b
UNIVERSITÄT
BERN

UNIVERSITÄT
BERN

Network Security

IX. Cellular Networks

Prof. Dr. Torsten Braun, Institut für Informatik

Bern, 25.04.2022 – 02.05.2022

Cellular Networks

Table of Contents

1. Introduction
2. GSM (2G)
3. UMTS (3G)
4. LTE (4G)
5. 5G

Introduction

1. Literature

Books

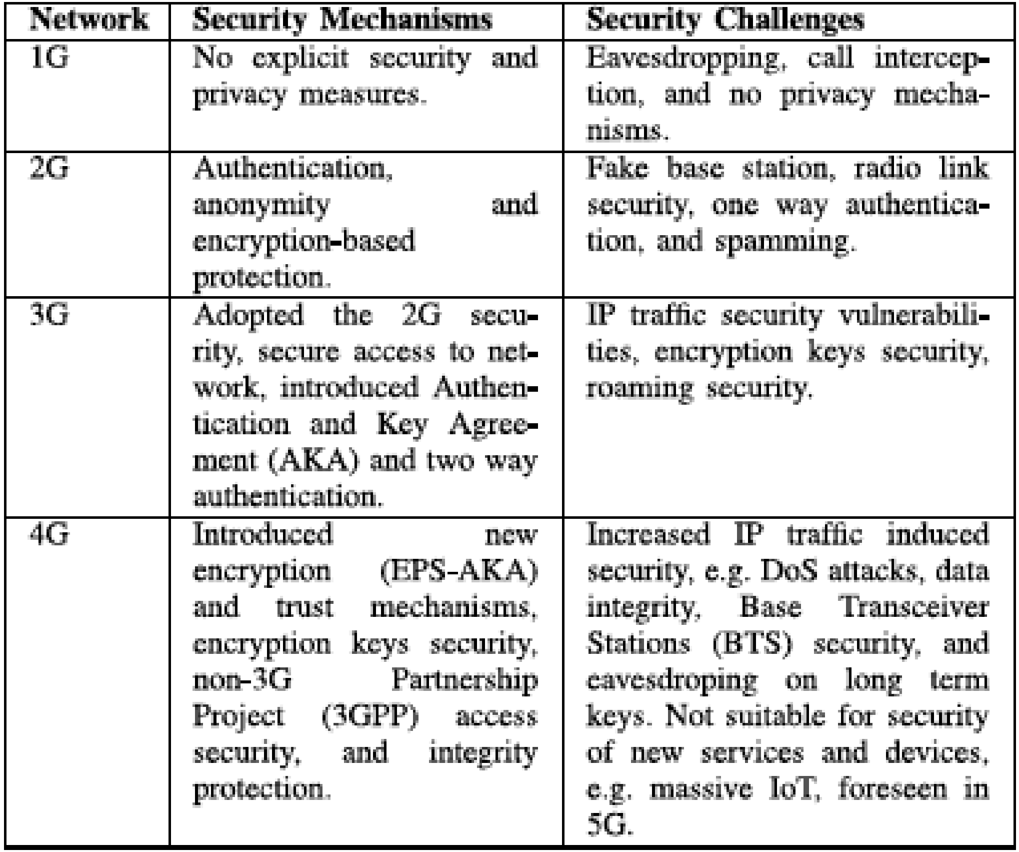
- Eberspächer et al.:
  GSM – Architecture, Protocols and Services, 3rd edition
- Forsberg et al.:
  LTE Security, 2nd edition
- Penttinen (ed.): The LTE/SAE Deployment Handbook
- Kreher et al.: LTE Signaling
- Penttinen: 5G Explained

Articles

- Ahmad et al.:
  Security for 5G and Beyond,
  IEEE Communications Surveys & Tutorials, Vol. 21, No. 4, 2019
- Zou et al.: A Survey on Wireless Security, Recent Advances and Future Trends,
  Proceedings of the IEEE,
  Vol. 104, No. 9, September 2016

1. Introduction

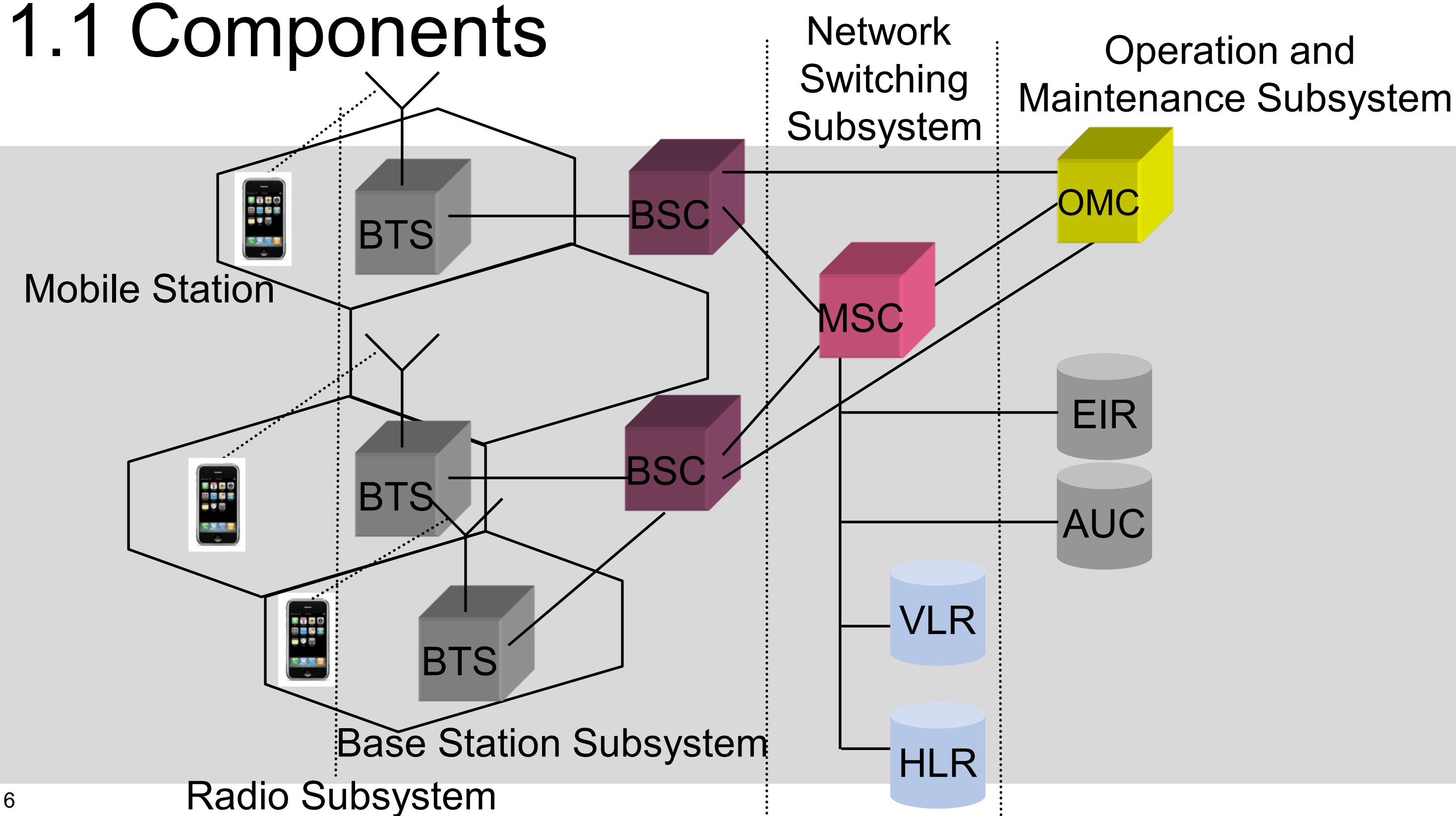
2. Security Evolution



Network	Security Mechanisms	Security Challenges
1G	No explicit security and privacy measures.	Eavesdropping, call interception, and no privacy mechanisms.
2G	Authentication, anonymity and encryption-based protection.	Fake base station, radio link security, one way authentication, and spamming.
3G	Adopted the 2G security, secure access to network, introduced Authentication and Key Agreement (AKA) and two way authentication.	IP traffic security vulnerabilities, encryption keys security, roaming security.
4G	Introduced new encryption (EPS-AKA) and trust mechanisms, encryption keys security, non-3G Partnership Project (3GPP) access security, and integrity protection.	Increased IP traffic induced security, e.g. DoS attacks, data integrity, Base Transceiver Stations (BTS) security, and eavesdroping on long term keys. Not suitable for security of new services and devices, e.g. massive IoT, foreseen in 5G.

