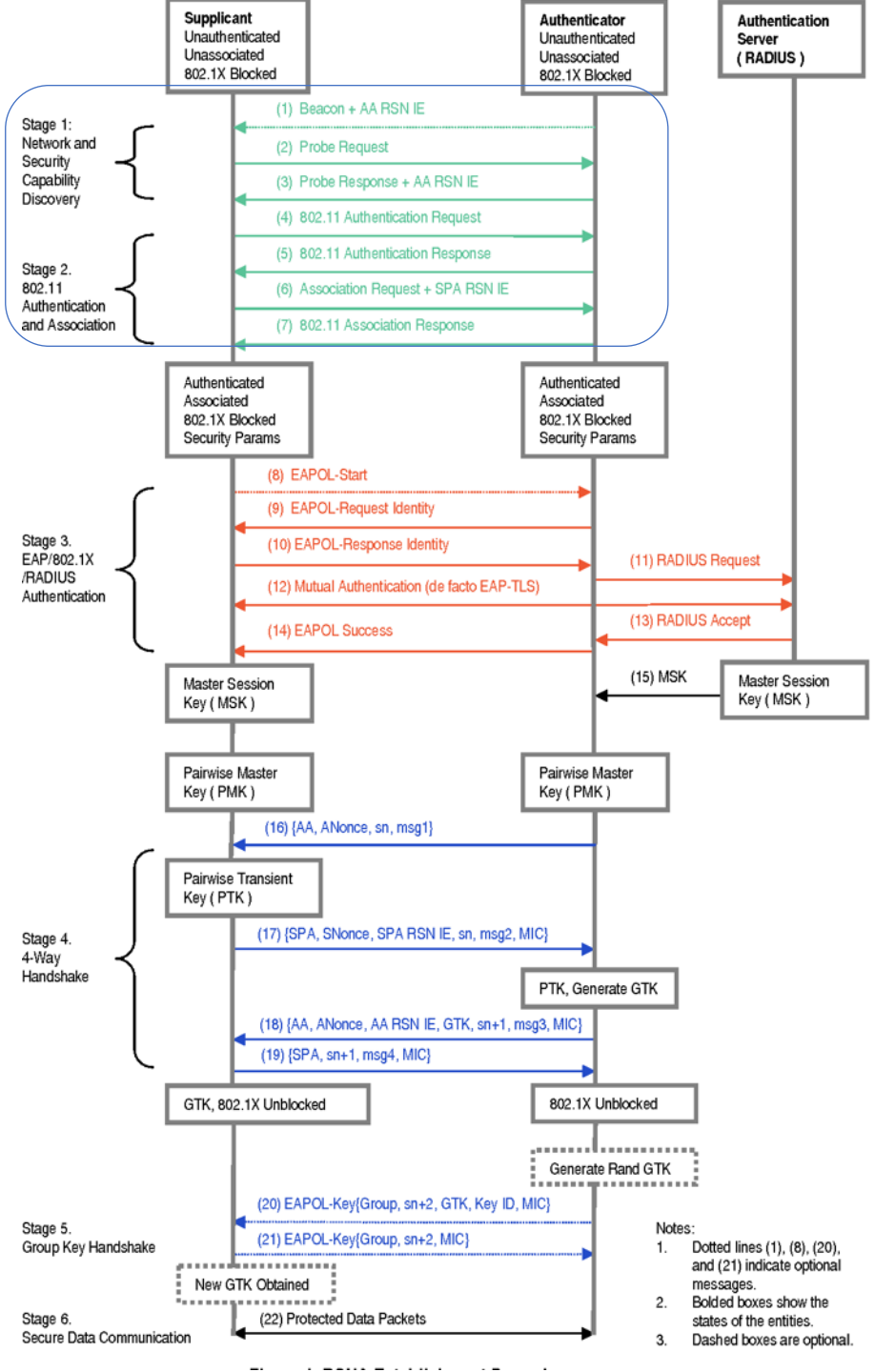


RSN IE: RSN Identification Element (set of capabilities)
AA: Authenticator Address
SA: Supplicant Address
ANonce: nonce generated by the Authenticator (AP)
SNonce: nonce generated by the Supplicant (STA)

[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i https://theory.stanford.edu/~jcm/papers/NDSS05.pdf]

RSN/WPA2

Association Overview



RSN IE: RSN Identification Element (set of capabilities)
AA: Authenticator Address
SA: Supplicant Address
ANonce: nonce generated by the Authenticator (AP)
SNonce: nonce generated by the Supplicant (STA)

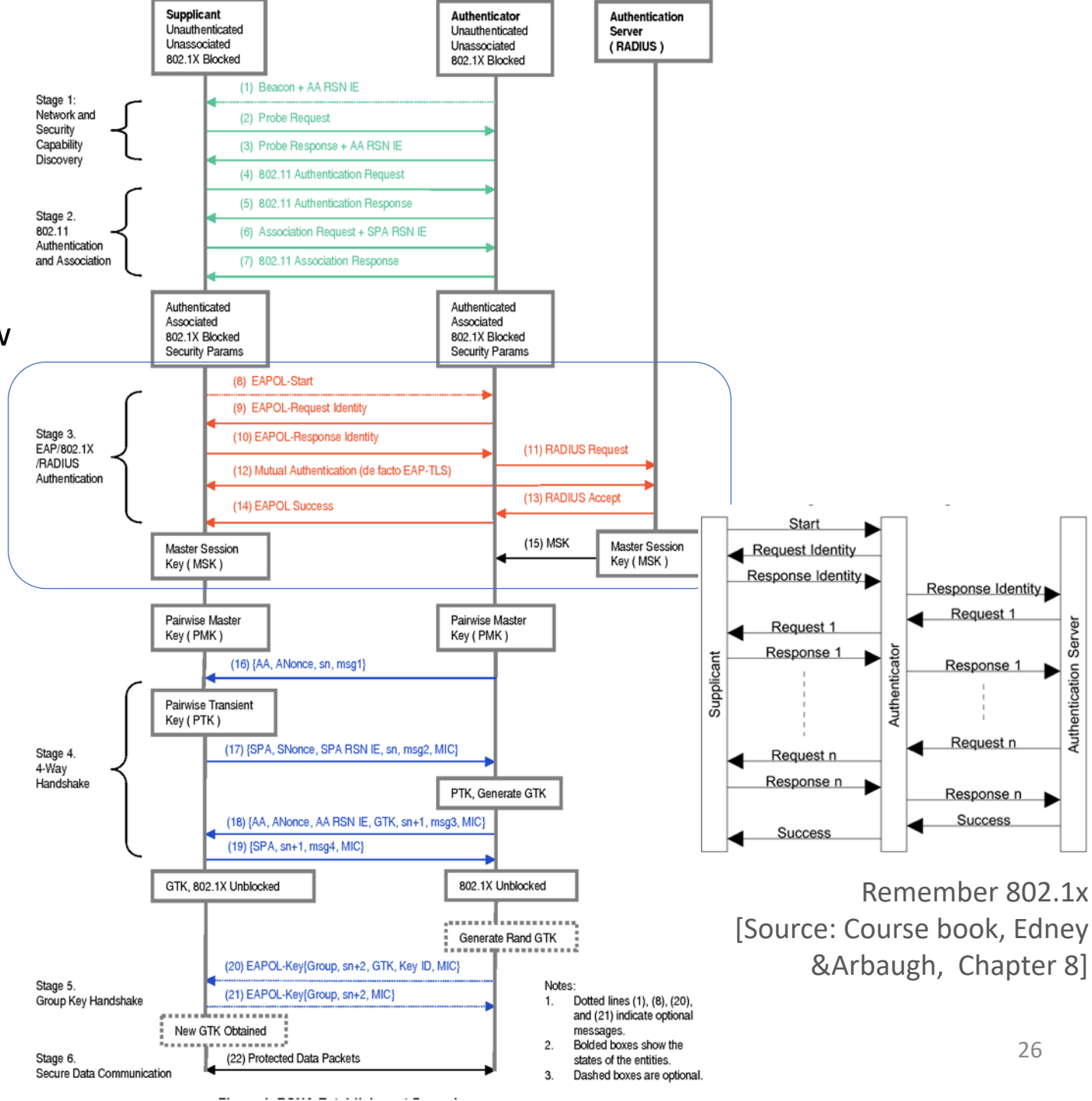
[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i https://theory.stanford.edu/~jcm/papers/NDSS05.pdf]

RSN/WPA2

Association Overview

Both parties prove to know the same MSK

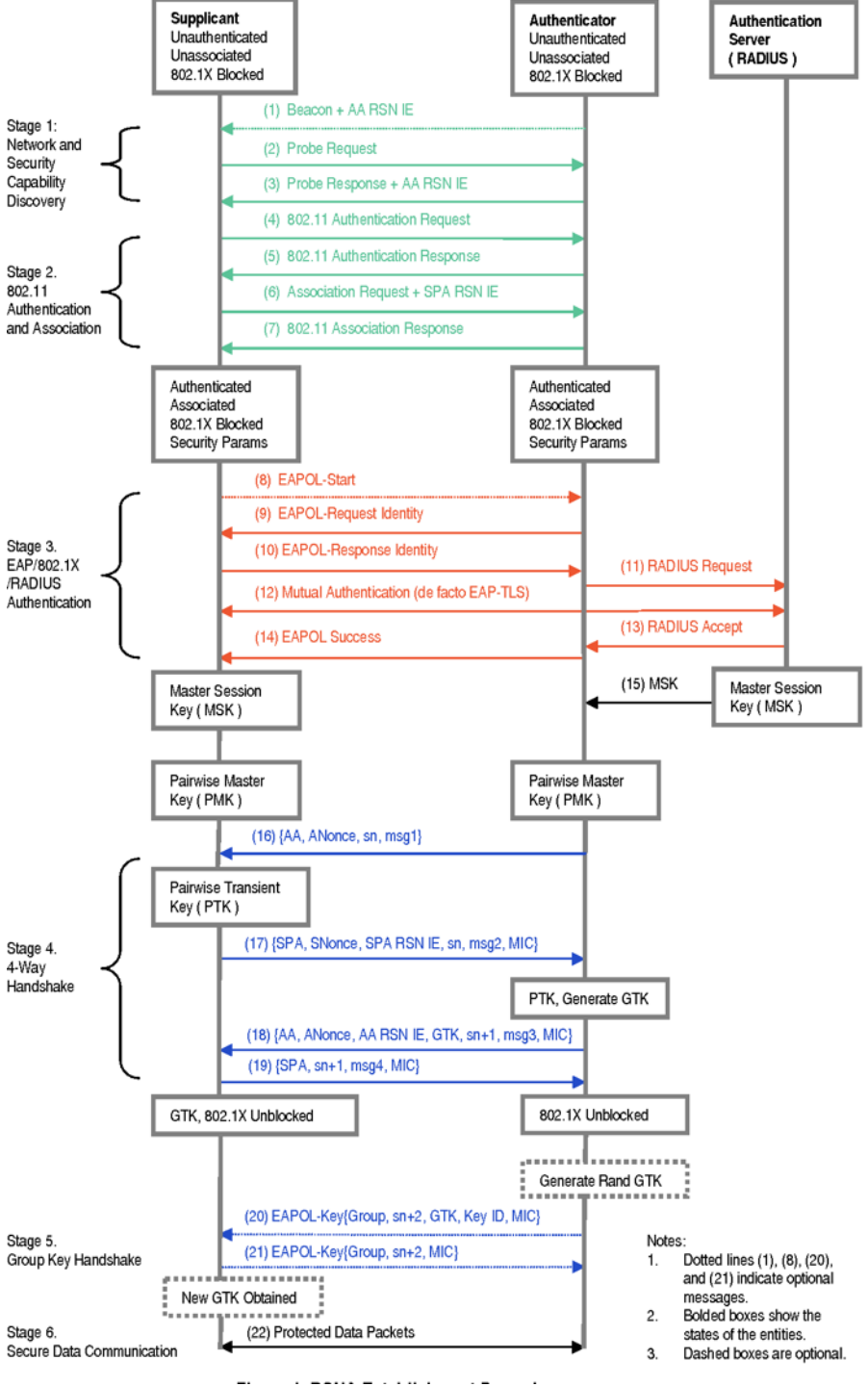
RSN IE: RSN Identification Element (set of capabilities)
AA: Authenticator Address
SA: Supplicant Address
ANonce: nonce generated by the Authenticator (AP)
SNonce: nonce generated by the Supplicant (STA)



Remember 802.1x
[Source: Course book, Edney &Arbaugh, Chapter 8]

RSN/WPA2

Association Overview



RSN IE: RSN Identification Element (set of capabilities)
AA: Authenticator Address
SA: Supplicant Address
ANonce: nonce generated by the Authenticator (AP)
SNonce: nonce generated by the Supplicant (STA)

[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i https://theory.stanford.edu/~jcm/papers/NDSS05.pdf]

Security / Attacks

- CCM Mode: theoretical security proof

[Jonsson, J. (2003, January). On the security of CTR+ CBC-MAC. In SelectedAreas in Cryptography(pp. 76-93). Springer Berlin Heidelberg]

- In practice: does the security proof model applies to the protocol?

https://www.krackattacks.com/

Paper: https://papers.mathyvanhoef.com/ccs2017.pdf

Video: https://youtu.be/Oh4WURZoR98

WPA2

- We will look into WPA3 next time

WPA3

Network Security - Lecture 5

Ruxandra F. Olimid

Faculty of Mathematics and Computer Science, University of Bucharest

Outline

- SAE
- Dragonfly Handshake
- Attacks / Vulnerabilities

Changes

- Introduces Simultaneous Authentication of Equals (SAE) to replace the pre-shared key exchange
- SAE is a variant of the Dragonfly Handshake
- Enterprise: must offer at least 192 bits of security (e.g., 384-bit EC)
- Enforces 802.11w – security of management frames (e.g., radio management, QoS)

The Dragonfly Handshake

- Is a Password Authenticated Key Exchange (PAKE)
- Starts with a password and generates a higher entropy key
- Supports Elliptic Curve Cryptography (ECC)
- Has 2 phases:
  - *Commit*
  - *Confirm*

WPA3 – SAE Handshake

[Source: Vanhoef, M. and Ronen, E., 2020, May. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 517-533). IEEE.]

P: Password
k: the final / negotiated key

(k is further used in the 4WH, as in WPA2; i.e. *k* is like the PMK)

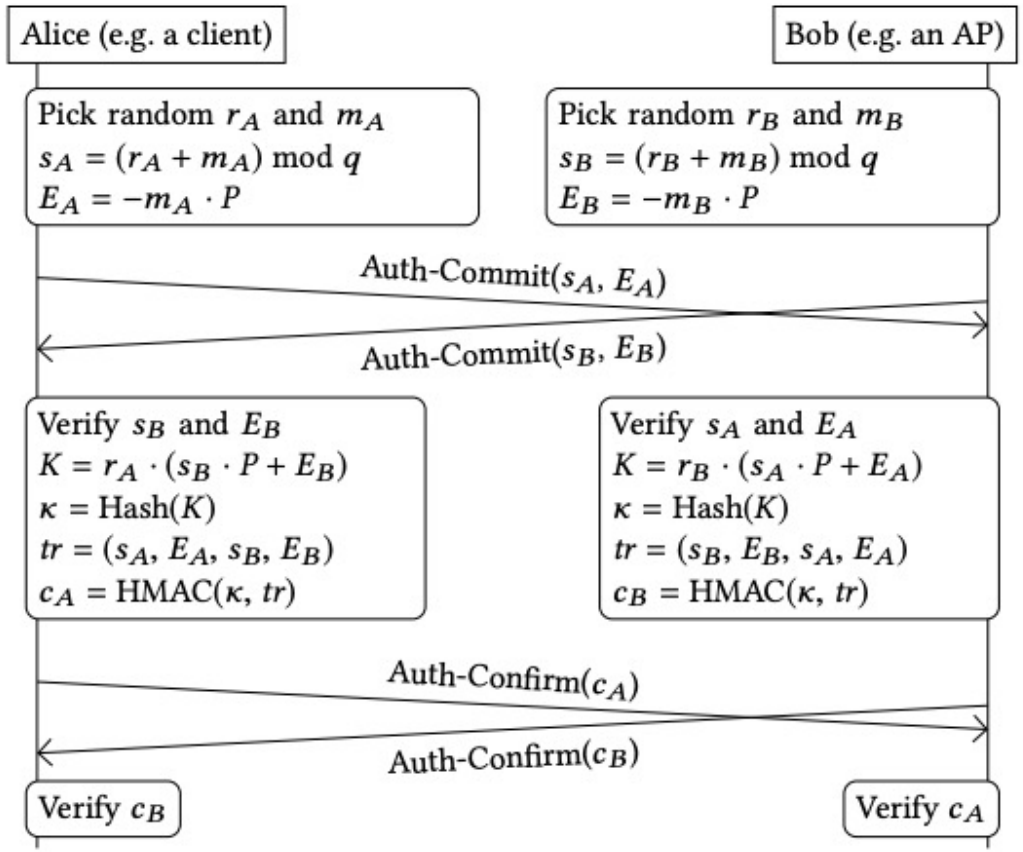


Figure 1: WPA3's SAE handshake. Both stations can simultaneously initiate the handshake, hence the crossed arrows. We assume elliptic curves are used, though similar operations are performed when using multiplicative groups.

WPA3 – Security against a dictionary attack

[Source: Vanhoef, M. and Ronen, E., 2020, May. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 517-533). IEEE.]

P: Password
k: the final / negotiated key

Remember: WPA2 was vulnerable to a dictionary attack by capturing a handshake.
WPA3 offers protection, why?

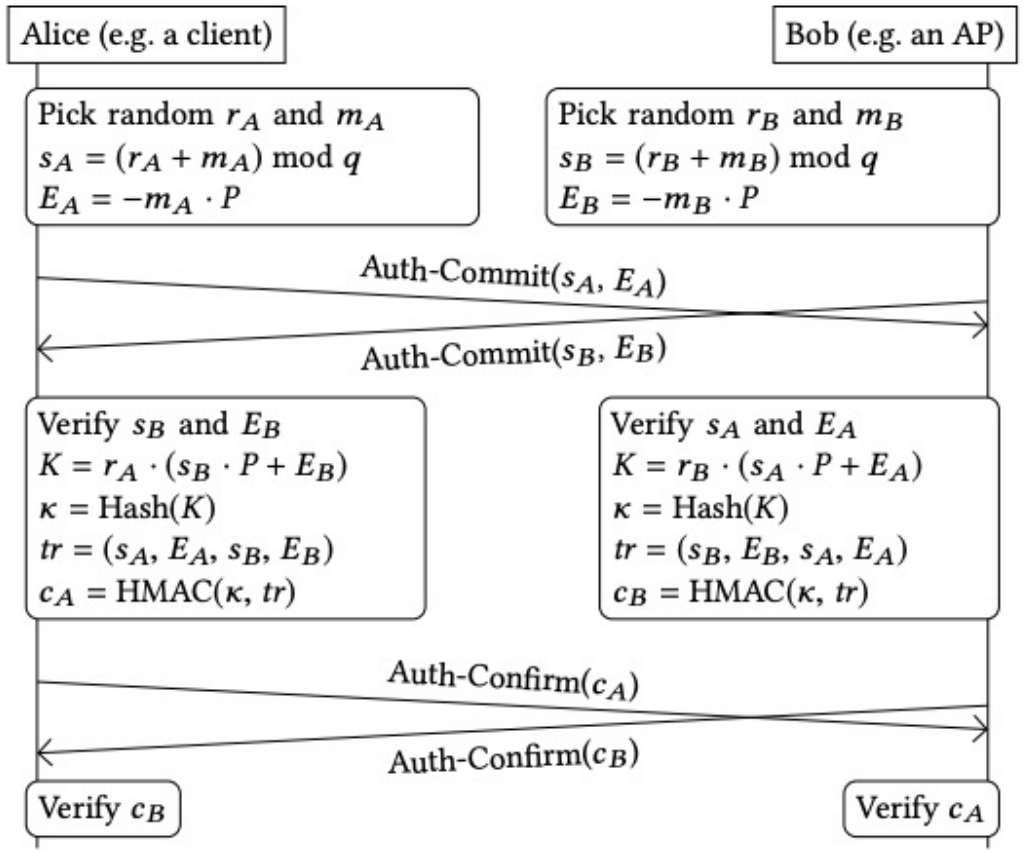


Figure 1: WPA3's SAE handshake. Both stations can simultaneously initiate the handshake, hence the crossed arrows. We assume elliptic curves are used, though similar operations are performed when using multiplicative groups.

Backward compatibility

- Scenario: both WPA2 and WPA3 are supported, and the same password is used
- WPA3 has some detection of downgrade to WPA2 (at changing the AP capabilities in the RSN IE), but this does not help (until detection, a handshake capture already makes the password vulnerable to a dictionary attack in WPA2).

[Source: Vanhoef, M. and Ronen, E., 2020, May. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 517-533). IEEE.]