2. GSM

1.1 Components



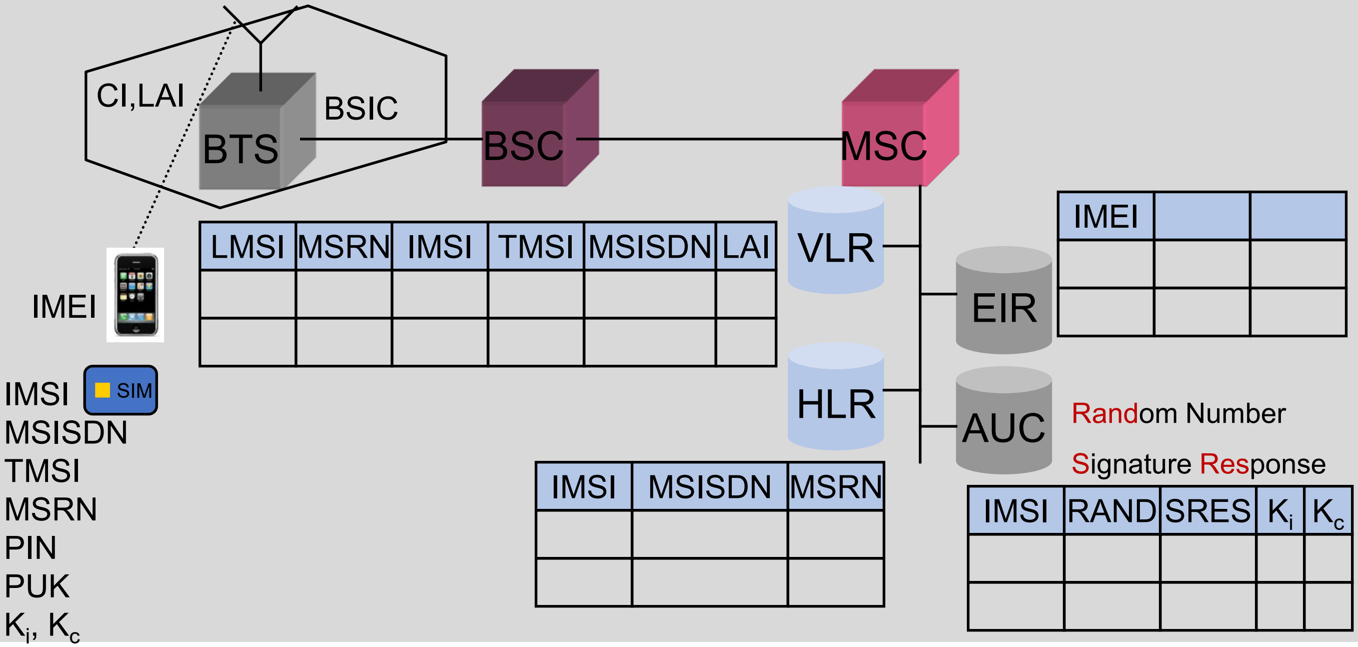
2. GSM

1.2 Components

- Mobile device
- Subscriber Identity Module for user identification
  - Tamper-resistant smart-card
  - stores
    - static data, e.g., Identifiers, Authentication keys, Serial number
    - dynamic data, e.g., Location information, Carrier frequencies, Encryption keys, Short messages, Telephone numbers
- Base Station Subsystem
  - Base Transceiver Station
  - Base Station Controller
- Mobile Switching Center
- Home Location Register
  - per GSM network
  - Entries for each registered user with its fixed and temporary data, e.g., ISDN number, subscribed services, current location
- Visitor Location Register
  - for one or more MSC regions
  - includes data of visiting users
  - registration of a mobile station via MSC
  - informs user's HLR
- Operation and Maintenance Center
- Authentication Center
- Equipment Identity Register

2. GSM

2. Tables



IMSI
MSISDN
TMSI
MSRN
PIN
PUK
K_i, K_c

LMSI	MSRN	IMSI	TMSI	MSISDN	LAI

IMEI		

IMSI	MSISDN	MSRN

Random Number

Signature Response

IMSI	RAND	SRES	K_i	K_c

2. GSM

3. Terminology

- International Mobile Station Subscriber Identity
  - for accounting purposes
- Mobile Subscriber ISDN Number
- Personal Identity Number
  - for SIM activation
- PIN Unblocking Key
  - for de-blocking after wrong PIN inputs
- Authentication key K_i
- Encryption key K_c
- Location Area Identity
  - Broadcast by base station to support LAI change
- Cell Identifier
  - for cell identification
- Base Transceiver Station Identity Code
  - Broadcast by base stations, to distinguish base stations
- Mobile Station Roaming Number
  - Temporary location dependent ISDN number
  - assigned by VLR to mobile station
  - allows identification of responsible MSC
- Temporary Mobile Subscriber Identity
  - for unique identification of a subscriber (TMSI + LAI) during visit of VLR region
  - replaces IMSI
- Local Mobile Station Identity
  - to support fast search

2. GSM

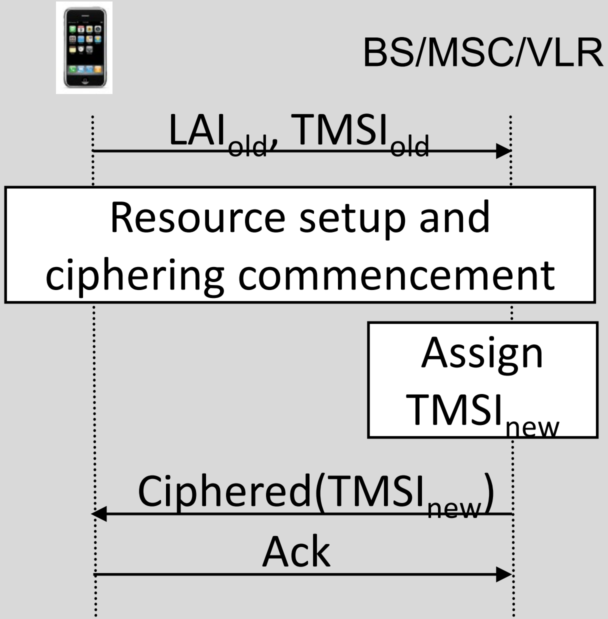
4. Security Functions

- Subscriber identity confidentiality
- Subscriber identity authentication
- Signaling information element confidentiality
- Data confidentiality

2. GSM

5.1 Subscriber Identity Protection I

- use TMSI instead of IMSI on radio channel for identification of subscribers
- TMSI is issued by VLR when MS changes between LAs.

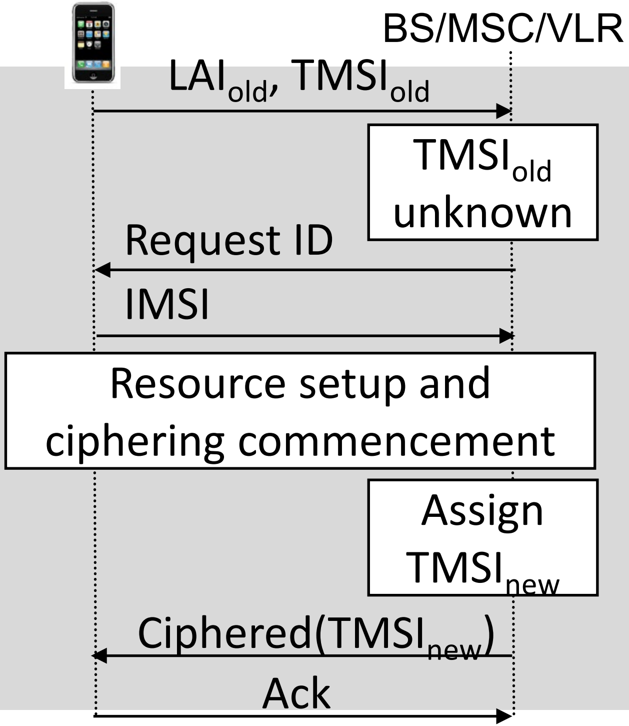

BS/MSC/VLR
LAI$_{old}$, TMSI$_{old}$
Resource setup and ciphering commencement
Assign TMSI$_{new}$
Ciphered(TMSI$_{new}$)
Ack

2. GSM

5.2 Subscriber Identity Protection II

In certain cases, the IMSI is requested from MS.