Other problems

- DoS: spoof commit frames to the AP (the AP will have to do too many verifications)
- Timing attacks, side-channels attacks (mostly caused by how the pre-shared password is encoded into a group element in the Dragonfly handshake)

[Source: Vanhoef, M. and Ronen, E., 2020, May. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 517-533). IEEE.]

Dragonblood (2020)

DRAGONBLOOD

Analysing WPA3's Dragonfly Handshake

By Mathy Vanhoef (NYUAD) and Eyal Ronen (Tel Aviv University & KU Leuven)

INTRO NEW DETAILS PAPER TOOLS Q&A

INTRODUCTION

April 2019 — Modern Wi-Fi networks use WPA2 to protect transmitted data. However, because WPA2 is more than 14 years old, the Wi-Fi Alliance recently announced the new and more secure WPA3 protocol. One of the supposed advantages of WPA3 is that, thanks to its underlying Dragonfly handshake, it's near impossible to crack the password of a network. Unfortunately, we found that **even with WPA3, an attacker within range of a victim can still recover the password**. If the victim uses no extra protection such as HTTPS, this allows an attacker to steal sensitive information such as passwords and emails. We hope our disclosure motivates vendors to mitigate our attacks before WPA3 becomes widespread.

https://wpa3.mathyvanhoef.com/

WiFi Networks

- We have now finished studying WiFi security

Mobile Security

Network Security - Lecture 6

Ruxandra F. Olimid

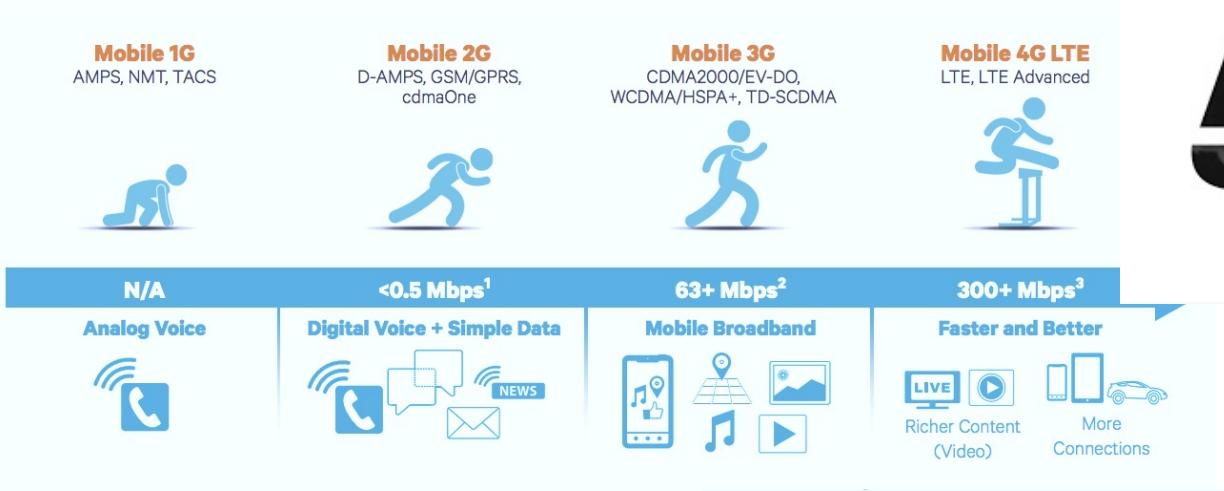
Faculty of Mathematics and Computer Science, University of Bucharest

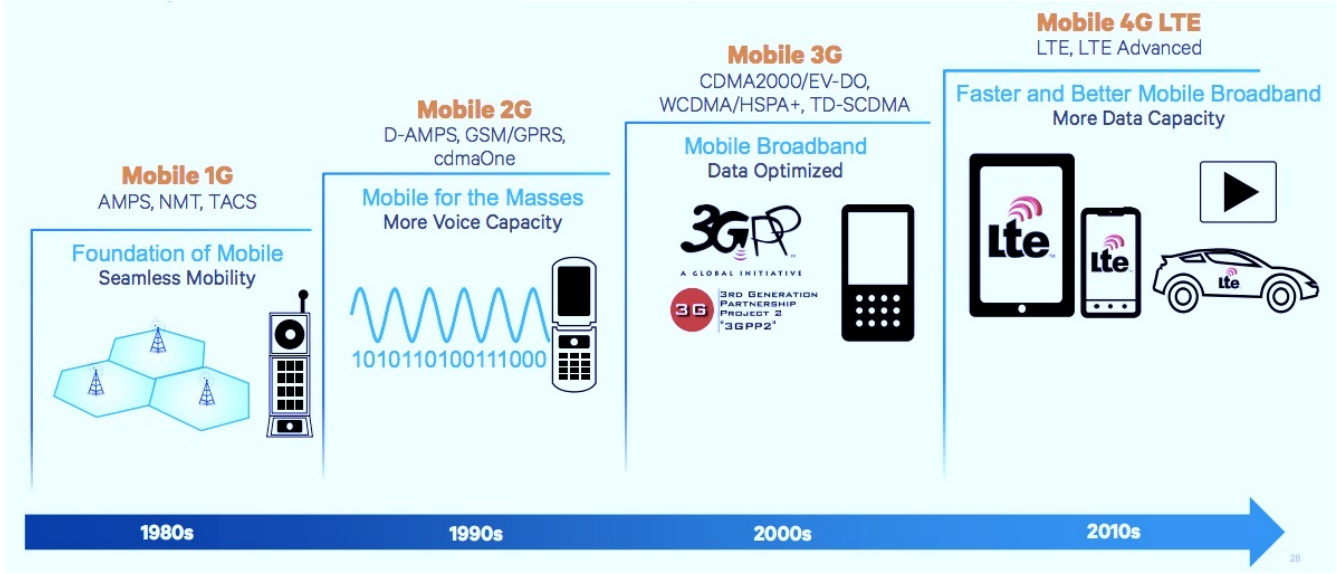
*slides adapted from the course TTM4137 thought at NTNU

Outline

- Intro to Mobile Security
- GSM Architecture
- GSM Security Requirements / Principles
- Vulnerabilities and Attacks

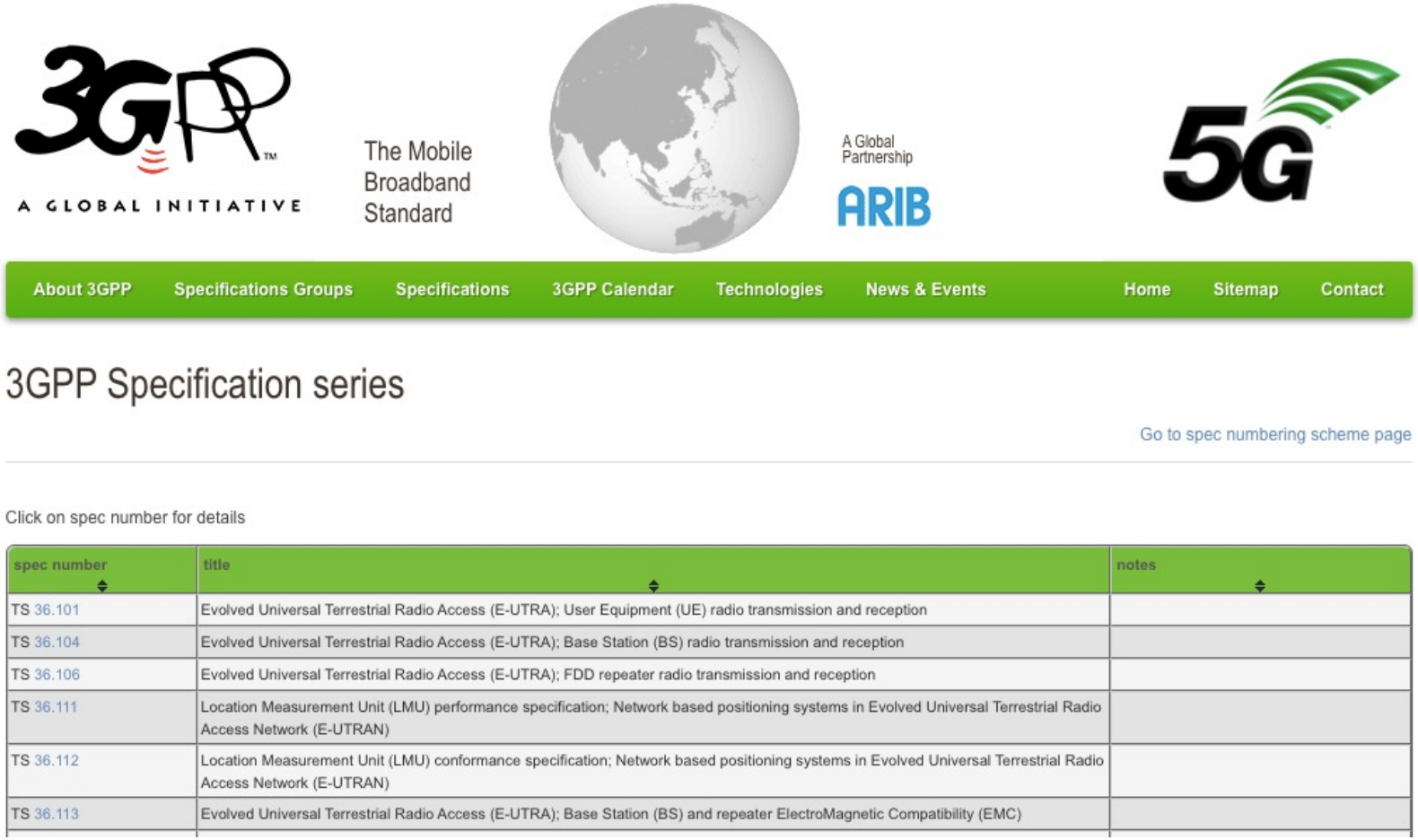
Evolution





[Source: Qualcomm – The Evolution of Mobile Technologies, ’14]

3GPP - Specifications

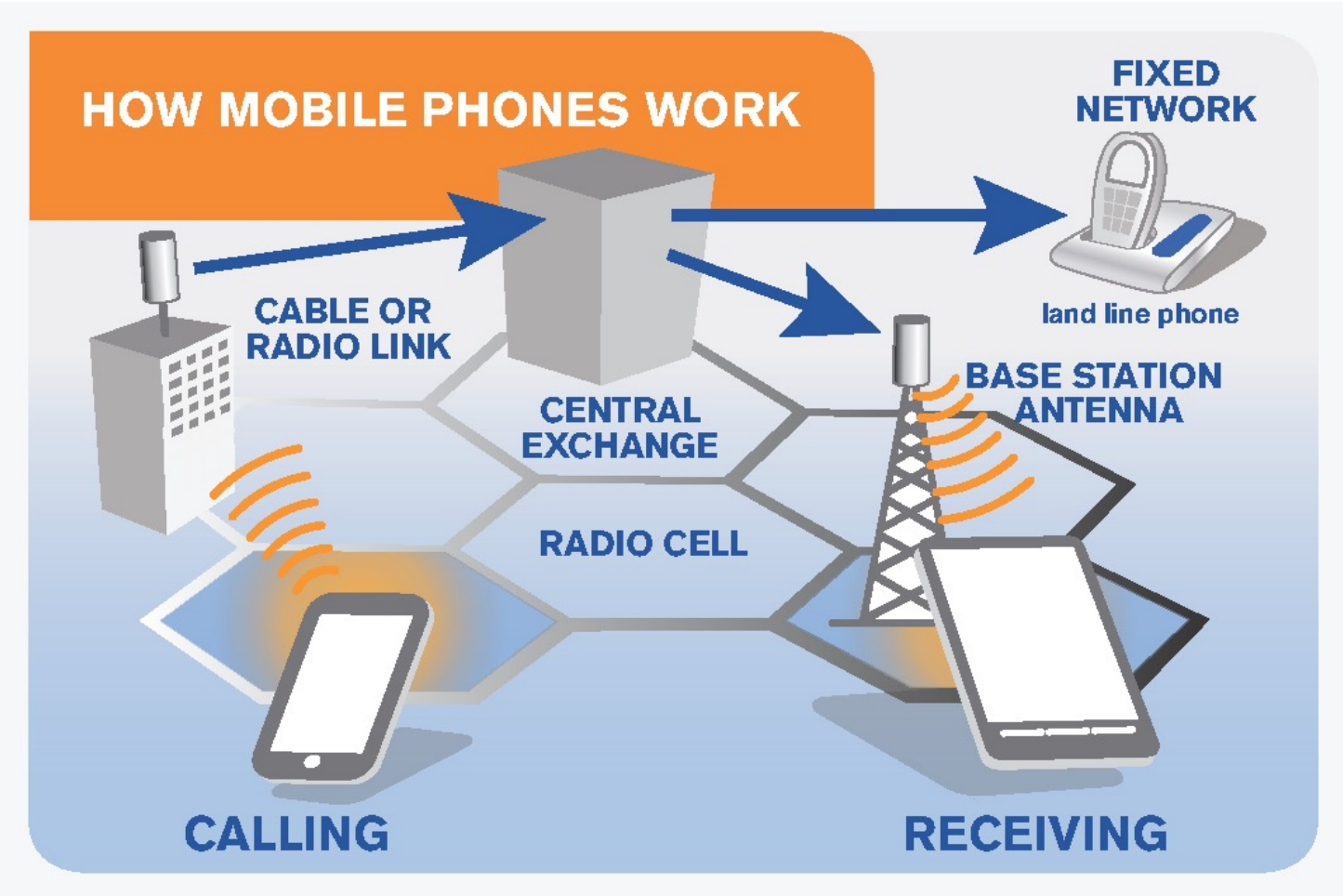


spec number	title	notes
TS 36.101	Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception	
TS 36.104	Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception	
TS 36.106	Evolved Universal Terrestrial Radio Access (E-UTRA); FDD repeater radio transmission and reception	
TS 36.111	Location Measurement Unit (LMU) performance specification; Network based positioning systems in Evolved Universal Terrestrial Radio Access Network (E-UTRAN)	
TS 36.112	Location Measurement Unit (LMU) conformance specification; Network based positioning systems in Evolved Universal Terrestrial Radio Access Network (E-UTRAN)	
TS 36.113	Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) and repeater ElectroMagnetic Compatibility (EMC)	

https://www.3gpp.org/

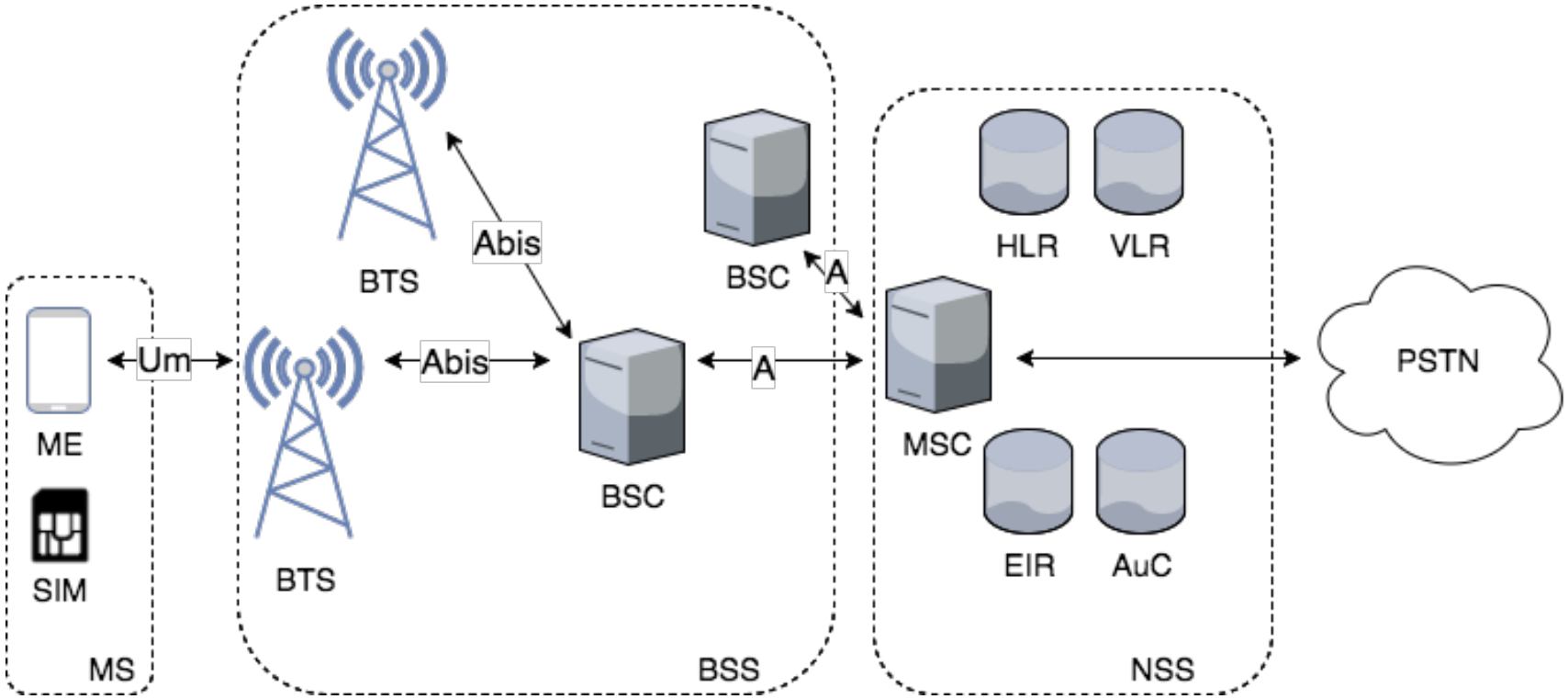
Overview

- User device
- Access network
  - Radio link
- Core network



[Source: ITU EMF Guide http://emfguide.itu.int/emfguide.html]

GSM - Architecture



MS: Mobile Station
ME: Mobile Equipment
SIM: Subscriber Identity Module

BSS: Base Station Subsystem
BTS: Base Transceiver Station
BSC: Base Station Controller

NSS: Network Subsystem
MSC: Mobile Services Switching Center
HLR: Home Location Register
VLR: Visitor Location Register
EIR: Equipment Identity Register
AuC: Authentication Center

PSTN: Public Switched Telephone Network

GSM - Arhitecture

- MS (Mobile Station):
  - Consists in a Mobile Equipment (ME) and the Subscriber's Identity Module (SIM)
- BSS (Base Station Subsystem):
  - Consists in several BTSs and BSCs
  - The BSC is a central element that controls the radio network, maintaining radio connectivity with several BTSs and providing connection to the NSS
  - BTS is the element to which the MS connects to in the GSM network via radio link; its functions include signal processing, signaling, ciphering
- NSS (Network SubSystem):
  - MSC is the main element of the NSS with respect to call functions, being responsible for call control, BSS control, and interconnecting to the external networks (PSTN)

GSM - Arhitecture

- VLR (Visitor Location Register):
  - Stores information about subscribers that are served by the MSC (it maintains copies of the data from HLR, increasing efficiency: decreases the number of messages that are exchanged between the MSC and the HLR)
  - Usually is not independent hardware, but a software component of the MSC
- HLR (Home Location Register):
  - It is the main database in GSM
  - Maintains information for each subscriber: IMSI, phone no. - MSISDN (Mobile Station International Subscriber Directory Number), available services for the subscriber, location, etc.
- AuC (Authentication Center):
  - For each subscriber, stores the permanent key K_i that is also stored in the SIM
  - Generates the authentication vectors (RAND, SRES, K_C) in the authentication phase

GSM - Arhitecture

- EIR (Equipment Identity Register):
  - Keeps inventory of the devices in the mobile network, which are identified by their IMEI
  - Keeps up to date 3 lists:
    - *White list:* contains the equipment that are compliant to the operator and can access the mobile network without any restriction
    - *Black list:* contains the equipment that have been reported as stolen or that have been proved to affect the network functionality, and that are restricted to access the mobile network
    - *Gray list:* contains the equipment that are not fully compliant to the operator, and are allowed to access the network but there are under surveillance

GSM – Security Principles

We will find a similar limitation for LTE, where for example 3GPP did not considered PKI to be a feasible solution

Goal: GSM should be as secure as the wired network (PSTN) …

…but, security mechanisms should not have a negative impact on the usability of the system

- Security requirements in GSM:
- *Access control to the MS:* provide authenticated user access to the mobile station
- *Anonymity of subscribers (privacy):* keep the identity of the subscribers (and their location, possibility of linking calls, etc.) hidden to external parties
- *Authentication of subscribers*: subscribers must prove their identity and their right to access mobile services
- *Confidentiality:* maintain the confidentiality on the radio link

GSM – Security Principles

Weaknesses in GSM security:

- *Breaking Kerckhoffs' principle*: cryptographic algorithms were kept confidential (e.g.: A5/1, A5/2), and their strength was not publicly tested
- *Short keys;* cryptosystems are vulnerable to *exhaustive search attack*
- *Limited encryption:* data is encrypted on the radio link only
- *Unilateral authentication:* The mobile station does not authenticate the network (only the network authenticates the mobile station)
- No specification about the *integrity of the data*
- *Active attacks are possible*; e.g.: IMSI Catchers, when an adversary masquerades a legitimate BTS
- *Users are (usually) not notified about the level of security used*

Mobile Equipment (ME)

- Identification:
  - **IMEI** (International Mobile Equipment Identity), a number used to identify the mobile phone; it is printed on the device, and it can be displayed by dialing *#06#
  - **IMEISV** (IMEI Software Version) discards the check digit from the IMEI and adds 2 digits SVN (Software Version Number)

- Access control:
  - IMEI can be used to deny connectivity to the network for stolen phones based on a blacklist stored by the operator
  - Biometric authentication; e.g.: fingerprint recognition, voice recognition
  - Screen unlock mechanisms; e.g.: codes, patterns

SIM Card

Identification:

- **IMSI** (International Mobile Subscriber Identity), a global unique identifier for the subscriber (≅15 digits)
- **ICCID** (Integrated Circuit Card ID) it is the identifier of the SIM itself and printed on the SIM card

- Access control:
  - **PIN** (Personal Identification Number), a sequence of numbers required to unlock the SIM card
  - **PUK** (Personal Unlocking Key), a code required when the PIN has been introduced incorrectly several times

IMSI (International Mobile Subscriber Identity)

MCC (Mobile Country Code) - 3 digits -	**MNC** (Mobile Network Code) - 2 digits (EU) / 3 digits (US) -	**MSIN** (Mobile Subscriber Identification Number)
242 (Norway)	01 (Telenor) / 02 (Telia)	XXXXXXXXXX
226 (Romania)	01 (Vodafone) / 10 (Orange)	XXXXXXXXXX

List of MCCs and MNCs: http://mcc-mnc.com/

SIM Card

Authentication and Confidentiality:

- **IMSI** (International Mobile Subscriber Identity)
- **TMSI** (Temporary Mobile Subscriber Identity), a temporary identity used to restrict the sending of IMSI over the air and mitigate eavesdrop attacks
- **K_i** a 128-bits permanent key
- Cryptographic mechanisms: a *challenge-response mechanism* that uses the permanent key for the authentication of the subscriber and a *key generation mechanism* for confidentiality of communication

SIM cards must be *tamper-resistant* (i.e. an adversary should not be able to read / modify the security information stored on the SIM card). Otherwise, SIM cards become vulnerable to *cloning attacks*, for which the attacker creates copies of the SIM card to use in different purposes (eavesdropping on the victim, making calls on the victim behalf, etc.)

*Terminology: Initially, the card itself was also called a SIM, later the card itself was called UICC (Universal Integrated Circuit Card) and the SIM was considered the application running on the card

Anonymity of Subscribers

- Goal: Keep the identity (presence/absence in an area, location, etc.) of the subscriber private to unauthorized parties

- A subscriber can identity itself by one of the following identifiers:
  - **IMSI** - permanent identity
  - **TMSI** - temporary identity

- Principles:
  - Introduce the TMSI as a way to avoid IMSI exposure on the radio interface
    - e.g.: IMSI uniquely identifies a subscriber, and if it intercepted it suffice to prove the presence of the subscriber in a location
  - TMSI is assigned to the MS when authenticates to the network, and it is local in the visiting network (VLR keeps the IMSI – TMSI correspondence); the MS stores the TMSI in the SIM to use it even after rebooting
  - TMSI must be renewed at specific intervals (tradeoff with efficiency); a TMSI that is not changed often enough can break privacy too

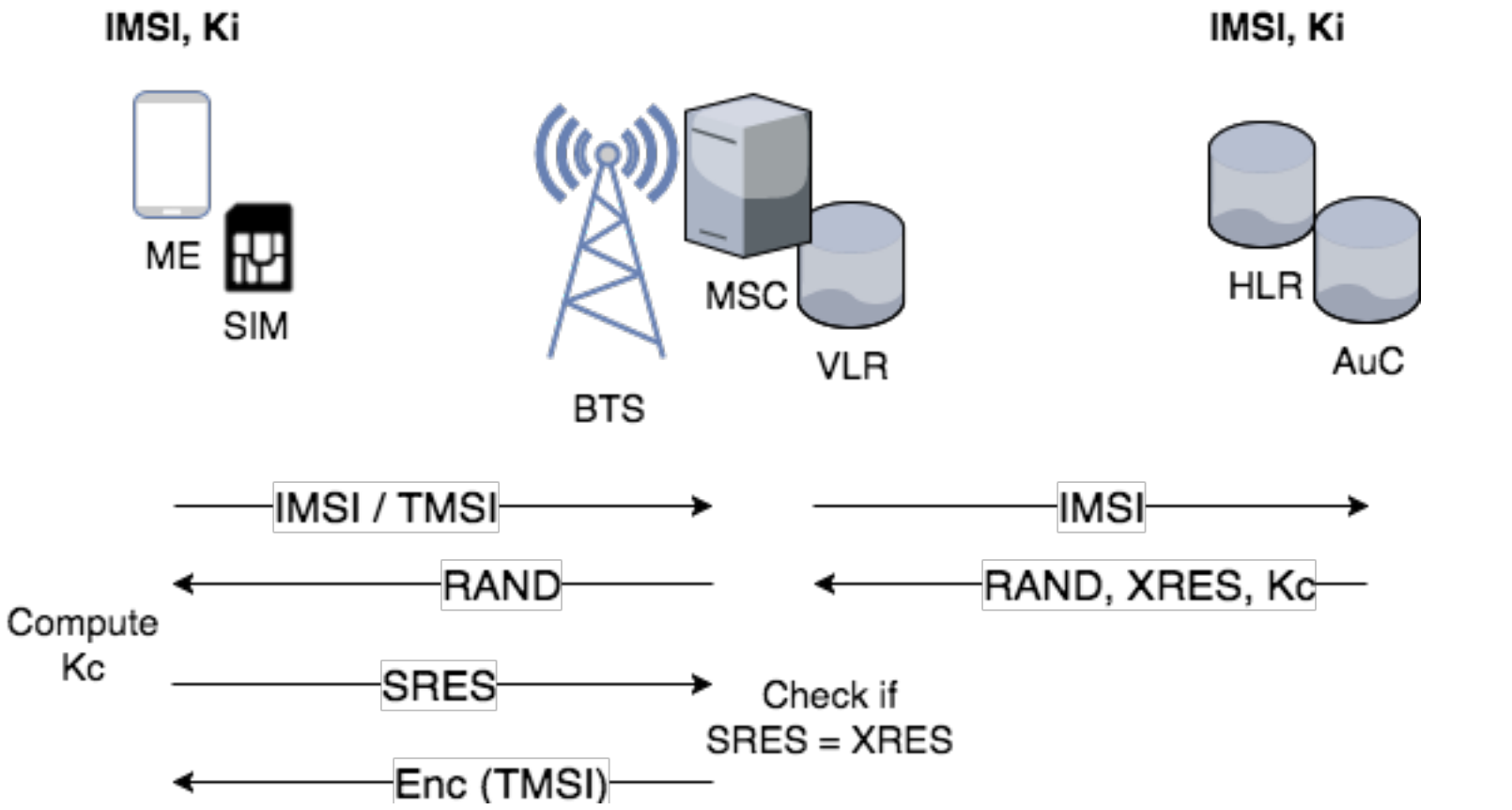
Authentication of Subscribers

- Goal: Prove the identity of the subscriber to the mobile network, and avoid unauthorized parties to access the mobile services

- The authentication mechanism uses:
  - The permanent key **K_i** , unique for each subscriber, that is stored:
    - in the SIM card (**subscriber's side**)
    - in the AuC (**network operator's side**)
  - Cryptographic algorithms: **A3** (subscriber authentication), **A8** (key generation)

- Principles:
  - K_i does never leave the 2 locations (SIM, AuC);
  - Authentication consists in checking if the subscriber knows the correct key K_i by using a *challenge-response mechanism*
  - The serving network does not have access to the key K_i, so it cannot perform authentication without help from the home network
  - During authentication phase, is derived a key K_c that will be later used for encryption

Authentication of Subscribers



$Kc = A8(K_i, RAND)$

$SRES / XRES = A3(K_i, RAND)$

Authentication Triplets

- Goal: Allow the visiting network to authenticate the MS without knowing K_i and improve efficiency by using batches of triplets

- A triplet used for authentication is

$$(RAND, XRES, K_c)$$

where $XRES = A3(K_i, RAND)$ and $Kc = A8(K_i, RAND)$

- Operation:
  - AuC produces batches of triplets for each MS, each with a different RAND and sends them to the HLR
  - For a single request, the VLR receives a batch of triplets from the HLR (to avoid often communication between the VLR and the HLR)
  - If the network runs out of triplets, it should request more from the HLR, but if not it is allowed to reuse triples

Encryption

- Goal: Encrypt all communication between the mobile station and the BTS (both phone calls and sensitive signaling information such as TMSI, MSISDN, etc.)

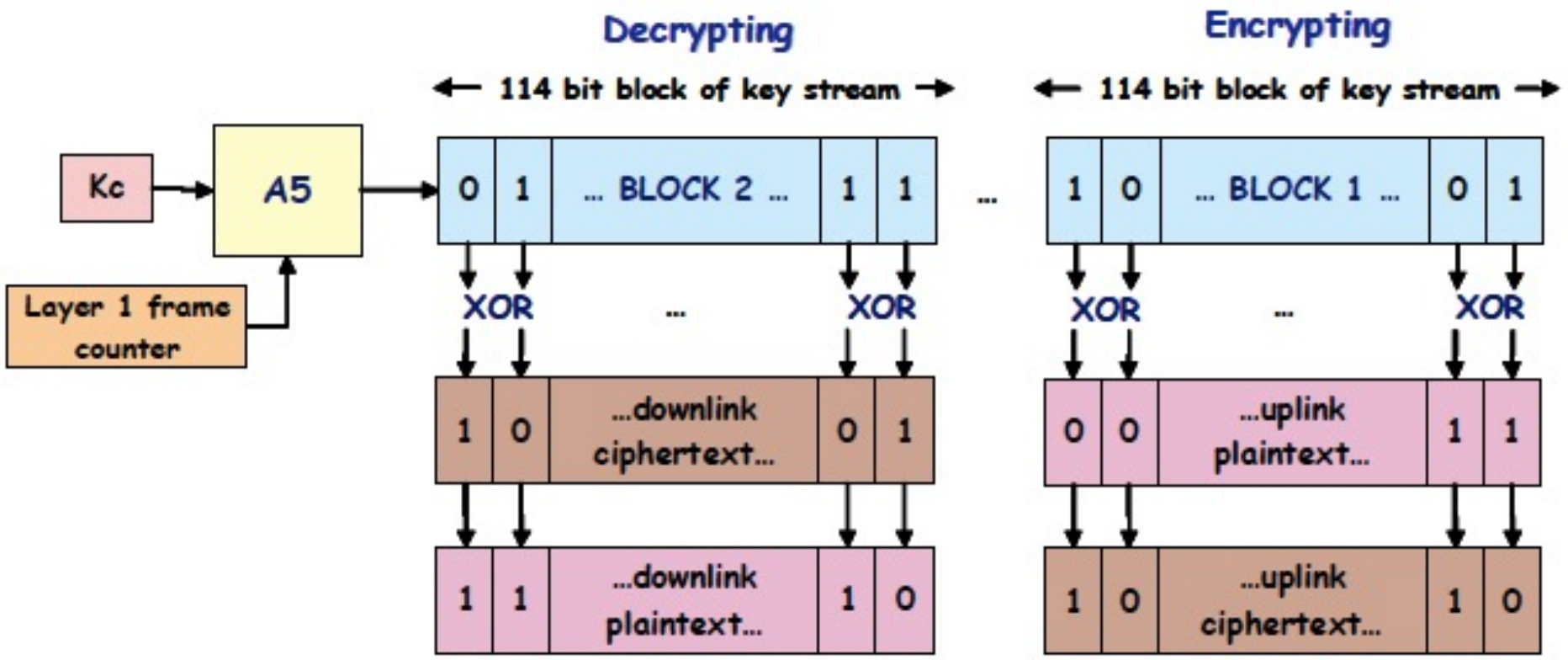
- The GSM encryption uses:
  - The key $\mathbf{K_c}$, derived in the authentication mechanism
  - Encryption algorithm: **A5** (radio encryption)
- Principles:
  - Encryption is only performed on the radio link (!)
  - The encryption algorithm uses as input the session ley K_c derived from the authentication phase
- Operation:
  - The key K_c is used as the encryption key for a stream cipher (LFSR-based):

$$\text{Ciphertext} = A5(K_c, \text{Plaintext})$$

Encryption

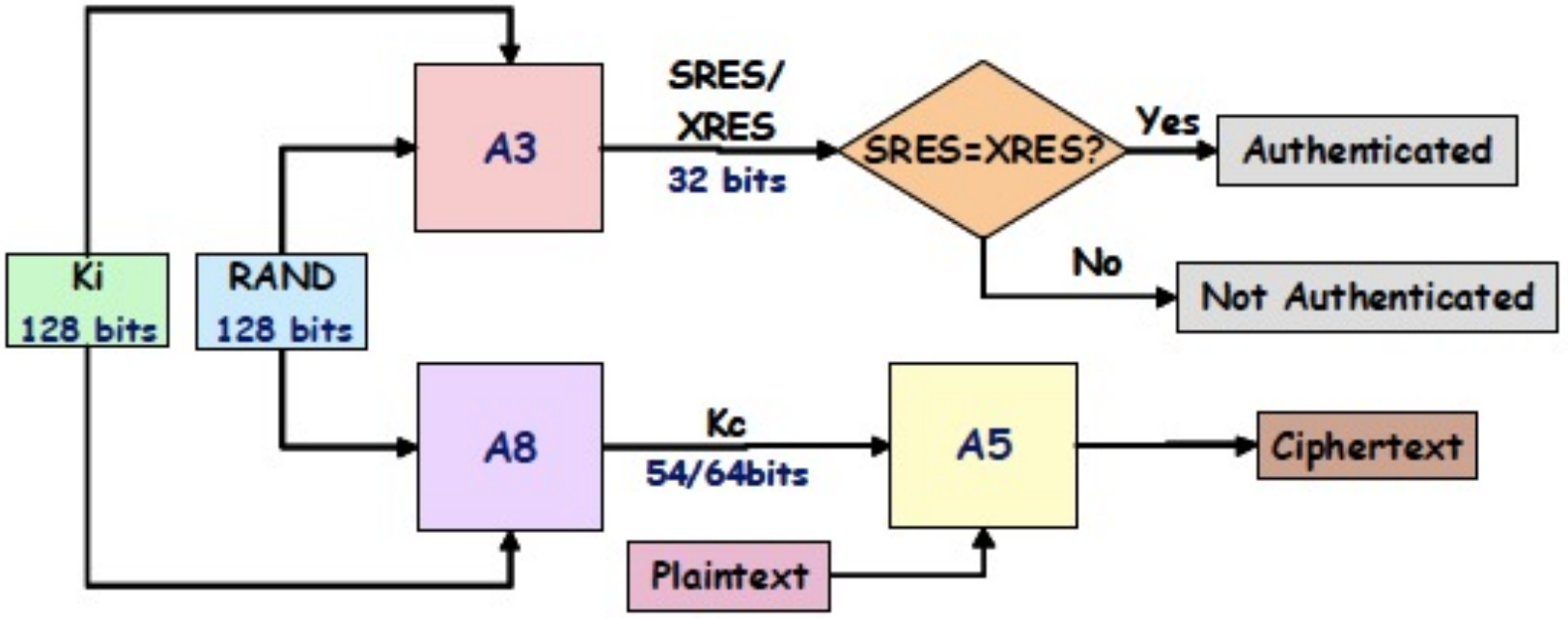
- Both A5/1 and A5/2 were not public, breaking *Kerckhoffs' principle*
- Encryption operates at the physical layer (Layer 1), which brings some advantages:
  - Maximum amount of data is encrypted (both user and signaling data)
  - The encryption algorithm can be implemented in hardware
- A5 algorithms are **stream ciphers**, so encryption is performed bit-by-bit
- A *frame counter* (22 bits) is used as an additional input together with the key K_c
- Vulnerability! The frame counter repeats every 2^{22} frames (approx. every 3.5 hours), so the key stream repeats if the K_c is not renewed meanwhile
- GSM is *full duplex*: for each frame, first 114-bit block (Block1) is used for encryption of data that is being transmitted, and the second 114-bit block (Block2) is used for decryption of data that is being received

Encryption



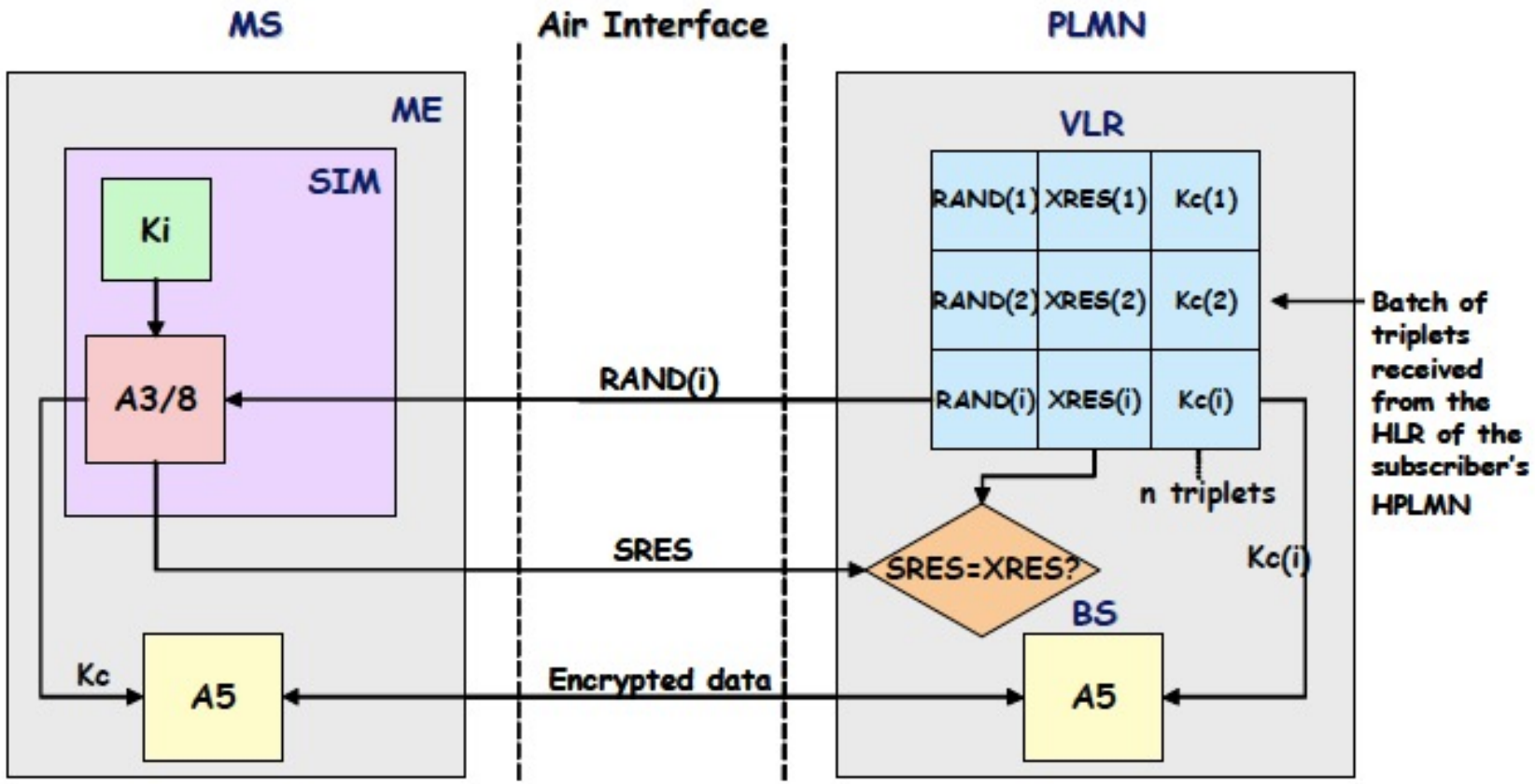
[Source: P.S.Pagliusi – A Contemporany Foreword on GSM Security, InfraSec '02]

Overview



[Source: P.S.Pagliusi – A Contemporany Foreword on GSM Security, InfraSec '02]

Overview



[Source: P.S.Pagliusi – A Contemporany Foreword on GSM Security, InfraSec '02]

Crypto

Key	Length / Input + Output	Info
K_i	128 bits	Key shared between the subscriber and the network operator, stored in the SIM and AuC
K_c	54/64 bits	Secret session key, that will be used for encryption Kc = A8(K_i, RAND)
RAND	128 bits	Random challenge
SRES / XRES (Signed Response / Expected Response)	32 bits	Response to the challenge request / Expected response to the challenge request SRES / XRES = A3(K_i, RAND)
A3, resp. A8	Input: K_i, RAND Output: SRES, resp. K_c	Generic algorithms for authentication, resp. key generation (no specific algorithms) e.g.: COMP128 combines A3 and A5 and generates XRES (32 bits) and K_c (54 random bits concatenated to 10 bits of 0) Stored in the SIM
A5	Input: Kc, plaintext Output: ciphertext	Class of standardized encryption algorithms: A5/0 (no encryption), A5/1 (CEPT + USA), A5/2 (Asia), A5/3 (Kasumi, UMTS) Stored in the mobile equipment (not SIM!)