- VLR database failures
- No correct subscriber data available (loss of TMSI, unknown TMSI)



2. GSM

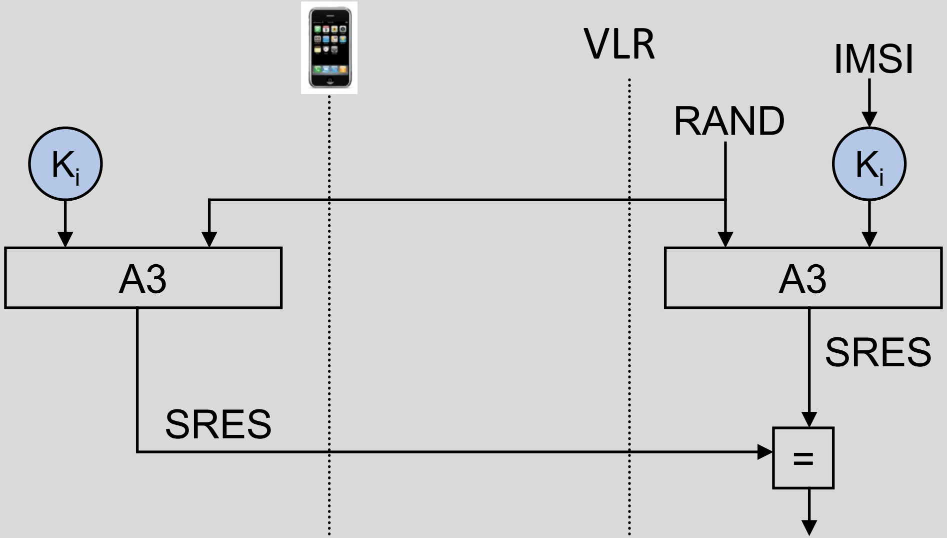
6. Cryptographic Algorithms

- A3: Subscriber Authentication
- A8: Radio Encryption
  - A3 and A8 are based on COMP algorithm
  - COMP
    - 9 rounds with hashing 256 to 128 bits
    - relatively unsecure.
- A5: Key Generation
  - A5/1: weak stream cipher
  - A5/2: weaker than A5/1
  - A5/3: based on KASUMI block cipher in counter mode with 64-bit keys
  - A5/4: A5/3 with 128-bit keys

2. GSM

7.1 Weakly Secure Authentication

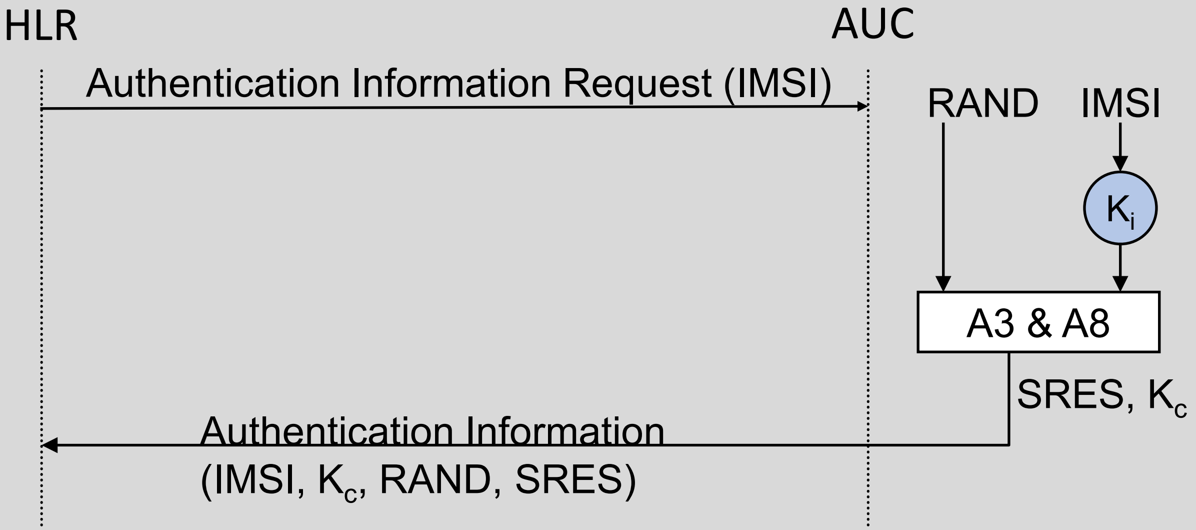
- Secret authentication key K_i is stored at SIM.
- Signature Response SRES = K_i(RAND)
- Transmission of K_i from AUC to VLR needed



2. GSM

7.2 Generation of Security Data for HLR

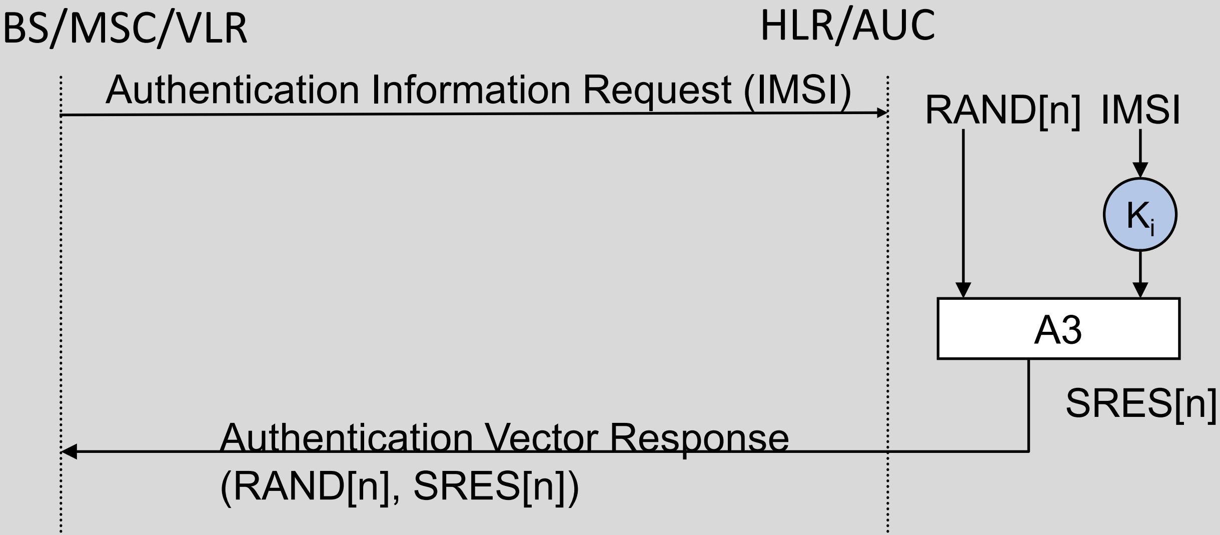
- Security data calculated by AUC allows keeping K_i at AUC.
- K_c: encryption key


HLR
AUC
Authentication Information Request (IMSI)
RAND
IMSI
K_i
A3 & A8
SRES, K_c
Authentication Information
(IMSI, K_c, RAND, SRES)

2. GSM

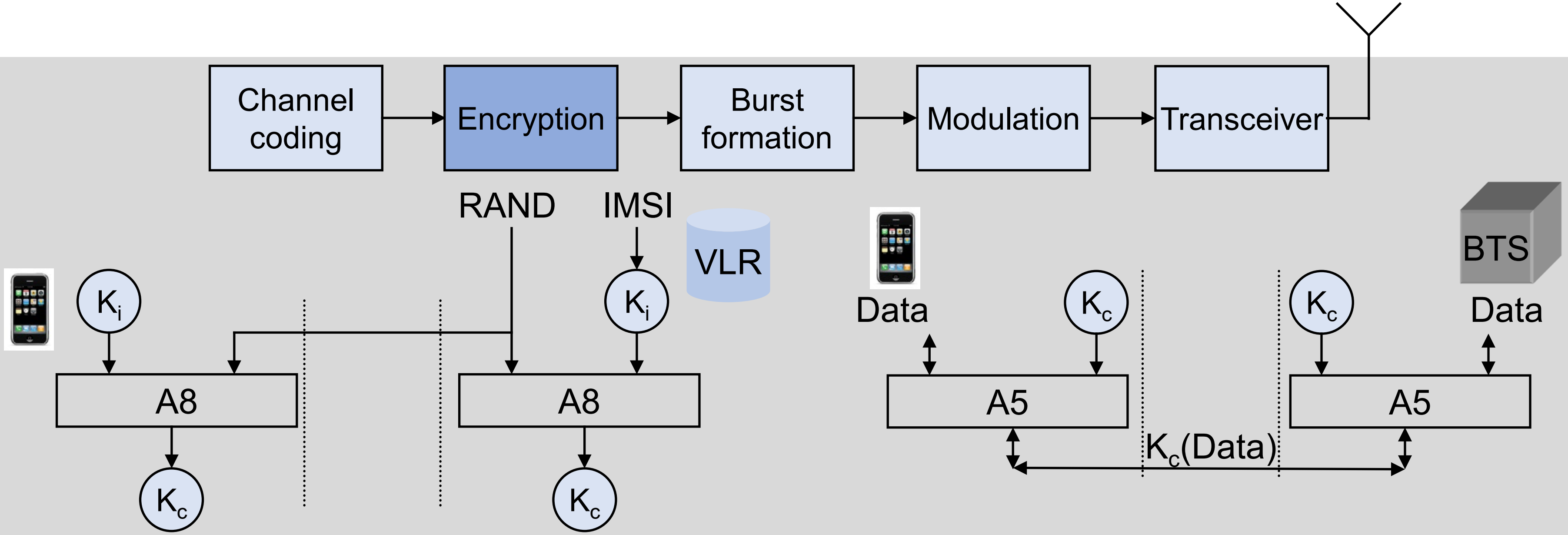
7.3 Highly Secure Subscriber Authentication