Security Principles

- Modularity:
  - GSM is modular in the sense that the cryptographic algorithms can be replaced with others, as long as maintain the same input-output structure
  - A5 refers to a family of algorithms; e.g.: A5/1, A5/2, A5/3 (64 bits key K_c); A5/0 (no encryption), A5/4 (128 bits key K_c) – some used for UMTS (e.g.: A5/3)

- Standardization:
  - A5 must be standardized (e.g.: MS must communicate to BTS in roaming)
  - A3, A8 must not necessary be standardized, because both parties involved (the SIM and the AuC) belong to the same network operator; however, 3GPP gave an example algorithm set TS55.205

[ETSI TS 155 205 V9.0.0 (2010-02): link]

Security Principles

- Use the SIM as a security module:
  - Authentication and confidentiality are performed based on a shared secret (K_i)
  - The SIM stores secret information of the subscriber (K_i, IMSI) and cryptographic algorithms (A3, A8)
  - Should be tamper-resistance
- Security in the visiting network:
  - The key K_i must not be shared to the visitor network
  - Authentication triplets allow authentication in visitor networks
- Algorithms' requirements:
  - Statistically impossible to guess SRES
  - Statistically impossible to find K_i, K_c from the eavesdropped data
  - … (assumptions that exclude trivial attacks)

Vulnerabilities and Attacks

- Passive attacks:
  - The adversary eavesdrops on the radio link and gets the IMSI
  - The attack is possible because the IMSI is sent in clear over the radio link when the MS posses no TMSI or it cannot be identified by using the TMSI

- Active attacks:
  - The adversary requests the IMSI from the MS
  - **IMSI Catcher**: the adversary masquerades a legitimate BTS and asks the MS for the IMSI
  - The attack is possible because the MS does not authenticate the network - and cell reselection criteria is signal strength
  - We will learn more on IMSI Catchers when we will study LTE

Vulnerabilities and Attacks

- Cryptanalysis:
  - **Key length**
    - the key length of K_c (54/64 bits) is too small to provide security
    - *Exhaustive search (brute force)* can break the key in a few hours
  - **COMP128** was cracked in 1998 (by Wagner and Goldberg, but apparently known before by some operators)
    - *Chosen plaintext attack*: K_i is found when about 16000 pairs RAND-SRES are collected
    - Possible ways to connect RAND-SRES pairs:
      - Steal the SIM and connect to a phone emulator (2 to 10 hours, dependent on the phone)
      - Use a false BTS (longer in time, but does not require physical access to the SIM)

Vulnerabilities and Attacks

- Cryptanalysis:
  - **A5/1** was broken in 1999 (by Biryukov, Shamir, later the attack was improved together with Wagner)
    - *Time-memory trade-off*:
      - *Pre-processing phase*: Compute a large database of states and related keys of the stream system
      - *Attack phase*: search subsequences of the key stream in the database; if a match is found, the state is the one in the database (with high probability)
      - 2s of known plaintext (both uplink and downlink) to succeed
  - **A5/2** was cryptanalysed in 1999 (Goldberg, Wagner, Green), 2003 (Barkan, Biham, Keller), etc.

Vulnerabilities and Attacks

- Radio links:
  - BTS to BSC link is sometimes not wired, making it easily susceptible to eavesdropping
  - Possible because GSM security do NOT consider encryption beyond the BTS-BSC link (but only on the MS – BTS radio link)

- Engineering attacks:
  - Attacks against the chip card, side-channel attacks
  - Software attacks

- Optionality:
  - Encryption was introduced as an optional feature
  - Very few terminals inform the user if encryption is taking place or not

To remember!

1. Apply Kerckhoffs' principle (make crypto public!)
2. Think about the future (e.g.: do not use small cryptographic keys, think about Moore's law!)
3. Trade-off between efficiency / usability and security might expose vulnerabilities
4. Do not underestimate your adversary! (active attacks were considered infeasible)
5. New notions: security aspects in GSM network

Mobile Security

Network Security - Lecture 7

Ruxandra F. Olimid

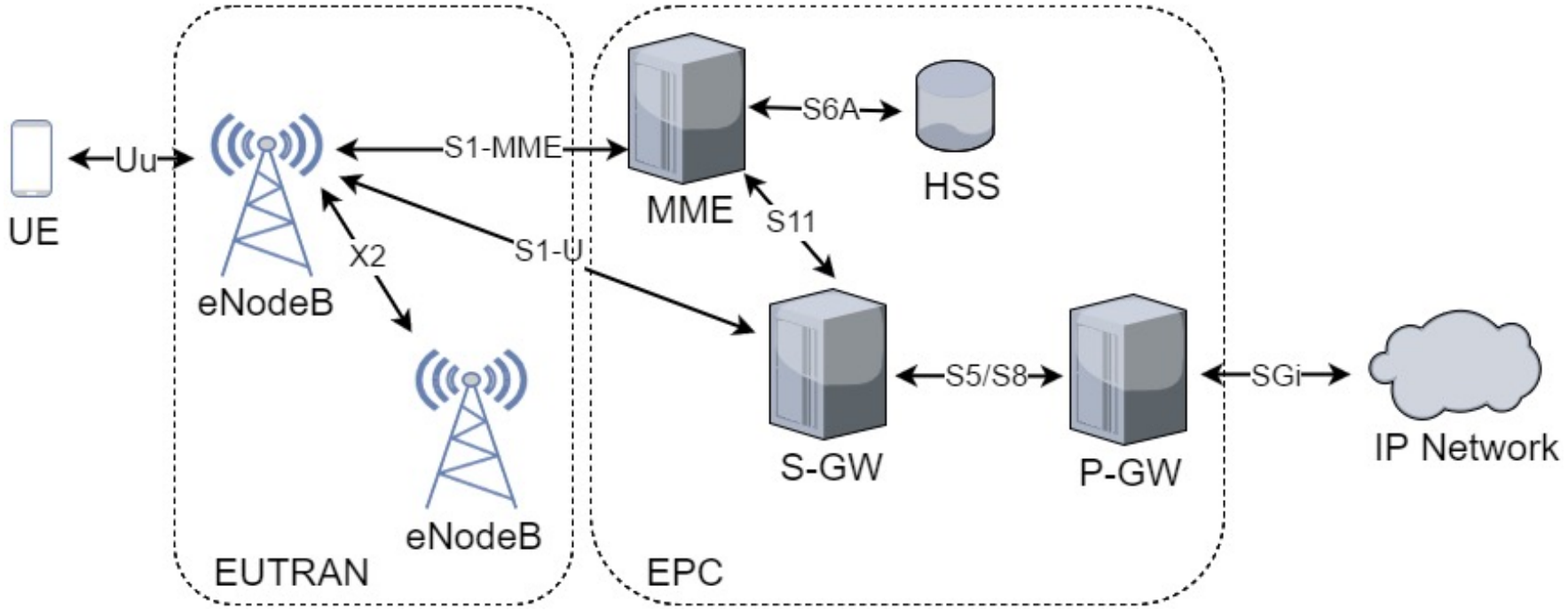
Faculty of Mathematics and Computer Science, University of Bucharest

*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

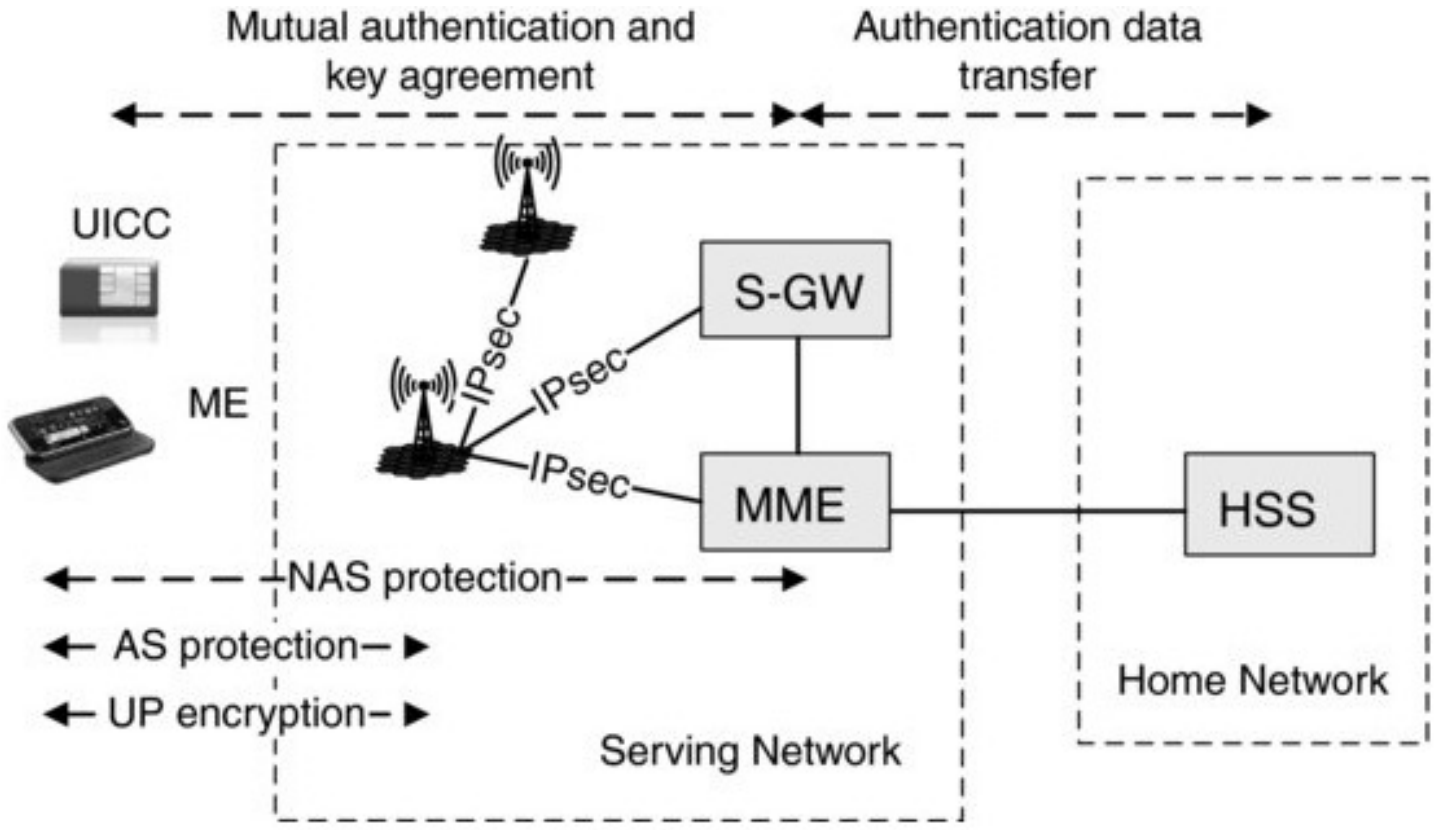
EPS Security Architecture

- 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



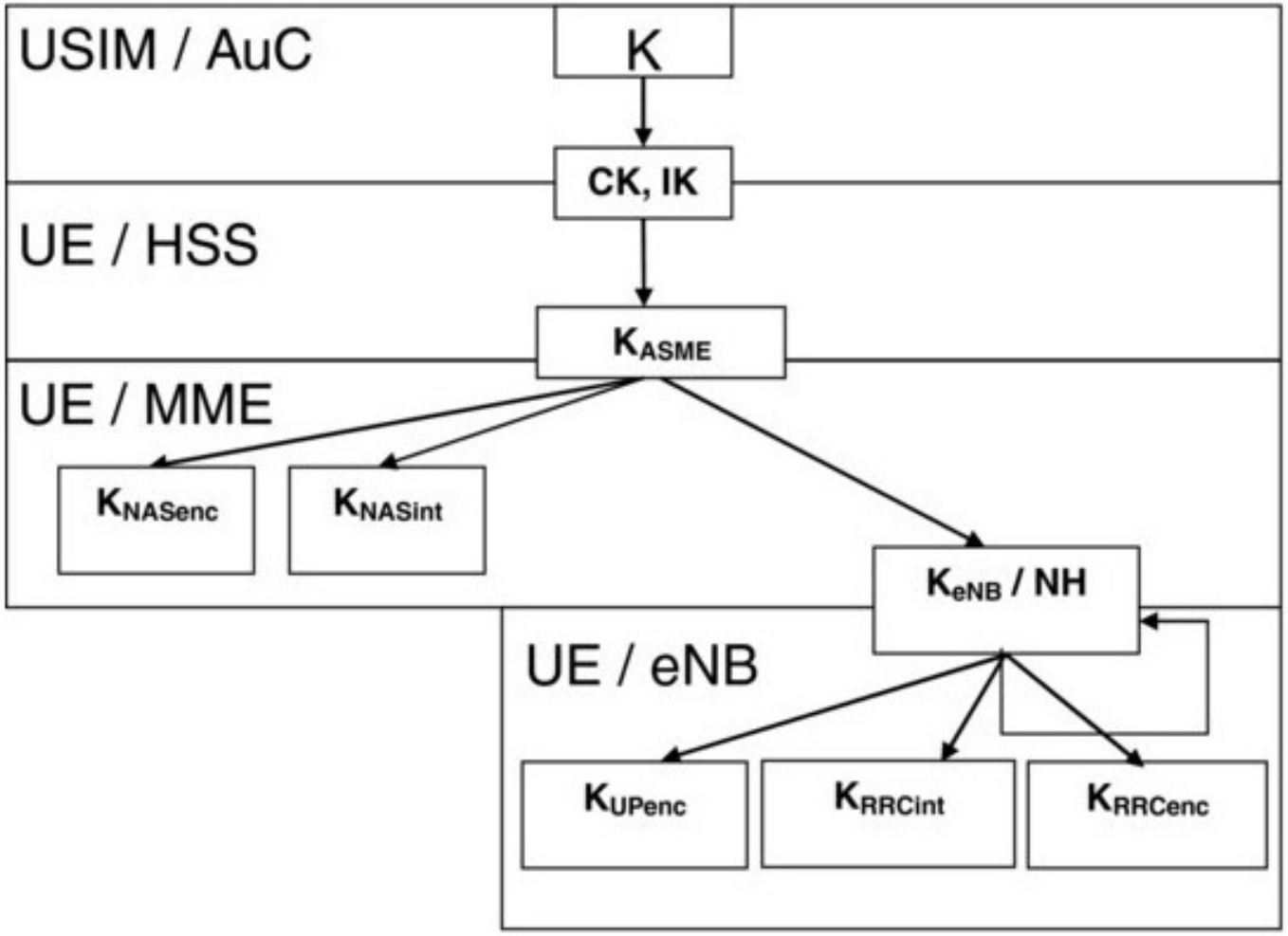
[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

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

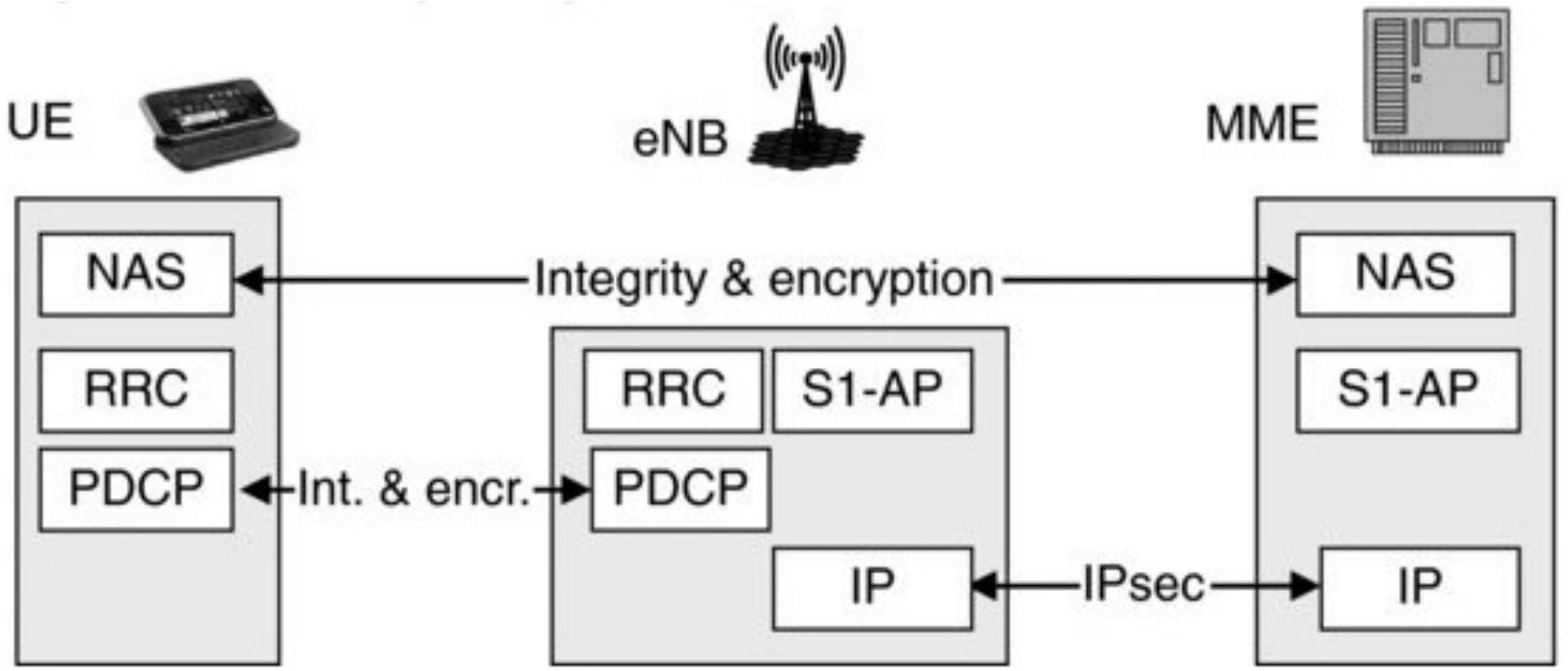


[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

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



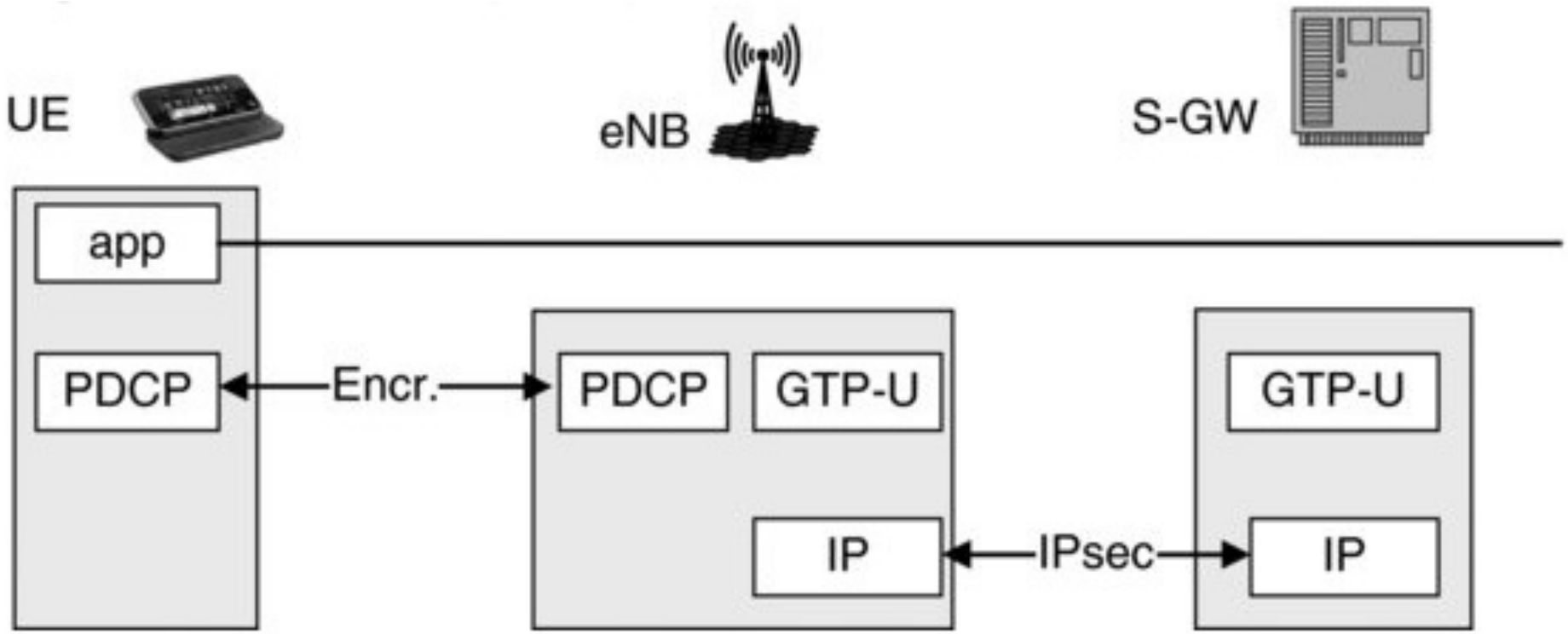
NAS: Non-Access Stratum
RRC: Radio Resource Control
PDCP: Packet Data Convergence Protocol
IP: Internet Protocol

[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)

Mobile Security – LTE (cont.)

Network Security - Lecture 8

Ruxandra F. Olimid

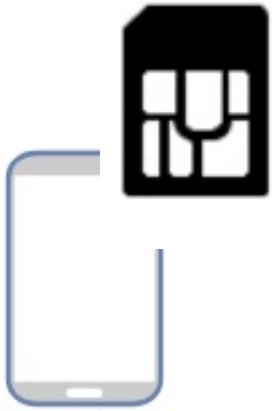
Faculty of Mathematics and Computer Science, University of Bucharest

*slides adapted from the course TTM4137 thought at NTNU

Outline

- UE Identification
- EPS AKA
- Key hierarchy (again)
- Cryptographical aspects
- AS / NAS Protection

UE Identification



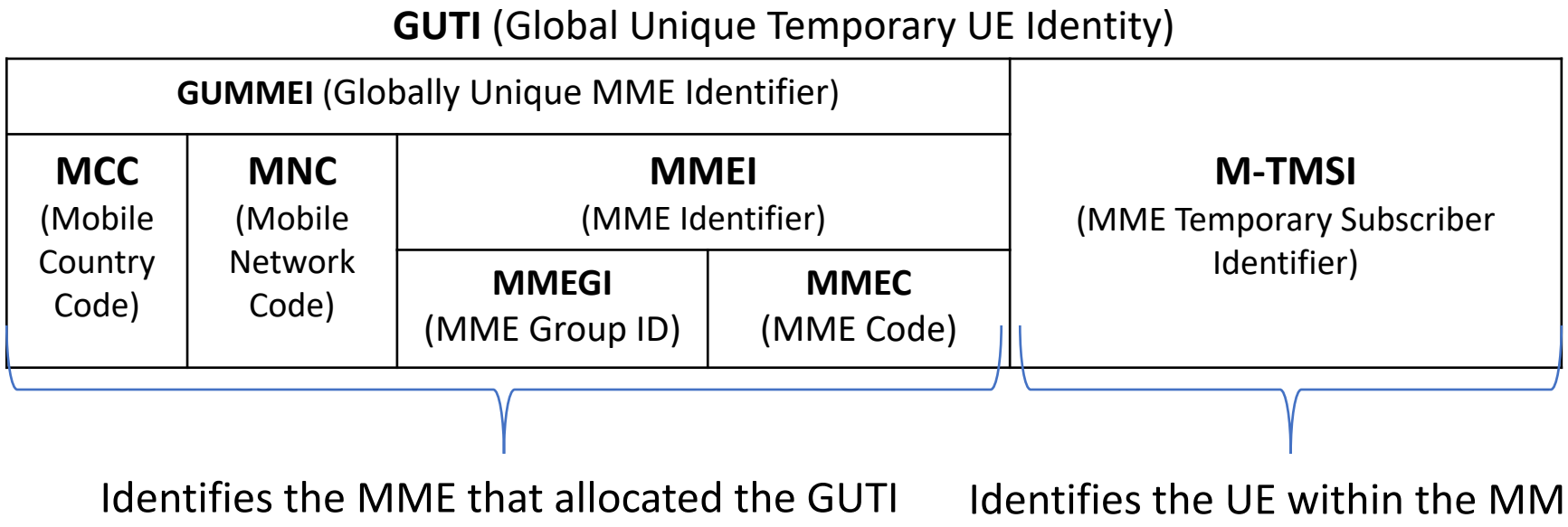
- Similar to identification in GSM and UMTS
  - **IMSI**
  - **IMEI , IMEI SV**

- **GUTI (**Global Unique Temporary UE Identity**),** allocated to provide user identity confidentiality
  - Similar to TMSI in GSM

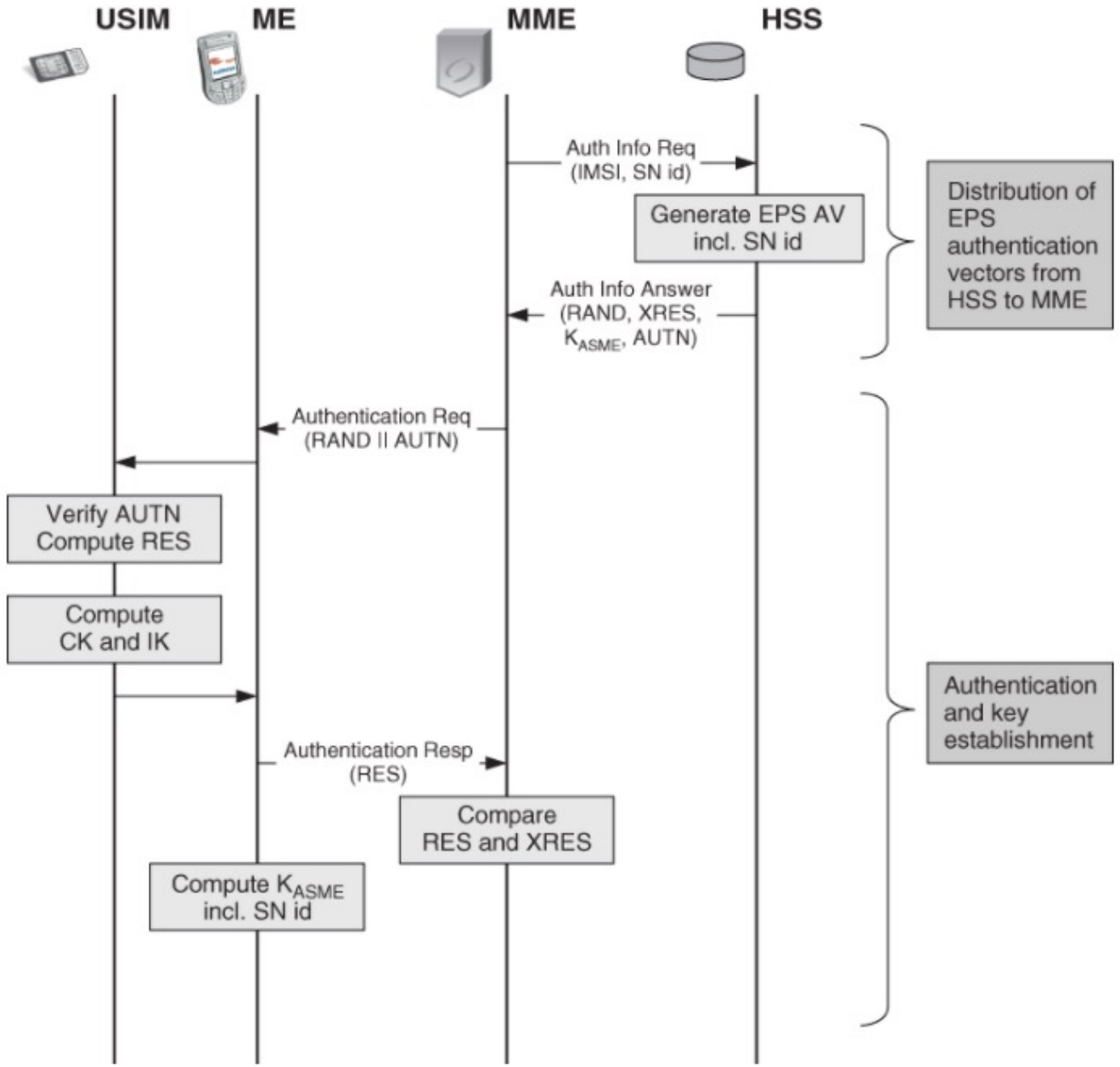
- **C-RNTI** (Cell Radio Network Temporary Identifier) with security role in handover preparation

UE Identification

- MME assigns a GUTI to the UE in `Attach Accept` or `Tracking Area Update Accept` messages
- MME can also assign GUTI in a separate `GUTI Reallocation` procedure



EPS AKA



SN id: Serving Network Identity
AV: Authentication Vector
AUTN: Authentication Token
RES: Response
XRES: Expencted Response
CK: Ciphering Key
IK: Integrity Key
ASME: Access Security Management Entity

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

EPS AKA – Network side

- The recommendation is to send a single AV at a time (not more)…
  … because the need to request fresh AV is reduced due to the existence of the K_{ASME}, which is not exposed as the CK and IK were exposed in UMTS

- Precomputed AV are not longer used when the UE moves to another network...
  ... because the SN id is input to the KDF

- Each AV is used only once

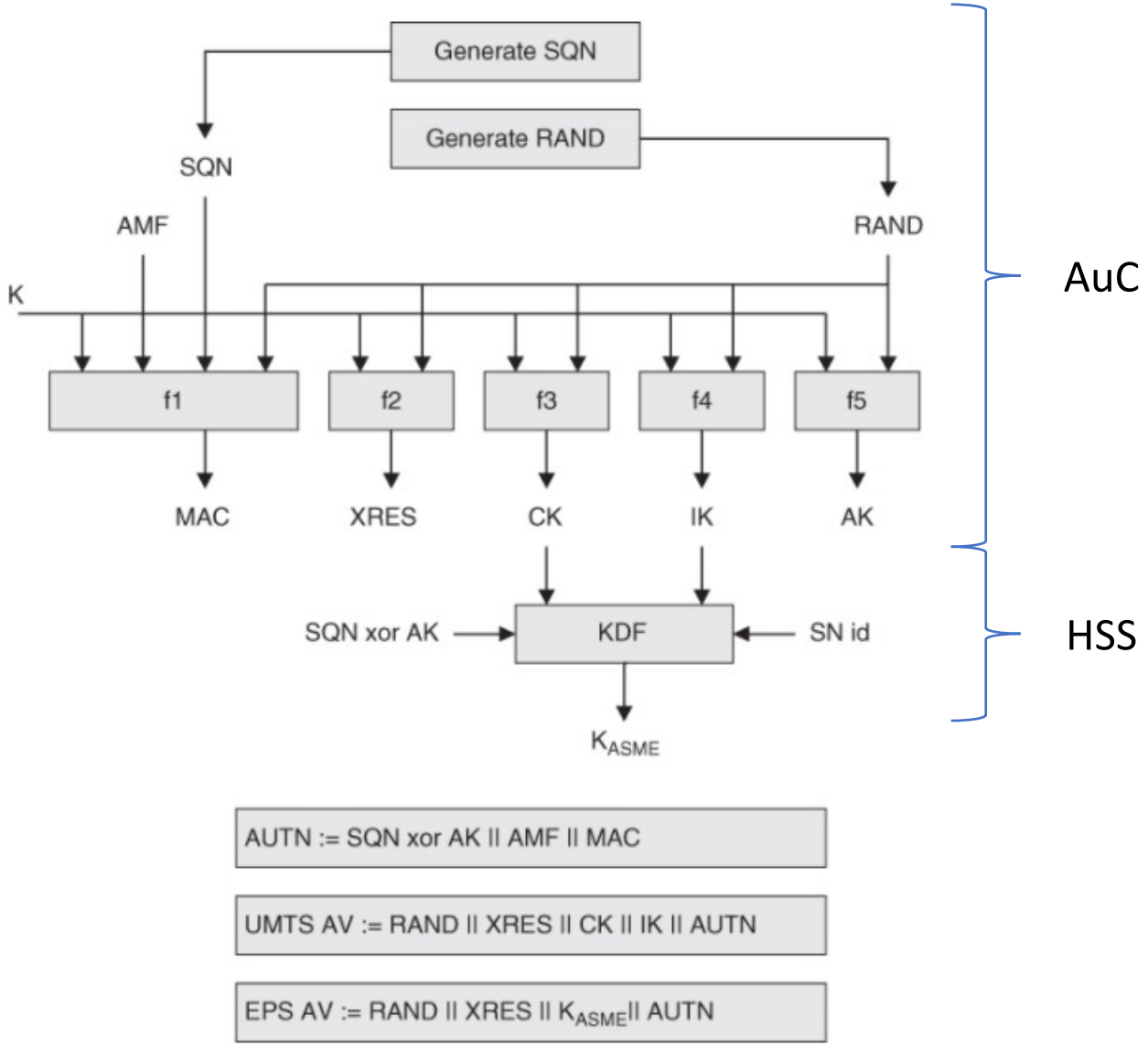
- CK and IK do not leave the HSS

- Operator specific: if AK=0, then AK XOR SQN = SQN (if the operator decides no need for concealment of SQN is required)

EPS AKA – Network side

UMTS AV:
(RAND, XRES, CK, IK, AUTN)

EPS AV:
(RAND, XRES,K_{ASME}, AUTN)



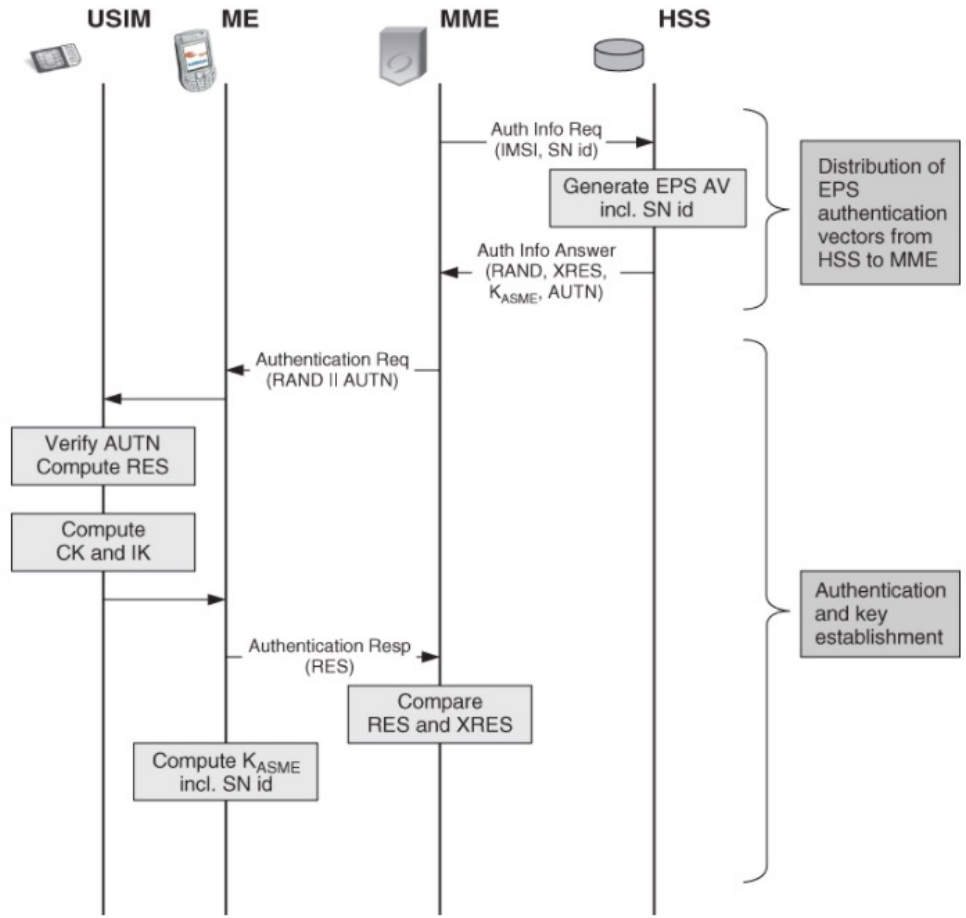
[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

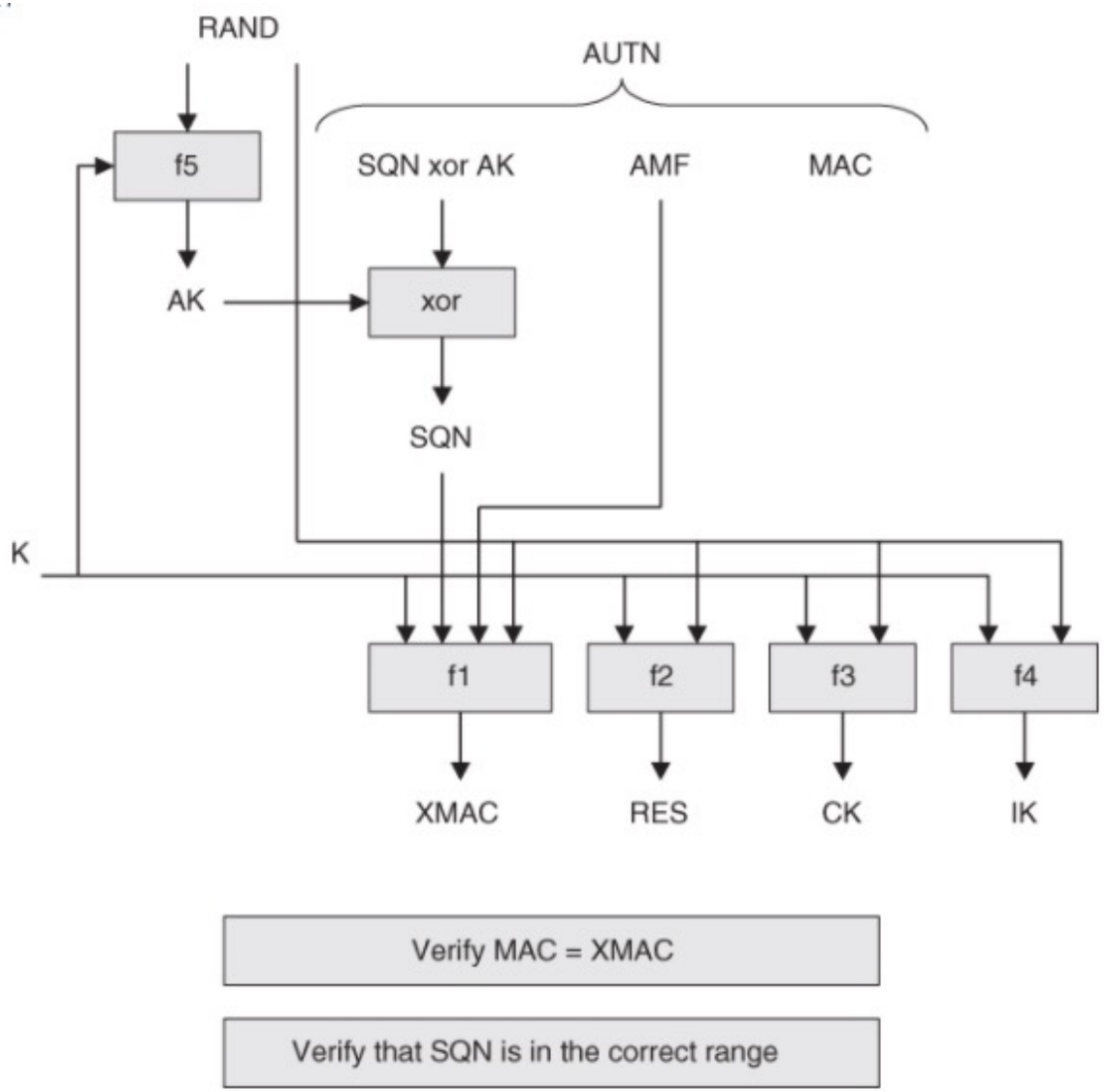
AMF: Authentication Management Field
AK: Anonymity Key

EPS AKA – Network side

- Both UMTS and EPS authentication vectors are generated
- The AuC generates the AVs in exactly the same way as for UMTS
- The HSS derives the K_{ASME} from CK and IK
- The AuC generates fresh SQN and unpredictable random RAND
- AMF (Authentication Management Field):
  - Indicates the algorithm used to generate a particular auth vector when several exist
  - Sets threshold values for key lifetimes
  - First bit is set to 1 to mark that the AV is for EPS use (this should be checked in the MME)