Authentication information (RAND, SRES) can be pre-calculated by AUC, stored by HLR and retrieved by VLR


BS/MSC/VLR
HLR/AUC
Authentication Information Request (IMSI)
RAND[n]
IMSI
K_i
A3
SRES[n]
Authentication Vector Response
(RAND[n], SRES[n])

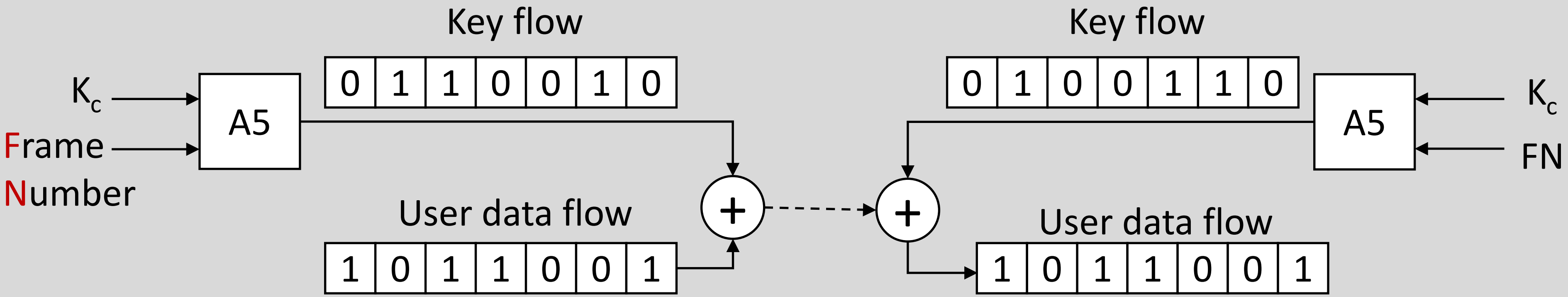
2. GSM

8.1 Encryption of Signalling and User Data



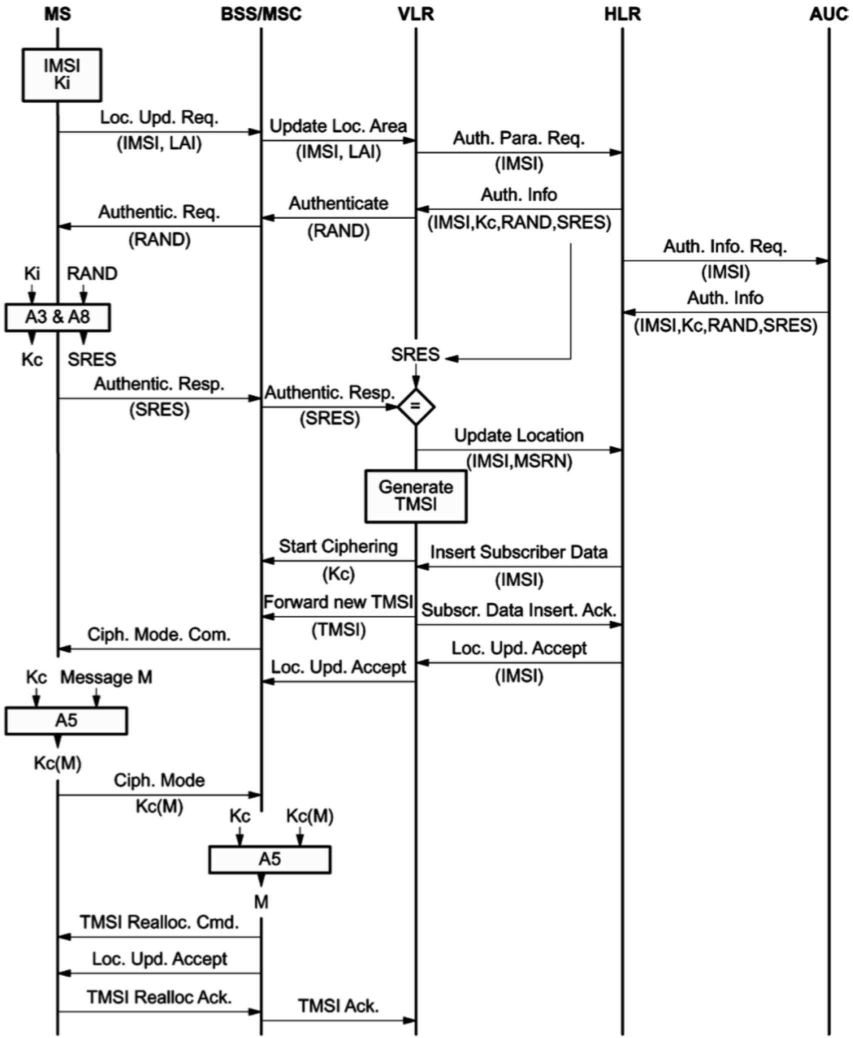
2. GSM

8.2 Combining Payload Data and Ciphering Stream



2. GSM

9.1 Location Registration



MS
BSS/MSC
VLR
HLR
AUC

IMSI
Ki

Loc. Upd. Req.
(IMSI, LAI)

Update Loc. Area
(IMSI, LAI)

Auth. Para. Req.
(IMSI)

Auth. Info
(IMSI,Kc,RAND,SRES)

Authenticate
(RAND)

Authentic. Req.
(RAND)

Auth. Info. Req.
(IMSI)

Auth. Info
(IMSI,Kc,RAND,SRES)

Ki
RAND
A3 & A8
Kc
SRES

SRES

Authentic. Resp.
(SRES)

Authentic. Resp.
(SRES)

=

Update Location
(IMSI,MSRN)

Generate
TMSI

Start Ciphering
(Kc)

Insert Subscriber Data
(IMSI)

Forward new TMSI
(TMSI)

Subscr. Data Insert. Ack.

Ciph. Mode. Com.

Loc. Upd. Accept
(IMSI)

Loc. Upd. Accept

Kc
Message M
A5
Kc(M)

Ciph. Mode
Kc(M)

Kc
Kc(M)
A5
M

TMSI Realloc. Cmd.