EPS AKA – User side





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

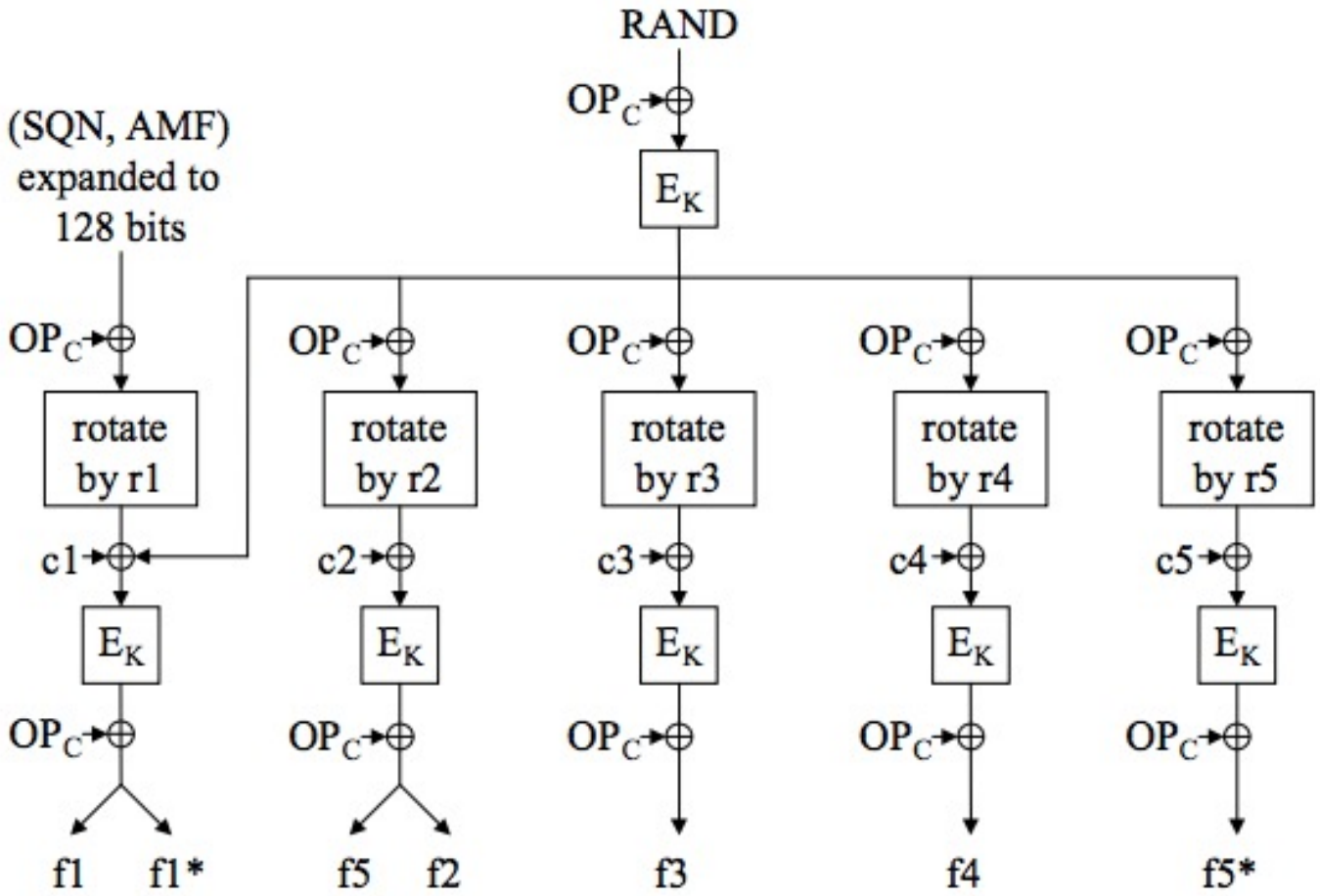
EPS AKA – User side

- SQN verification has not been standardized (generation and verification takes place in the home network, so it can be operator specific)
- Requirements for SQN:
  - No SQN should be used twice: USIM should not accept 2 AUTN with the same SQN after AUTN was verified
  - Allow, in a given threshold, out of order SQN numbers
    (might not accept a SQN if the jump from the last one is too big)
  - Reject too old time-based SQN
- Verification is performed in the USIM

An example: MILENAGE

OPc: Operator variable derived (128 bits)
r1…r5: fixed rotations constants
c1…c5: fixed addition constants
E_K: encryption with they K

Note: f1*, f5* used in case sync.failure at auth. (see Sect.7.2.3, Auth.failures) in the book

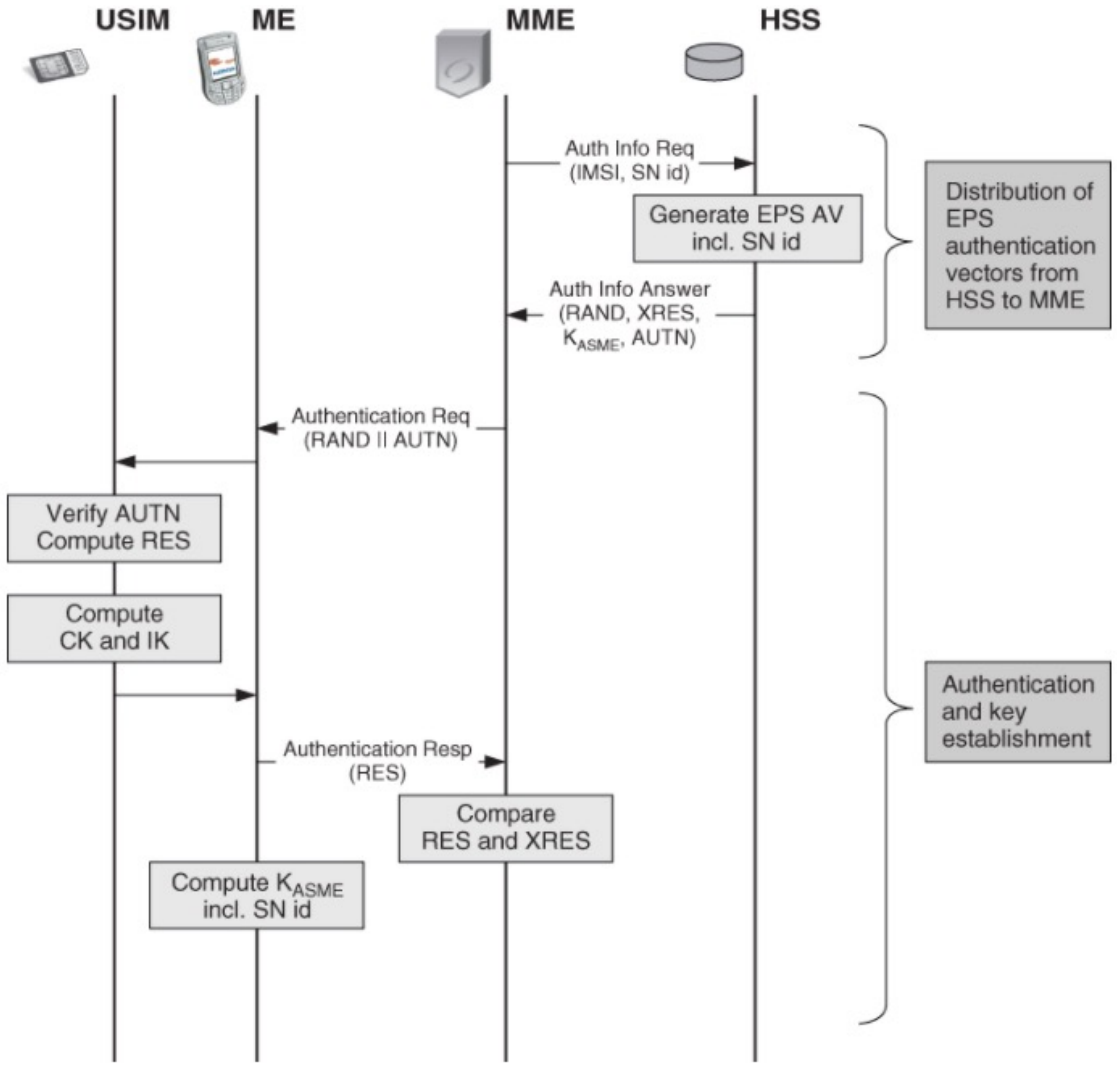


Definition of f1, f1*, f2, f3, f4, f5 and f5*

f0	the random challenge generating function;
f1	the network authentication function;
f1*	the re-synchronisation message authentication function;
f2	the user authentication function;
f3	the cipher key derivation function;
f4	the integrity key derivation function;
f5	the anonymity key derivation function.
f5*	the anonymity key derivation function for the re-synchronisation message.

[Source: ETSI TS 135 205 V13.0.0 (2016-01)]

EPS AKA – User side



- If USIM supports GSM, then it converts (CK, IK) to a GSM key K_c and sends it the the ME

Handover and Roaming

- When the UE changes MME, it identifies itself by GUTI in the `Attach Request` and `Tracking Area Update Request`

- The MME is unaware of the GUTI, so it has 2 possibilities:
  - *Request the IMSI* – breaks confidentiality!
  - *Ask the old MME to translate the GUTI to IMSI*

- Data exchanged between the old and the new MME in 2 scenarios:

  - *Old and new MME are in the **same** network (*Handover*)*
    - Transfer the EPS security context*
    - The old MME transfers the remaining AVs (if any)
  - *Old and new MME are in **networks of different operators** (*Roaming*)*
    - The current security context* is allowed, depending on the security of the networks (EPS to EPS only)
    - The old MME does not transfer the remaining AVs (if any), because they are not good in the new network

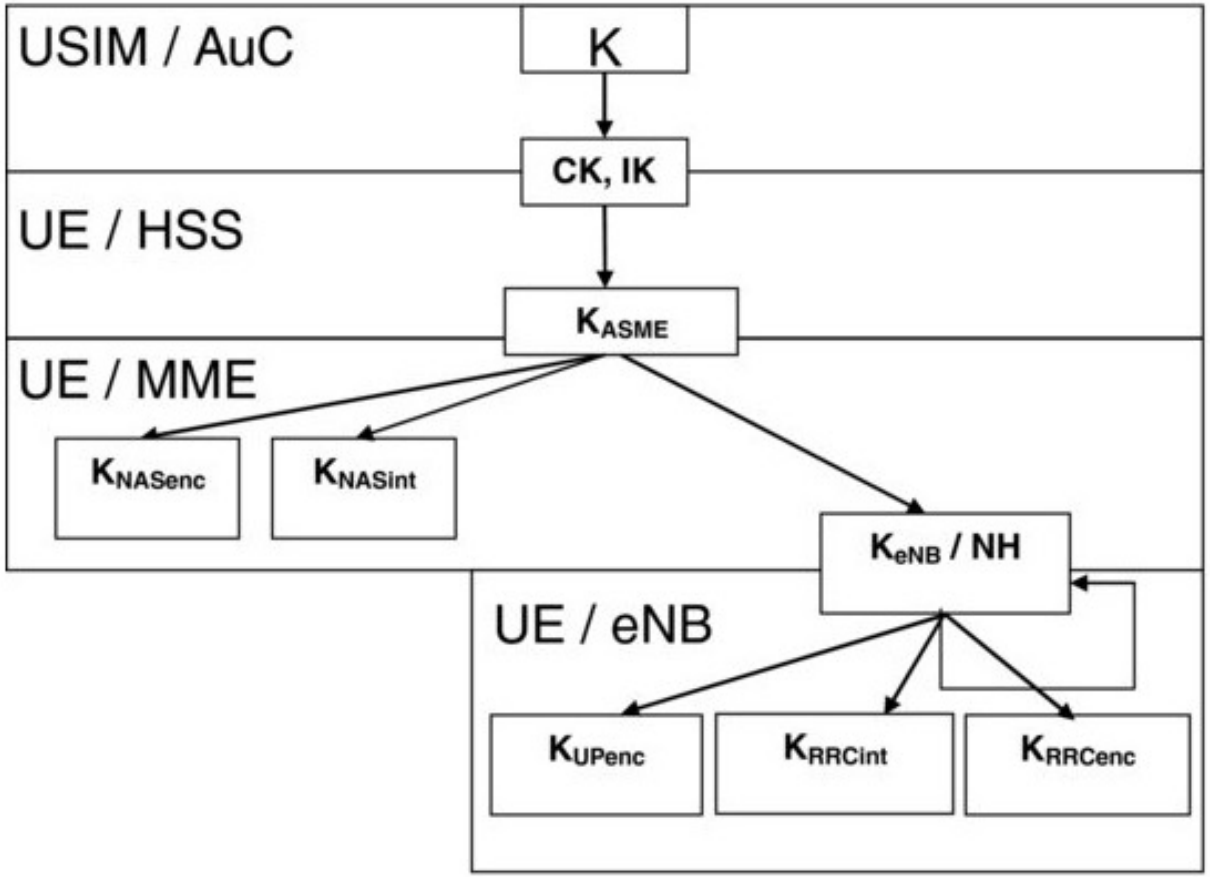
Security Context

- A security context is a set of parameters agreed by 2 parties when they engage in a secured communication

- Contains: algorithm identifiers, cryptographic keys, etc.

Key hierarchy (remember!)

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



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

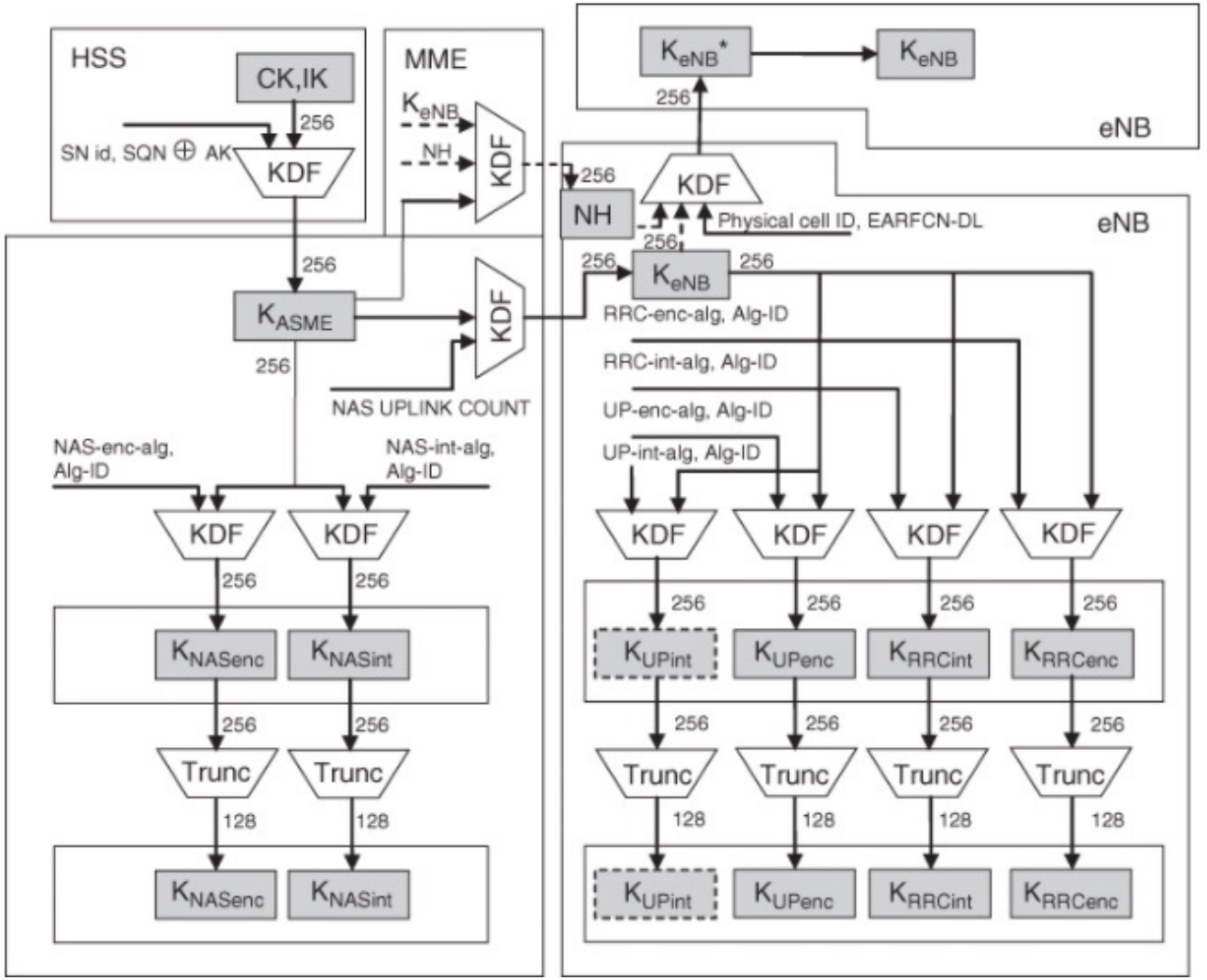
Key hierarchy

- K_{ASME} is derived in the ME (not the USIM!) and the HSS => its derivation it must be standardized; others not necessarily
- KDF used to derive keys in the hierarchy must be one-way; **why?**
- KDF based on **HMAC-SHA-256**
- Encryption and integrity keys (K_{NASenc}, K_{NASint}, K_{RRCint}, K_{RRCenc}, K_{UPenc}) are on 256 bits and truncated to 128 last significant bits (EPS accepts both 256 and 128 bits keys)
- Keys are derived in hierarchical manner, with additional parameters as input (e.g.: SN id, SQN xor AK, etc.) – the params are all **assumed to be known by a potential attacker** because they are sent in clear or easy computable from unencrypted communication

Key hierarchy

- A principle that brings **advantages**:
  - Cryptographic key separation:
    - Each key is used to one context only (e.g.: encryption of signalling traffic)
    - Prevents **expanding of leakage**: leakage of keys in one context do not help finding the key in another context
    - **Related key attacks**: the attacker can ask the exchange of the key in a way that he predetermines the relation between the old and new keys
  - Key freshness:
    - Keys can be renewed without affecting other keys (e.g.: renew of K_{eNB} does not require renewal of the K_{ASME} , X2 hadover)
    - Renewal of keys takes place more often
- … and **disadvantages**: added complexity

Key hierarchy



Question: Can K_{NASenc}, K_{NASint} be refreshed without refreshing the K_{ASME} ? How?