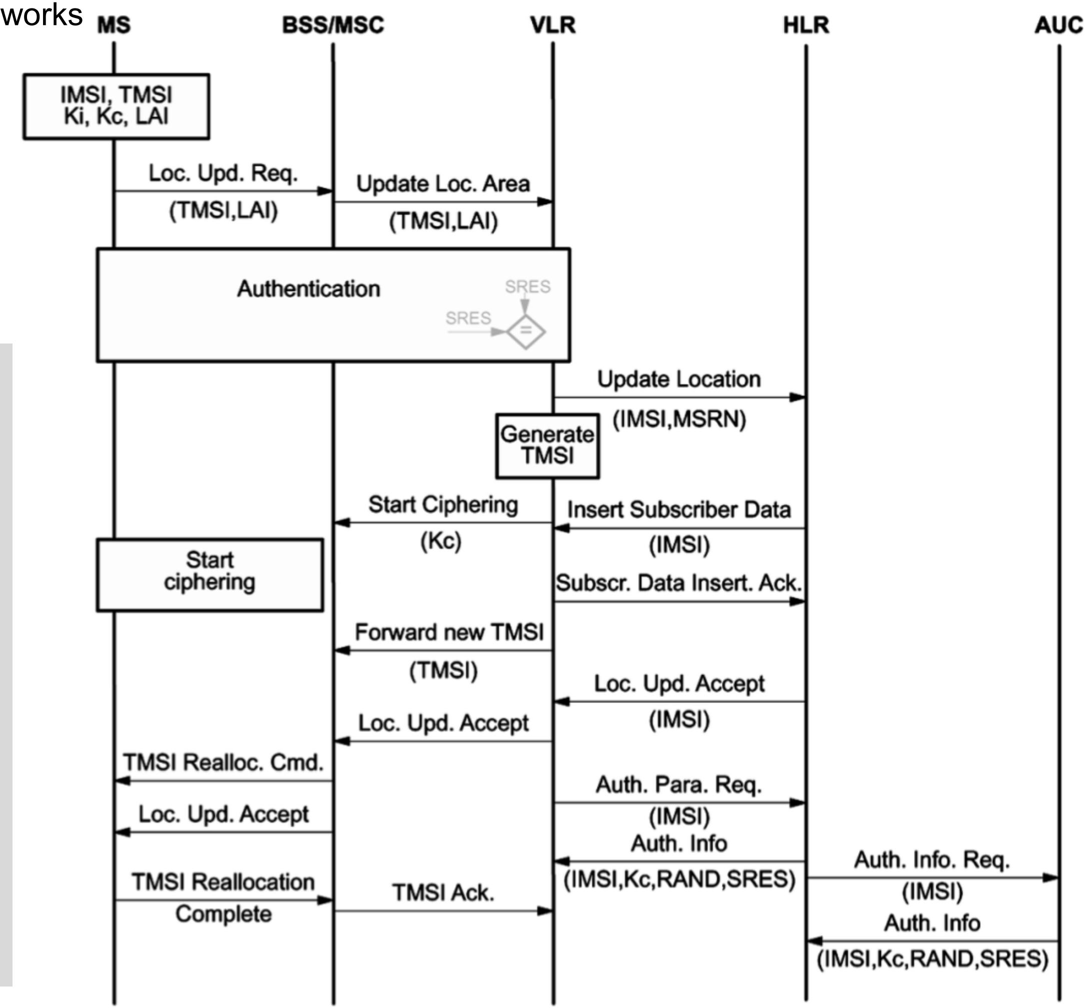
Loc. Upd. Accept

TMSI Realloc Ack.

TMSI Ack.

2. GSM

9.2 Location Update I



MS

BSS/MSC

VLR

HLR

AUC

IMSI, TMSI
Ki, Kc, LAI

Loc. Upd. Req.
(TMSI,LAI)

Update Loc. Area
(TMSI,LAI)

Authentication

SRES

SRES

=

Update Location
(IMSI,MSRN)

Generate
TMSI

Start Ciphering
(Kc)

Insert Subscriber Data
(IMSI)

Start
ciphering

Subscr. Data Insert. Ack.

Forward new TMSI
(TMSI)

Loc. Upd. Accept
(IMSI)

Loc. Upd. Accept

TMSI Realloc. Cmd.

Auth. Para. Req.
(IMSI)

Loc. Upd. Accept

Auth. Info
(IMSI,Kc,RAND,SRES)

Auth. Info. Req.
(IMSI)

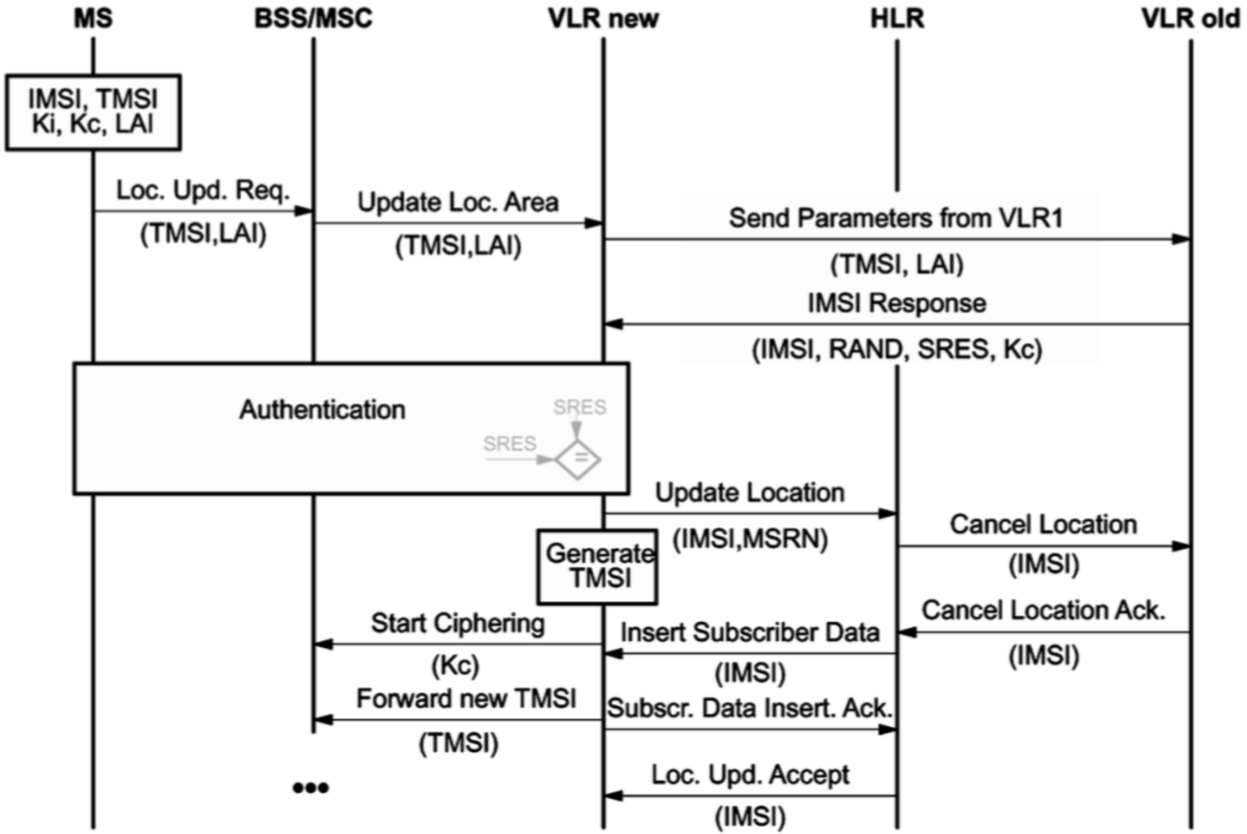
TMSI Reallocation
Complete

TMSI Ack.

Auth. Info
(IMSI,Kc,RAND,SRES)

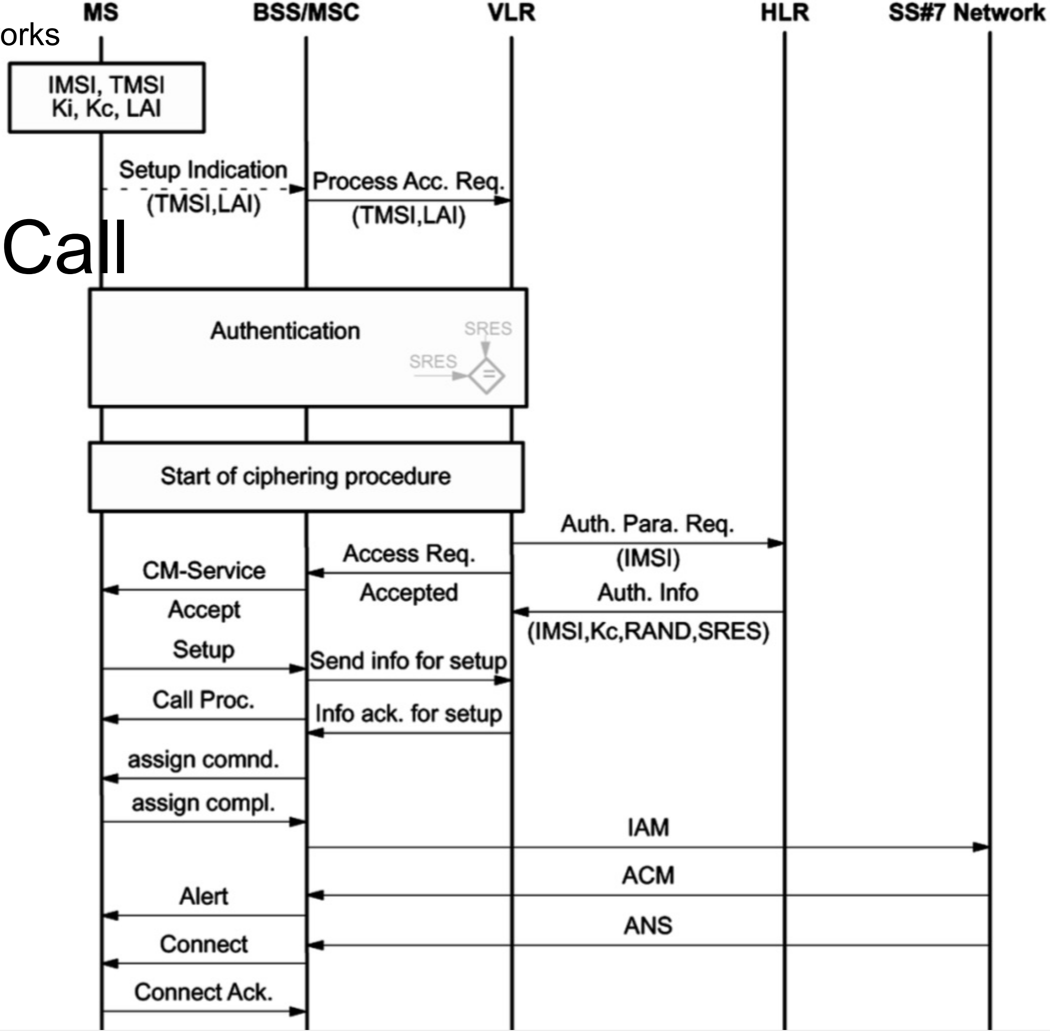
2. GSM

9.3 Location Update II



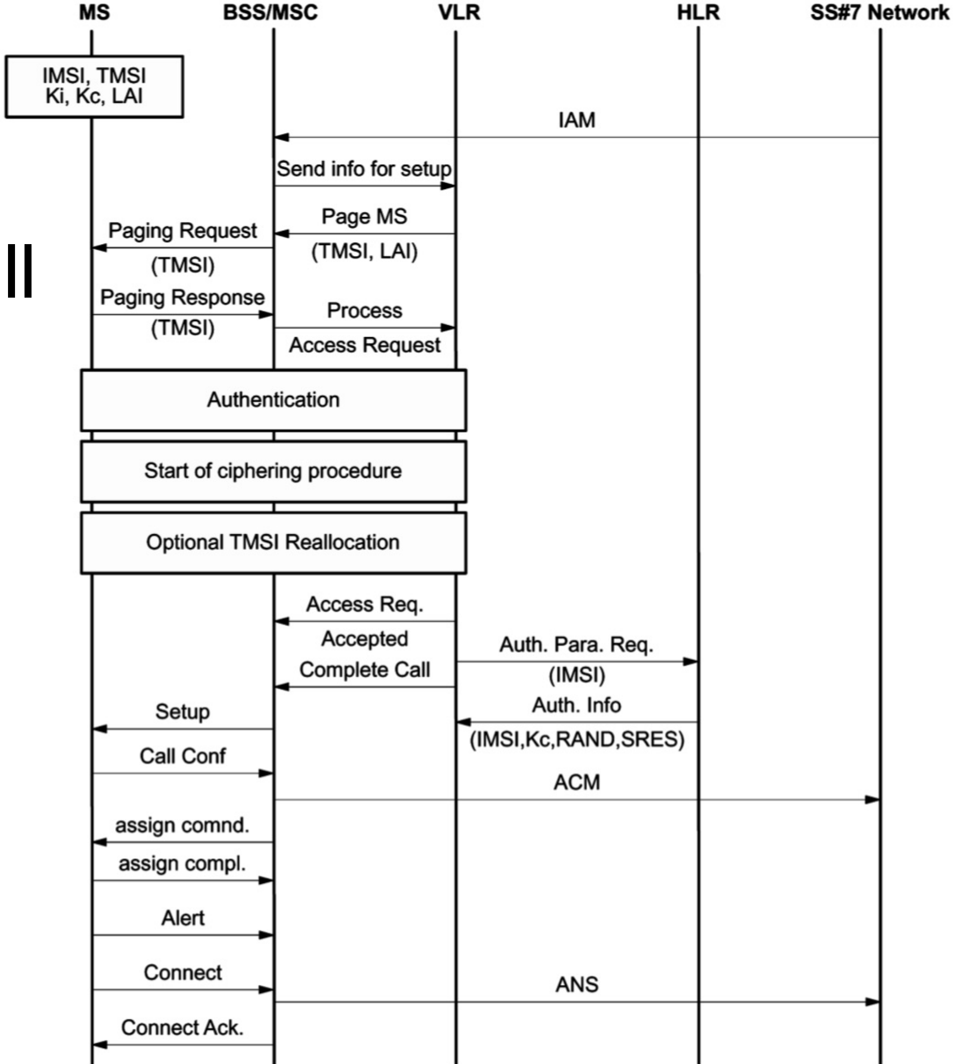
2. GSM

9.4 Outgoing Call



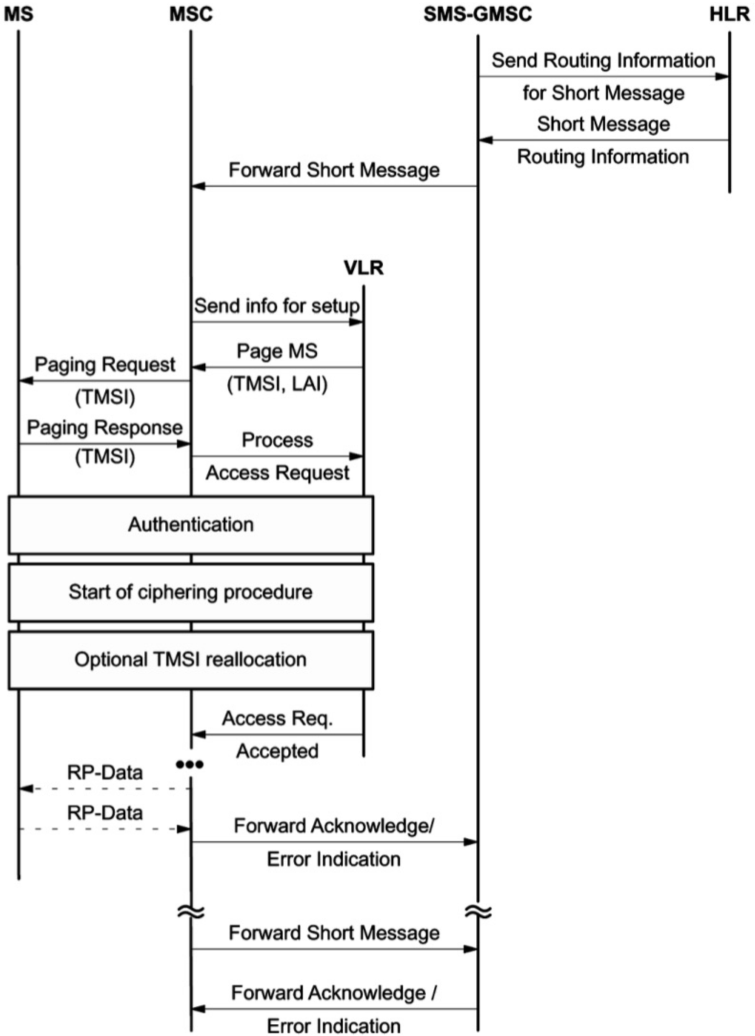
2. GSM

9.5 Incoming Call



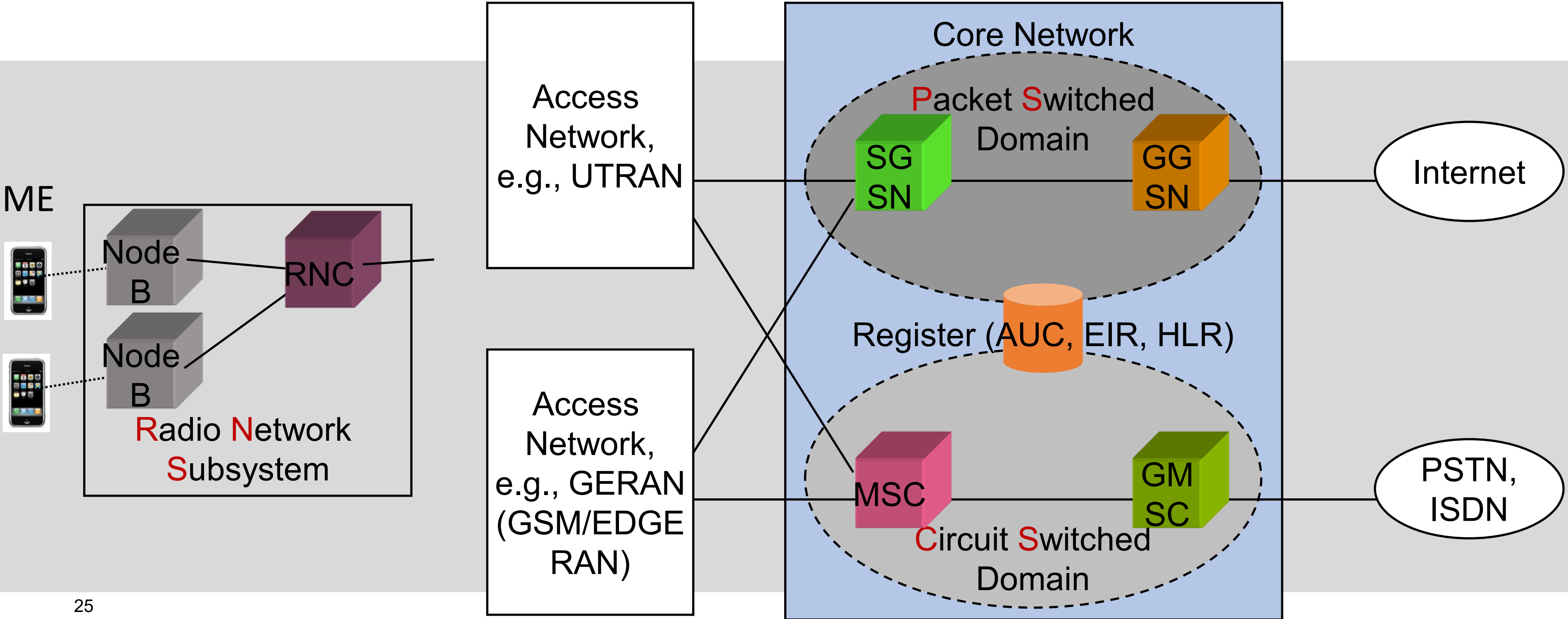
2. GSM

9.6 SMS


MS
MSC
SMS-GMSC
HLR
Send Routing Information for Short Message
Short Message Routing Information
Forward Short Message
VLR
Send info for setup
Page MS (TMSI, LAI)
Paging Request (TMSI)
Paging Response (TMSI)
Process Access Request
Authentication
Start of ciphering procedure
Optional TMSI reallocation
Access Req. Accepted
RP-Data
RP-Data
Forward Acknowledge/ Error Indication
Forward Short Message
Forward Acknowledge / Error Indication

3. UMTS

1.1 Network Architecture (3GPP Release 99)



3. UMTS

1.2 Components

- Radio Network Controller
- Radio Access Network
- UMTS Terrestrial RAN
- General Packet Radio Service
- GPRS Support Node
- Serving GSN
- Gateway GSN
- Mobile Equipment
- Universal SIM

3. UMTS

2. UMTS Approaches Addressing GSM Security Weaknesses

- Possible active attacks by false networks
  → mutual authentication
- Encryption keys and credentials are transmitted in clear text between and within networks
  → network domain security
- Encryption only covers radio interface → 3G encryption between ME and RNC