Just by changing the other param, NAS-enc/int-alg Alg_ID

Cryptography

- Algorithm agility / flexibility: the cryptographic **algorithms should be replaced** without much difficulty
  - Allows removal of out-dated algorithms
  - The number of algorithms should be keep small (for synchronization and management reasons), but more than 1…
  - … because if one algorithms fails (is broken), others will be used
- Algorithms diversity**: the design** of the algorithms **should differ** from each other as much as possible
  - *Why? Where did you encounter this principle before (in crypto)?*
- Emergency scenarios

Emergency

- Null algorithm: provides no cryptographic protection
  - Must exist for emergency cases
  - **Problematic** from security perspective because it can be triggered in cases where protection should be enabled
- Turn-off principle: the **cryptographic protection should be by default on**, and only by request (on special scenarios) should be turned off
- EEA0 (EPS Encryption Algorithm): the identity function (i.e. ciphertext equals the cleartext)
- EIA0 (EPS Integrity Algorithm) **: a 32-bit string of 0's** is appended to the message
  - Reason: **keep the protected and non-protected scenarios as similar as possible** (e.g.: same length)

Confidentiality

- Same structure for NAS and AS protection
- Out-of-the shelf algorithms (easier than to invite submission and go through a selection process) …
- … keeping in mind **reusability** from 3G (compatibility reasons)

- 128-EEA1: **SNOW 3G** adapted to the EPS security architecture
  - 128 bits keys
- 128-EEA2: **AES** over **KASUMI**
  - 128 bits keys
  - Counter mode

Integrity

- Same principles as for confidentiality
- Usage of the same main cryptographic blocks (re-usability)

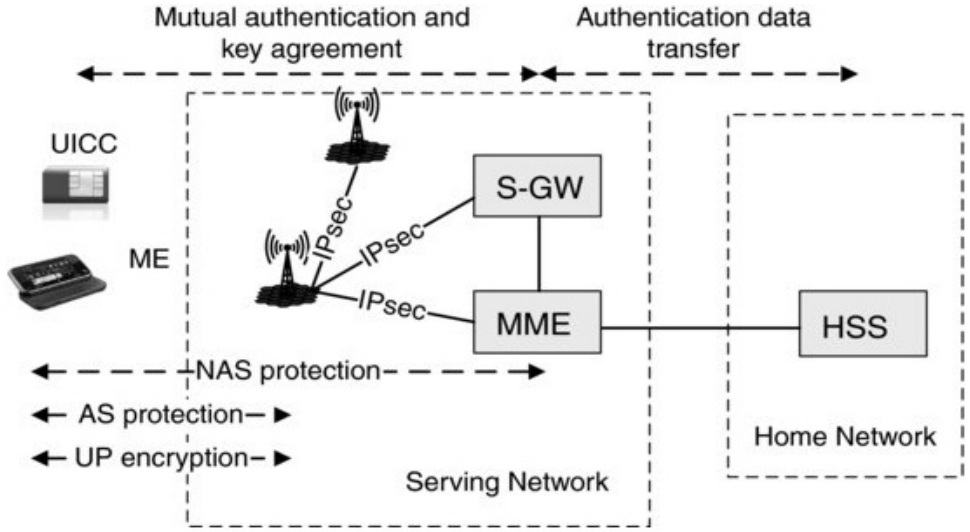
- 128-EIA1: **UIA 2 (SNOW 3G)** adapted to the EPS security architecture
  - 128 bits keys
- 128-EIA2: **Cipher- based MAC (AES)**
  - 128 bits keys
- The key length in the naming implies that other key lengths (e.g.:192, 256) can be used in case of improved security

Key derivation

- One-way: an adversary cannot use one key to derive a key located upper in the hierarchy
- Independence: 2 keys derived from the same key should be independent
- **SHA-256** used in the **HMAC** mode

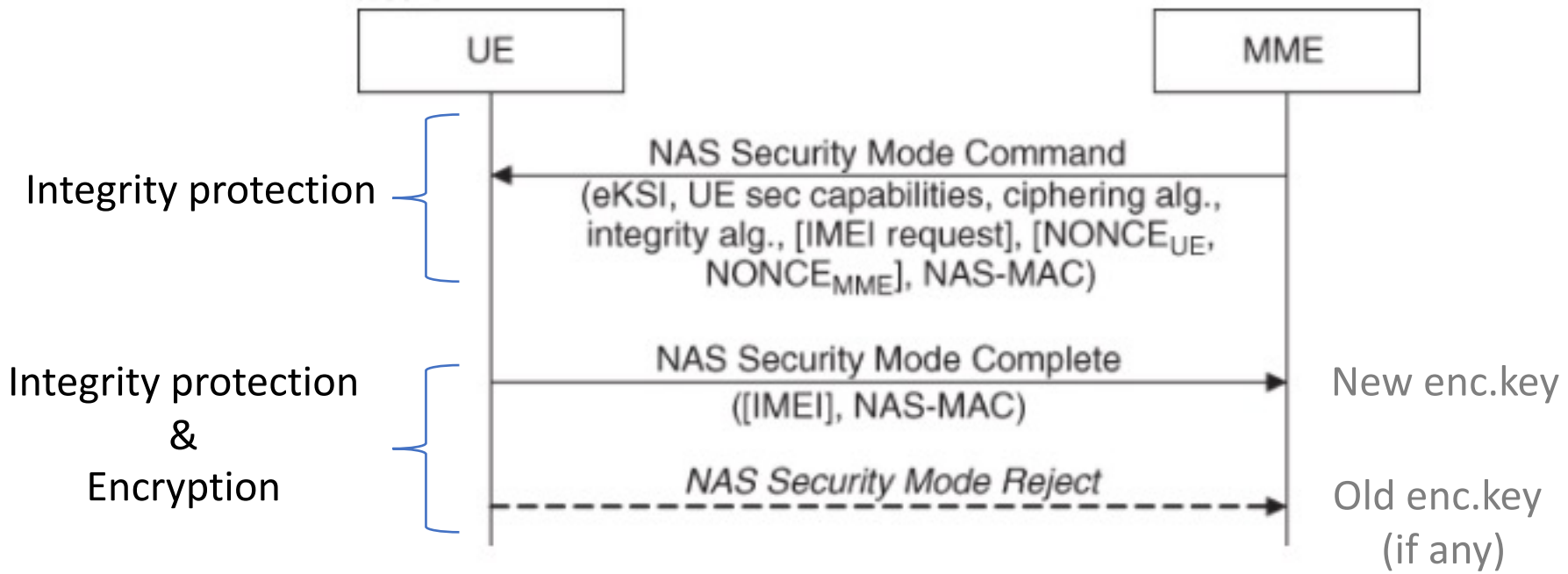
Algorithm negotiation

- Algorithms are **negotiated separately** for AS (between UE and eNodeB) and NAS (between UE and MME)
- Negotiation is based on the UE capabilities and a list of allowed cryptographic algorithms in the eNodeB, respectively MME in priority order
- eNodeB and MME are responsible for selecting the AS level, respectively the NAS level algorithms, after UE sends its capabilities in the attachment procedure
- Selection is indicated in AS Security Mode Command, respectively NAS Security Mode Commands



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

NAS signalling protection



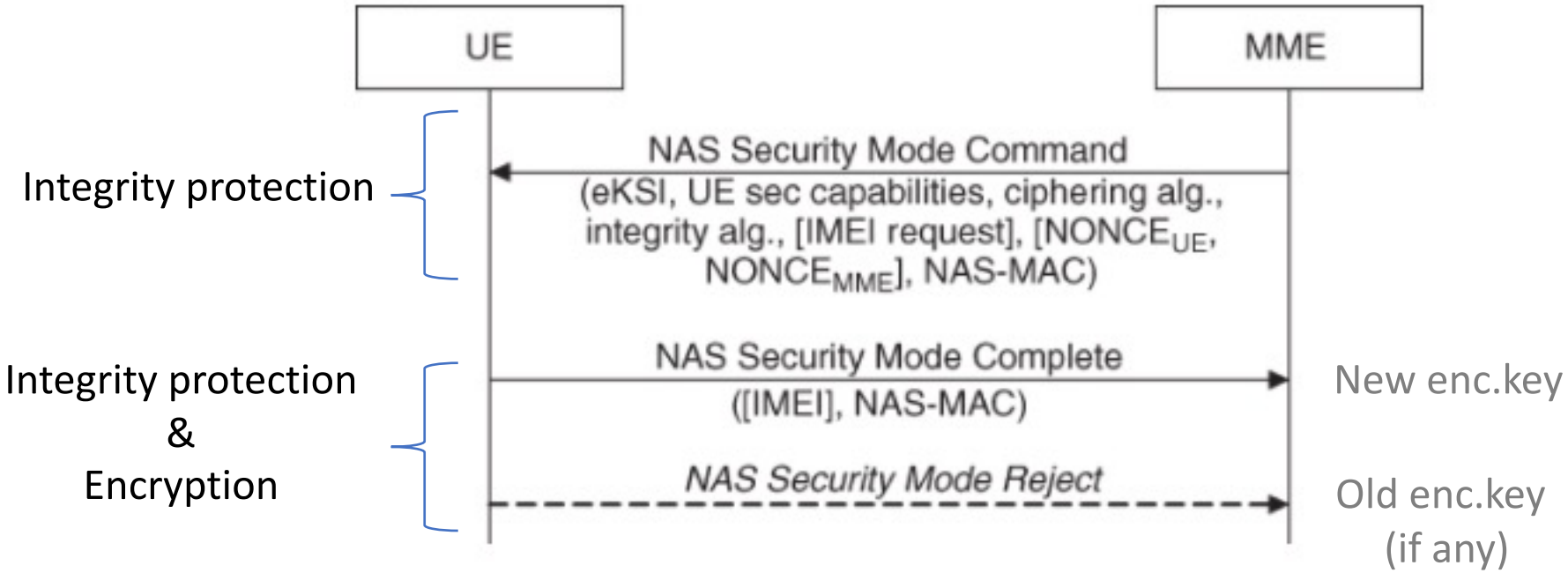
[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

eKSI: key set identifier that identifies the key K_{ASME}
$NONCE_{UE}$, $NONCE_{MME}$: used for mobility

Question: Why is the NAS Security Mode Command not encrypted?

The UE does not know what algorithm and key to use for decryption

NAS signalling protection



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

eKSI: key set identifier that identifies the key K_{ASME}
$NONCE_{UE}$, $NONCE_{MME}$: used for mobility

Question: Why is the NAS Security Mode Complete encrypted?

To not expose IMEI

NAS signalling protection

- **Integrity** and **replay protection** are part of the NAS protocol itself
- Integrity algorithm's **input** params:
  - K_{NASint} , 128 bits key
  - COUNT, 32 bits
  - DIRECTION, 1 bit indicating upstream or downstream signalling
  - BEARER, constant value – used for similarity with AS

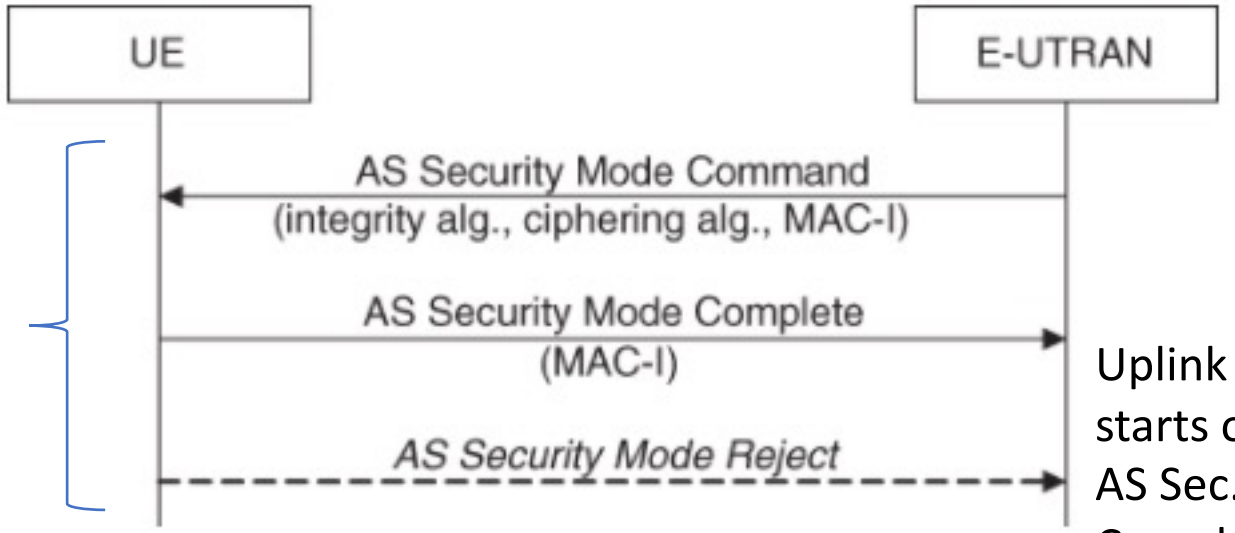
COUNT = 0x00 || NAS OVERFLOW || NAS SQN

  - NAS OVERFLOW, 16 bits – incremented every time NAS SQN overflows
- Integrity algorithm's **output**:
  - NAS-MAC, 32 bits
- For efficiency reasons, `NAS Service Request` message uses 16 bits NAS-MAC (e.g.: when UE responds to paging from the MME)

NAS signalling protection

- **General rule:** messages that are not integrity protected are discarded in the UE and MME once the NAS protection has been activated
- **Exceptions:** emergency calls, etc.
- Ciphering: same inputs, except K_{NASenc} instead of K_{NASint} and an additional parameter LENGTH that specifies the length of the keystream to be generated

AS signalling protection



Integrity protection

Uplink enc. starts only after AS Sec.Mode Complete is sent

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

Question: Why is the AS Security Mode Complete not encrypted?

No need, it contains no private information

AS signalling and User data protection

- Radio Resource Control (RRC): the AS level signalling protocol
- The security is implemented in the PDCP (Packet Data Convergence Protocol) layer, which carries both RRC and user data
- Integrity algorithm's **input** params:
  - K_{RRCint} , 128 bits key
  - COUNT, 32 bits, for each radio bearer (PDCP seg.no).
  - DIRECTION, 1 bit, indicating upstream or downstream
  - BEARER, 5 bits indicating the radio bearer identity, mapped from RRC bearer identity:

Same inputs as for NAS, but a different key and BEARER not constant

Signalling Radio Bearers (SRB):	**SRB0** RRC control messages not protected	**SRB1** RRC control messages protected after sec. activation	**SRB2** NAS messages Always protected
Data Radio Bearers (DRB)	multiple ciphered, but not integrity-protected		

- Integrity algorithm's **output**:
  - MAC-I, 32 bits

AS signalling and User data protection

- Ciphering: same inputs, except K_{RRCenc} instead of K_{RRCint} and an additional parameter LENGTH that specifies the length of the keystream to be generated

NAS vs AS Security Mode Commands (SMC)

AS (Access Stratum)

- Signalling protection **and user data protection**
- Security is implemented in the **PDCP protocol**
- It is **not possible** to change algorithms using `AS Security Mode Command`
- Encryption starts **after** the `AS Security Mode Complete`
- **Several bearers** (there are several AS level connections between UE and eNodeB)

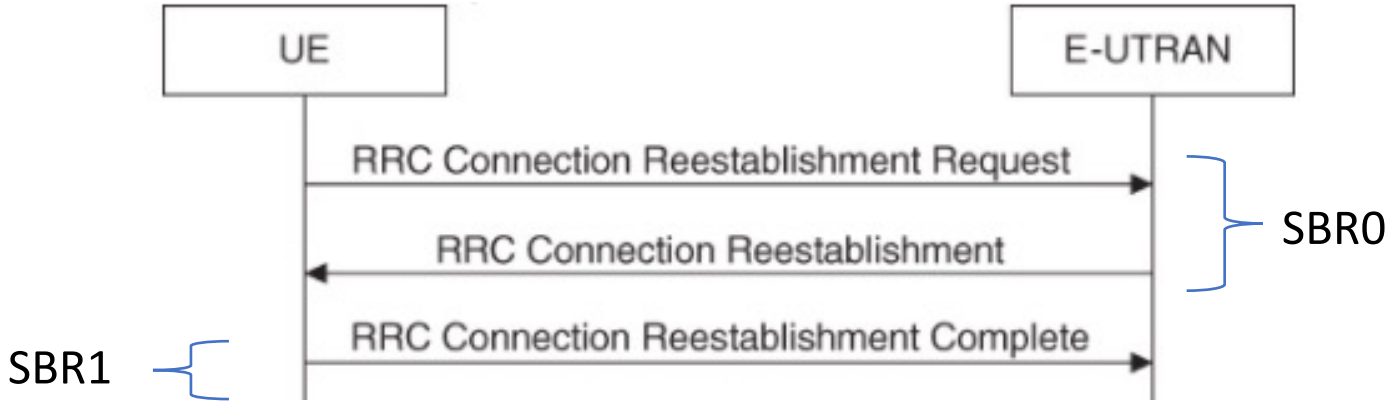
NAS (Non-Access Stratum)

- Signalling protection
- Security is implemented in the **NAS protocol itself**
- It is **possible** to change algorithms using `NAS Security Mode Command`
- Encryption starts **with** the `NAS Security Mode Complete`
- **One bearer** of **constant value** (there is only one NAS level connection between UE and MME)

RRC Connection re-establishment

- Initiated by the UE when there are problems (physical connection, integrity checksum errors, handover errors, etc.)

- Purpose:
  - Resume SRB1 operation
  - Reactivate security without change of security algorithms



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

RRC Connection re-establishment

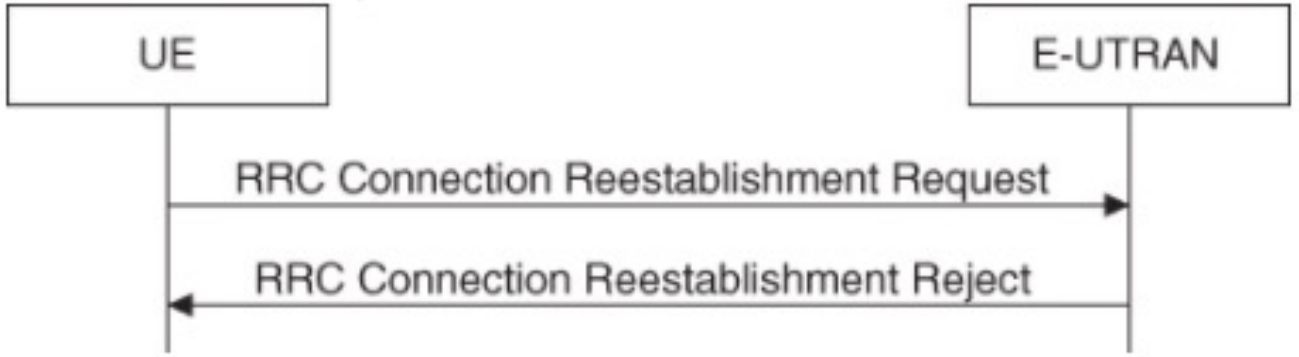
- Parameters:

RRC Connection Reestablishment Request	
ShortMAC-I	16 lsb of MAC-I (calculated with the RRC integrity key used in the source cell or the cell in case of handover, or in the cell that triggers re-establishment)
COUNT **BEARER** **DIRECTION**	All set to binary ones

RRC Connection Reestablishment	
NCC (Next hop Chaining Count)	Used to synchronize the K_{eNB}

RRC Connection re-establishment

- Upon failure, UE moves to *idle state*
- Coming back from idle to *connection state* include new C-RNTI allocation, NAS signalling and fresh key delivery from the MME



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

To remember!

1. The principles of EPS AKA
2. The advantages of key hierarchy
3. Principles to select and use cryptographic algorithms
4. Implementation in LTE

Mobile Security – 5G

Network Security - Lecture 9

Ruxandra F. Olimid

Faculty of Mathematics and Computer Science, University of Bucharest

Outline

- Arhitecture
- EPS AKA
- Key hierarchy
- Cryptographical aspects
- New concepts

5G Security

Figure 1: Standardisation organisations of relevance for 5G security

https://www.3gpp.org/

https://www.ieee.org/

https://www.etsi.org/

https://www.itu.int

https://www.ietf.org/

[ENISA – Security in 5G Specifications – Controls in 3GPP
Available at: https://www.enisa.europa.eu/publications/security-in-5g-specifications]

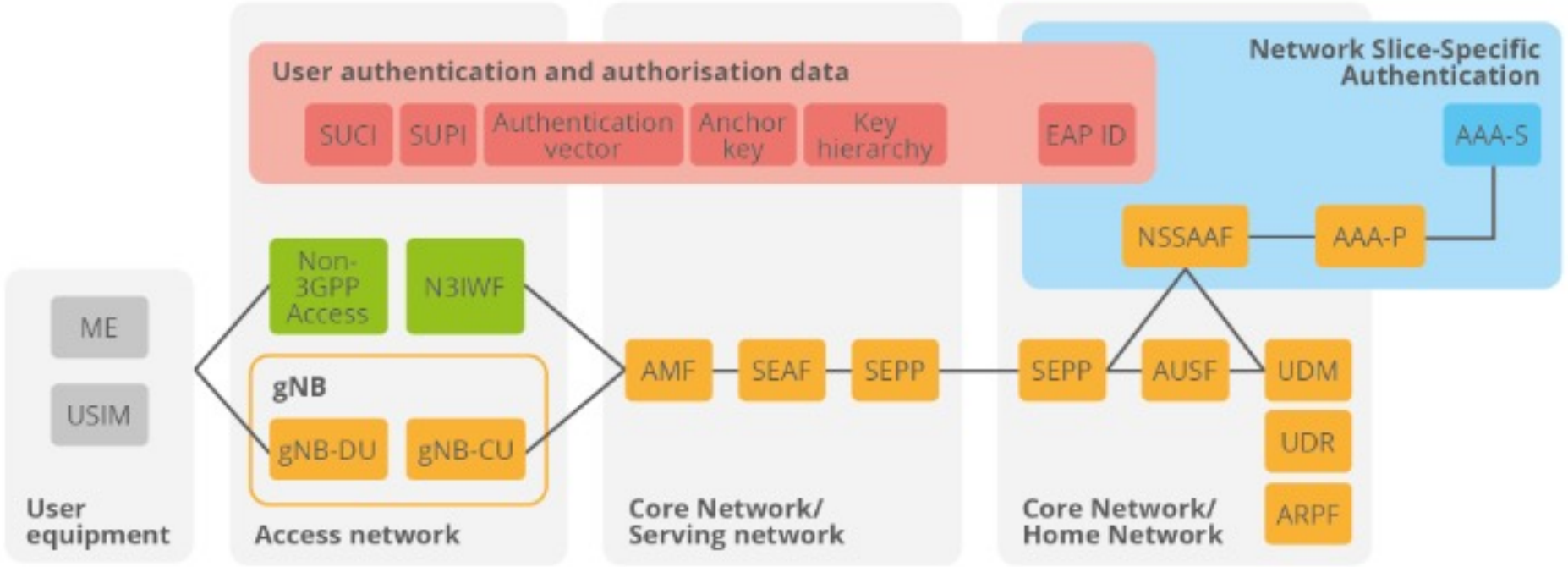
3GPP Security Standards

TS 33.501	Security architecture and procedures for 5G System
TS 33.511	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
TS 33.512	5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)
TS 33.513	5G Security Assurance Specification (SCAS); User Plane Function (UPF)
TS 33.514	5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class
TS 33.515	5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class
TS 33.516	5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class
TS 33.517	5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class
TS 33.518	5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class
TS 33.519	5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class
TS 33.520	5G Security Assurance Specification (SCAS); Non-3GPP InterWorking Function (N3IWF)
TS 33.521	5G Security Assurance Specification (SCAS); Network Data Analytics Function (NWDAF)
TS 33.522	5G Security Assurance Specification (SCAS); Service Communication Proxy (SECOP)
TS 33.535	Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)