- No data integrity
  → signaling integrity protection
- Home network does not know whether Serving Network authenticates mobile users
  → mandatory integrity and authentication

3. UMTS

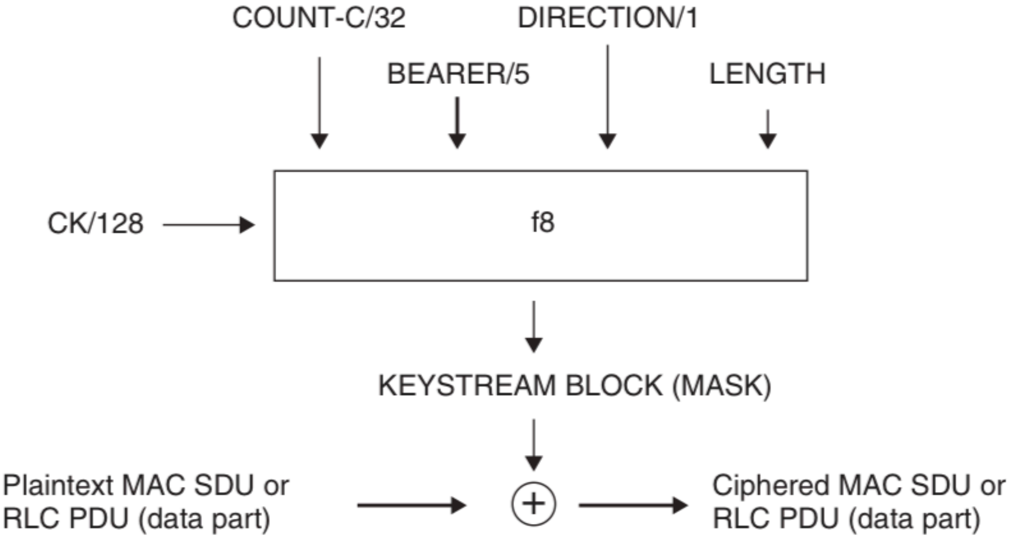
3. Authentication and Key Agreement

- Permanent key K shared between ME and AUC. K never leaves ME and AUC.
- Authentication after transmitting IMSI or TMSI to VLR or SGSN
- AUC generates authentication vectors for users.

- Prerequisites
  - Users trust their home networks.
  - Secure network between home network and SN
  - Symmetric key-based functions f1-f5
- Goals
  - Entity authentication
  - Session key agreement and freshness
  - User identity confidentiality (TMSI)

3. UMTS

4. Encryption


COUNT-C/32
BEARER/5
DIRECTION/1
LENGTH
CK/128
f8
KEYSTREAM BLOCK (MASK)
Plaintext MAC SDU or RLC PDU (data part)
Ciphered MAC SDU or RLC PDU (data part)

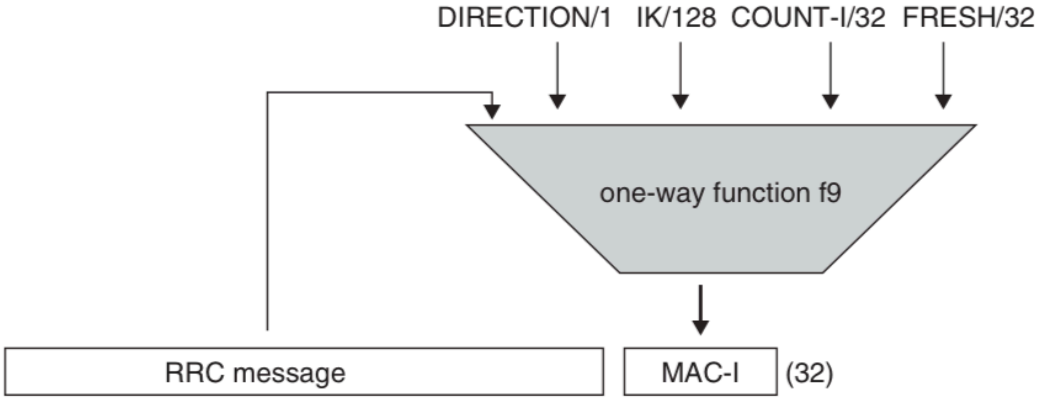
Parameters

- Cipher Key is obtained by RNC from AUC.
- Counter: Connection Frame Number and Hyperframe Number
- Radio Bearer Identity
- Direction: uplink / downlink

Radio Link Control

3. UMTS

5. Integrity Protection



Parameters

- Secret key IK generated during AKA procedure
- Random number FRESH as protection against replay attacks