[Source: https://www.3gpp.org/DynaReport/33-series.htm]

Security Architecture

Figure 8: Security architecture zoom-in from the ENISA 5G Threat Landscape 2020



[ENISA – Security in 5G Specifications – Controls in 3GPP
Available at: https://www.enisa.europa.eu/publications/security-in-5g-specifications]

UE Privacy

SUCI: Subscription Concealed Identifier
SUPI: Subscription Permanent Identifier
GUTI: Globally Unique Temporary UE Identity

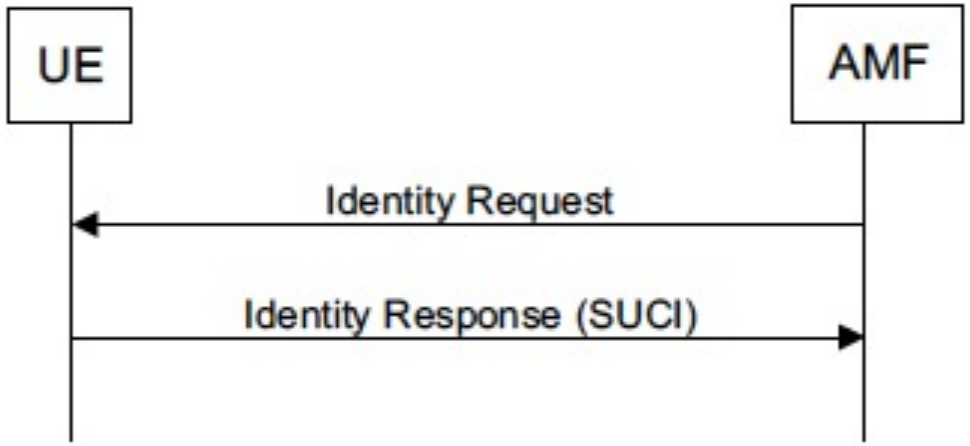


Figure 6.12.4-1: Subscription identifier query

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

Protection of SUPI - SUCI

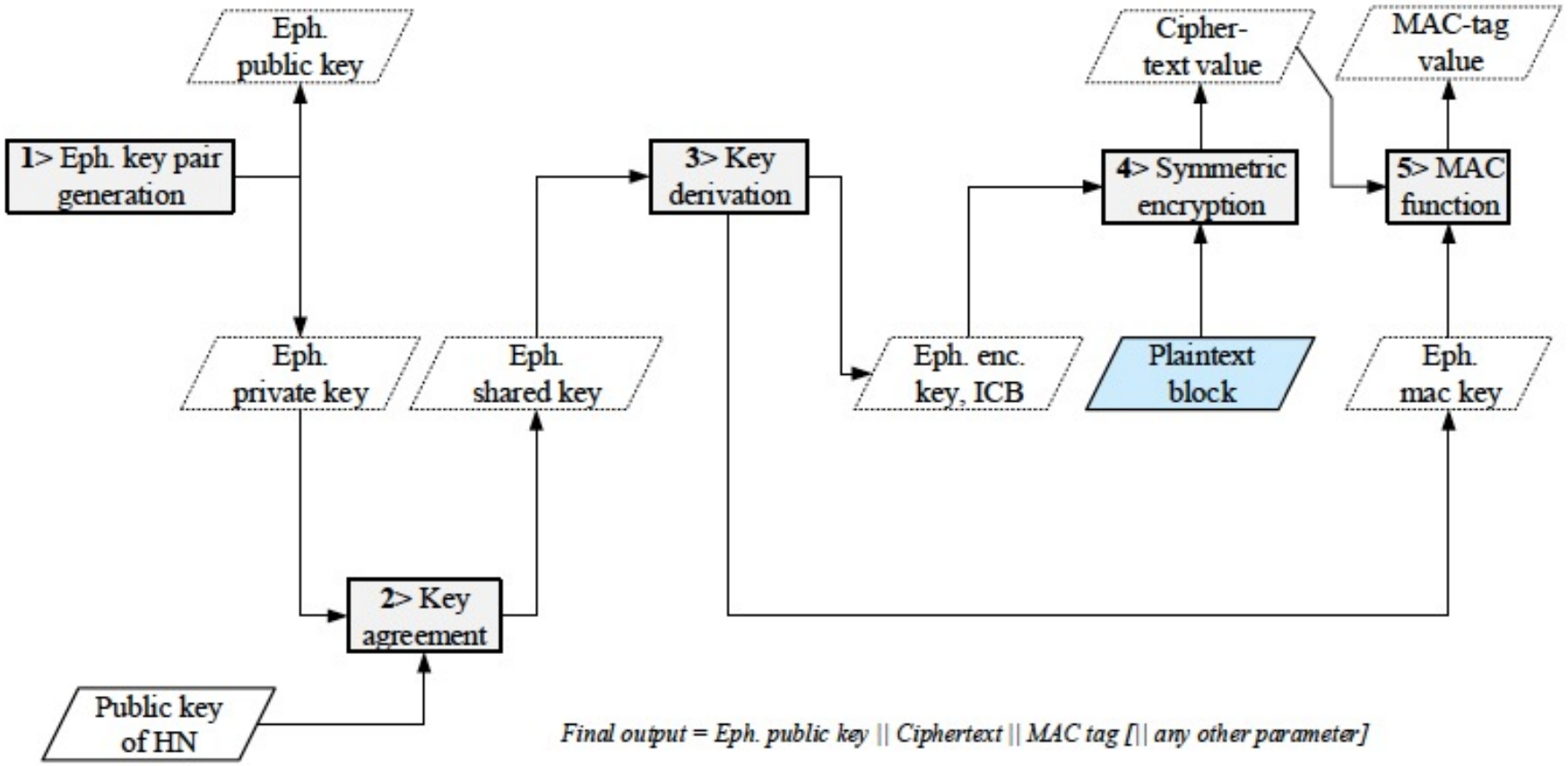


Figure C.3.2-1: Encryption based on ECIES at UE

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

Protection of SUPI - SUCI

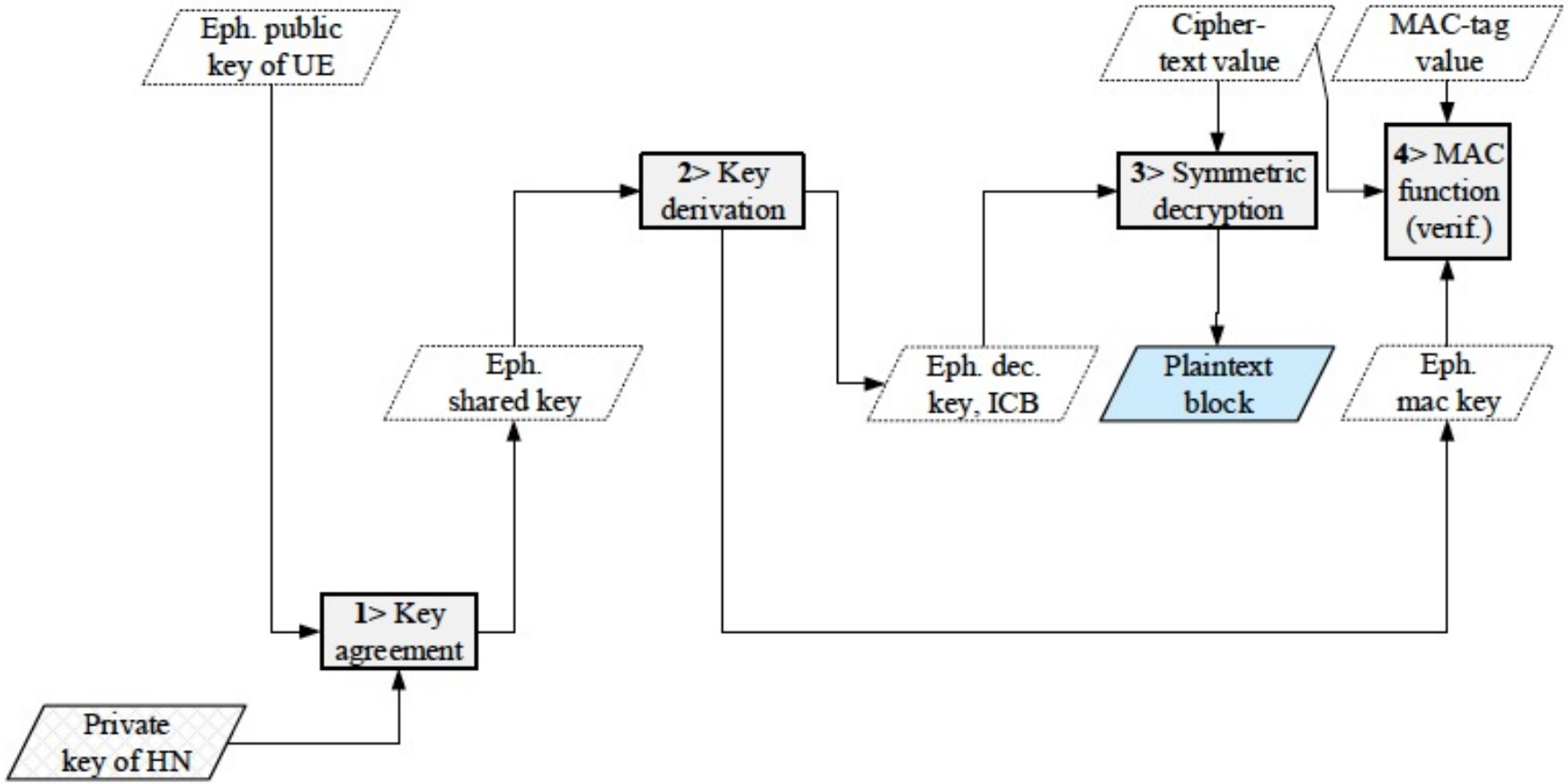


Figure C.3.3-1: Decryption based on ECIES at home network

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

5G-AKA

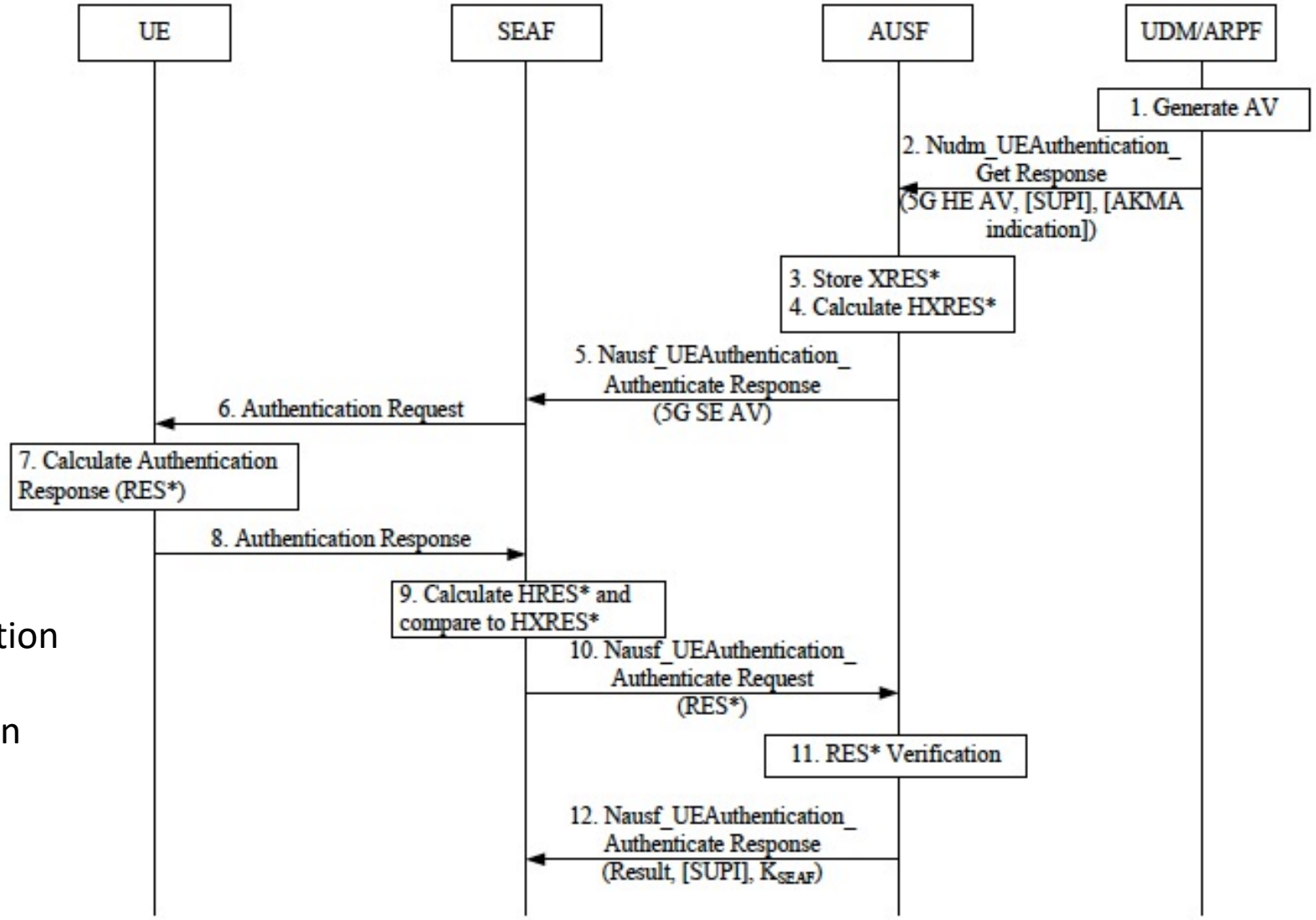


Figure 6.1.3.2-1: Authentication procedure for 5G AKA

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

AUSF: AUthentication Server Function
ARPF: Authentication credential Repository and Processing Function
SIDF: Subscription Identifier De-concealing Function
SEAF: SEcurity Anchor Function

Key Hierarchy

AUSF: AUthentication Server Function
ARPF: Authentication credential Repository and Processing Function
SEAF: SEcurity Anchor Function
AMF Access and Mobility Management Function

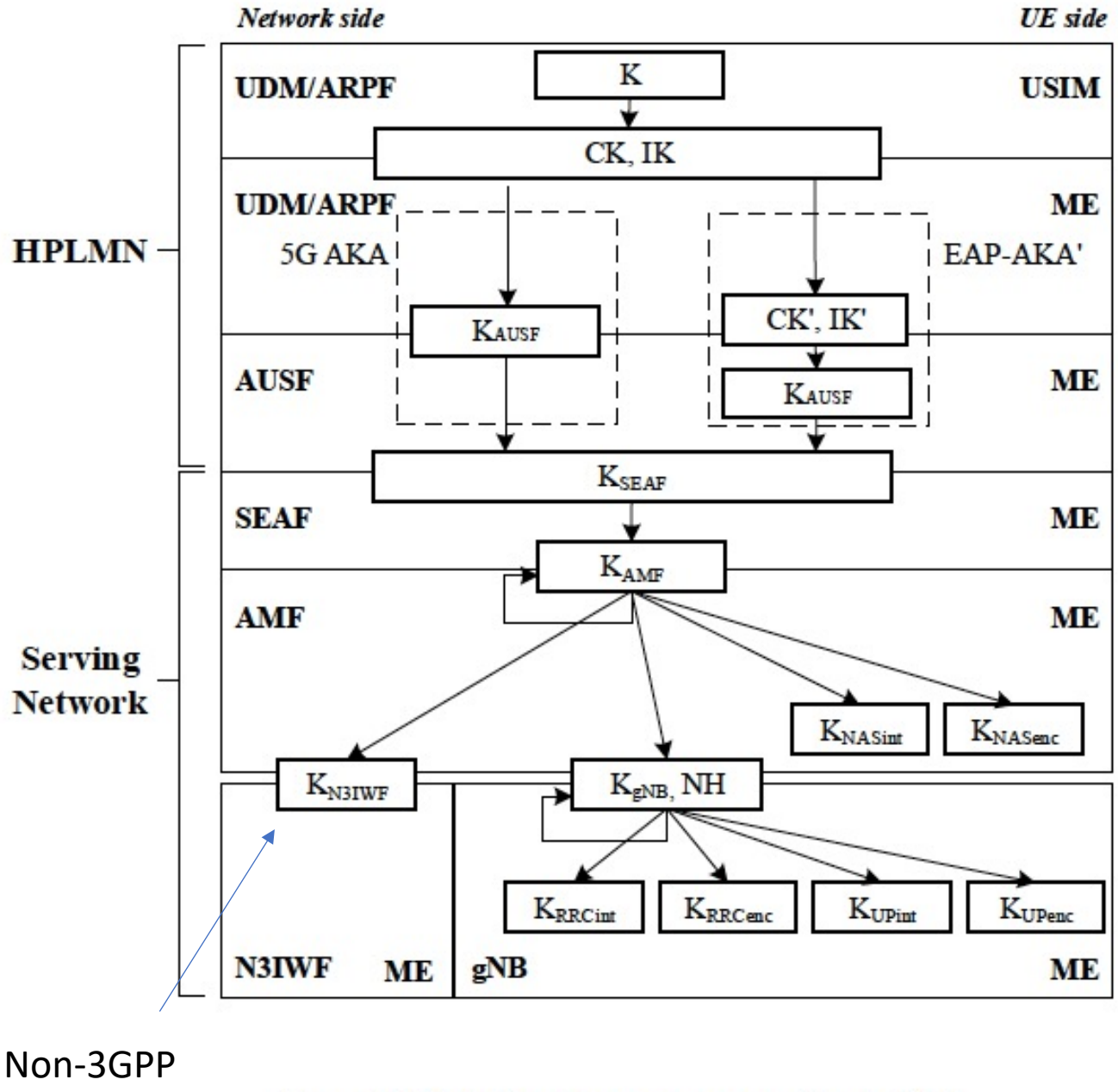


Figure 6.2.1-1: Key hierarchy generation in 5GS

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

Cryptographical Aspects

"0000_2"	NEA0	Null ciphering algorithm;
"0001_2"	128-NEA1	128-bit SNOW 3G based algorithm;
"0010_2"	128-NEA2	128-bit AES based algorithm; and
"0011_2"	128-NEA3	128-bit ZUC based algorithm.

5.2.2 User data and signalling data confidentiality

The UE shall support ciphering of user data between the UE and the gNB.

The UE shall activate ciphering of user data based on the indication sent by the gNB.

The UE shall support ciphering of RRC and NAS-signalling.

The UE shall implement the following ciphering algorithms:

NEA0, 128-NEA1, 128-NEA2 as defined in Annex D of the present document.

The UE may implement the following ciphering algorithm:

128-NEA3 as defined in Annex D of the present document.

The UE shall implement the ciphering algorithms as specified in TS 33.401 [10] if it supports E-UTRA connected to 5GC.

Confidentiality protection of the user data between the UE and the gNB is optional to use.

Confidentiality protection of the RRC-signalling, and NAS-signalling is optional to use.

Confidentiality protection should be used whenever regulations permit.

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

Cryptographical Aspects

"0000_2"	NIA0	Null Integrity Protection algorithm;
"0001_2"	128-NIA1	128-bit SNOW 3G based algorithm;
"0010_2"	128-NIA2	128-bit AES based algorithm; and
"0011_2"	128-NIA3	128-bit ZUC based algorithm.

5.2.3 User data and signalling data integrity

The UE shall support integrity protection and replay protection of user data between the UE and the gNB. The UE shall support integrity protection of user data at any data rate, up to and including, the highest data rate supported by the UE.

The UE shall activate integrity protection of user data based on the indication sent by the gNB.

The UE shall support integrity protection and replay protection of RRC and NAS-signalling.

The UE shall implement the following integrity protection algorithms:

NIA0, 128-NIA1, 128-NIA2 as defined in Annex D of the present document.

The UE may implement the following integrity protection algorithm:

128-NIA3 as defined in Annex D of the present document.

The UE shall implement the integrity algorithms as specified in TS 33.401 [10] if it supports E-UTRA connected to 5GC.

Integrity protection of the user data between the UE and the gNB is optional to use.

NOTE: Integrity protection of user plane adds the overhead of the packet size and increases the processing load both in the UE and the gNB.

Integrity protection of the RRC-signalling, and NAS-signalling is mandatory to use, except in the following cases:

All NAS signalling messages except those explicitly listed in TS 24.501 [35] as exceptions shall be integrity-protected.

All RRC signalling messages except those explicitly listed in TS 38.331 [22] as exceptions shall be integrity-protected with an integrity protection algorithm different from NIA0, except for unauthenticated emergency calls.

The UE shall implement NIA0 for integrity protection of NAS and RRC signalling. NIA0 is only allowed for unauthenticated emergency session as specified in clause 10.2.2.

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

New Concepts

- SDN
- NFV
- MEC
- Slicing
- Virtualisation
- … … …

To remember!

1. Improvements over 4G security

2. New concepts