Radio Resource Control

3. UMTS

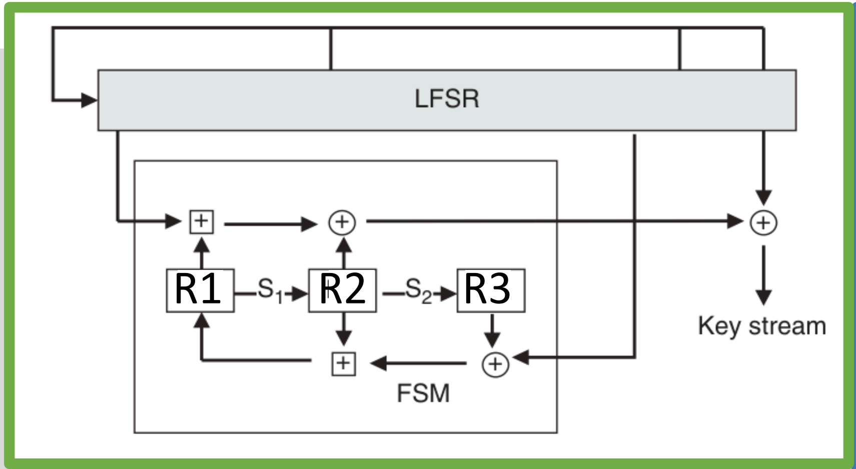
6. Identity Confidentiality

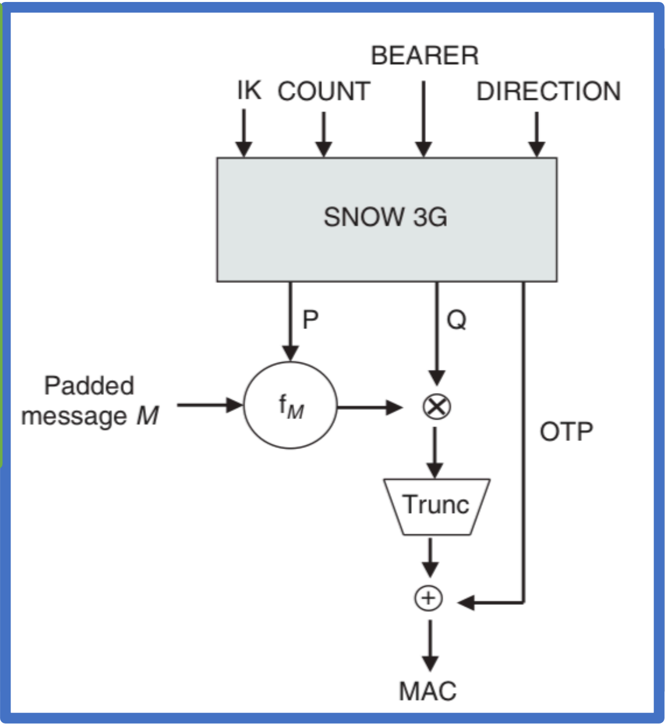
- TMSI and P-TMSI for CS and PS domains.
- (P-)TMSI are transferred to user once encryption has been turned on.
- (P-)TMSI are used for paging, location update, attach and detach procedures.
- If UE arrives in a new area, the association between IMSI and (P-)TMSI can be derived from old location area.
- If old area can not be determined or contacted, then IMSI must be requested from ME.
- Possible risk at places where people switch on their phones, e.g., airports

3. UMTS

7. Cryptographic Algorithms

- KASUMI
- SNOW 3G
- UIA2



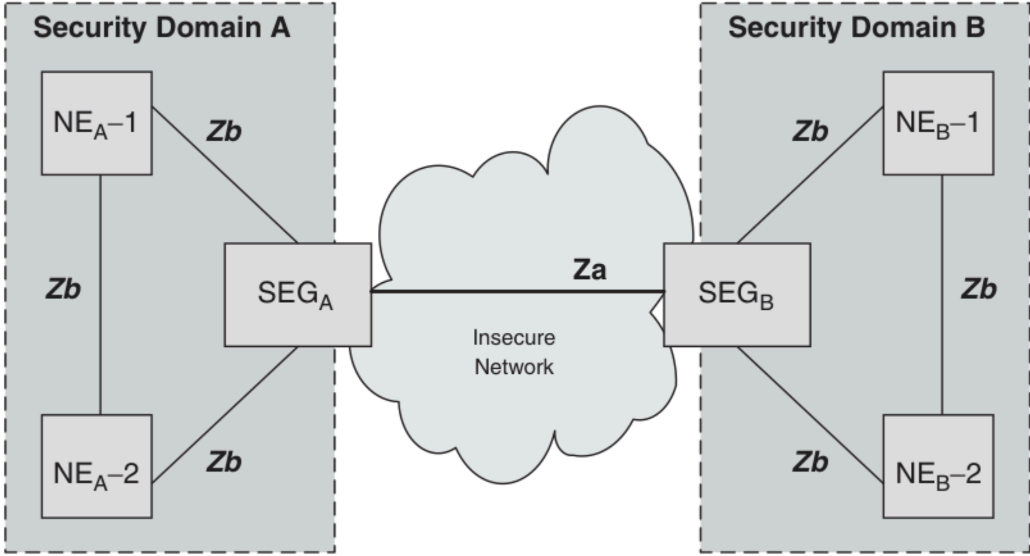


Linear Feedback Shift Register
Finite State Machine
Register
One Time Password

3. UMTS

8. Network Domain Security

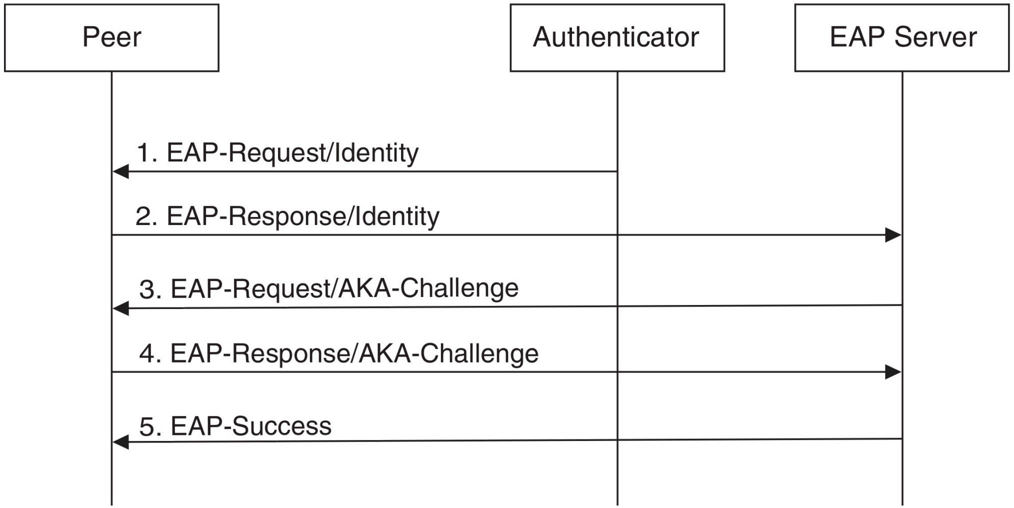
- Security domain is administrated by a single authority, i.e., a single operator
- Security gateways at border of domains
- Services by NDS/IP
  - Data integrity
  - Data origin authentication
  - Anti-replay protection
  - Confidentiality
  - Limited protection against traffic analysis
- Mechanisms
  - IPsec ESP SAs
  - IKE
  - Transport Layer Security



3. UMTS

9. WLAN Interworking with EAP-Authentication and Key Agreement

- Security procedures to support users accessing 3G networks via WiFi
- Approach: use (U)SIM for Authentication, Authorization, and Accounting
- EAP methods
  - EAP-SIM (GSM)
  - EAP-AKA (3G)
    3. EAP server fetches authentication vectors and sends random number and authentication token to peer.
    4. Peer decrypts parts of message with keys from USIM and responds to challenge
    5. EAP Server checks RES/XRES and confirms message integrity.



4. LTE

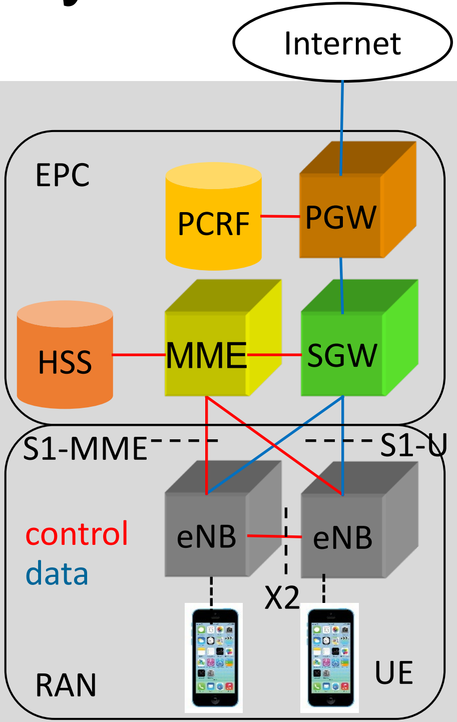
1. Network Architecture: Evolved Packet System

Evolved Packet Core

- Mobility Management Entity
  - Authentication
  - Mobility management and handover
  - Bearer and connection management
- Home Subscription Server
  - stores authentication and subscription information
- PDN Gateway
  - bridging EPC to the Internet
  - Packet Data Network
- Policy and Charging Rules Function
  - Filtering rules for PGW
- Serving Gateway
  - Mobility anchor for UE

Radio Access Network

- evolved Node B
  - Scheduling and resource control
- User Equipment



4. LTE

2.1 EPS Security Features

- User and Device Confidentiality
  - Transmission of device identities after traffic protection activation
- Mutual UE and Network authentication
- User and Signaling Data Confidentiality
- Signaling Data Integrity
- eNB platform security
- Lawful interception
- Emergency calls
- Interworking Security with other systems
- Network Domain Security (from 3G)

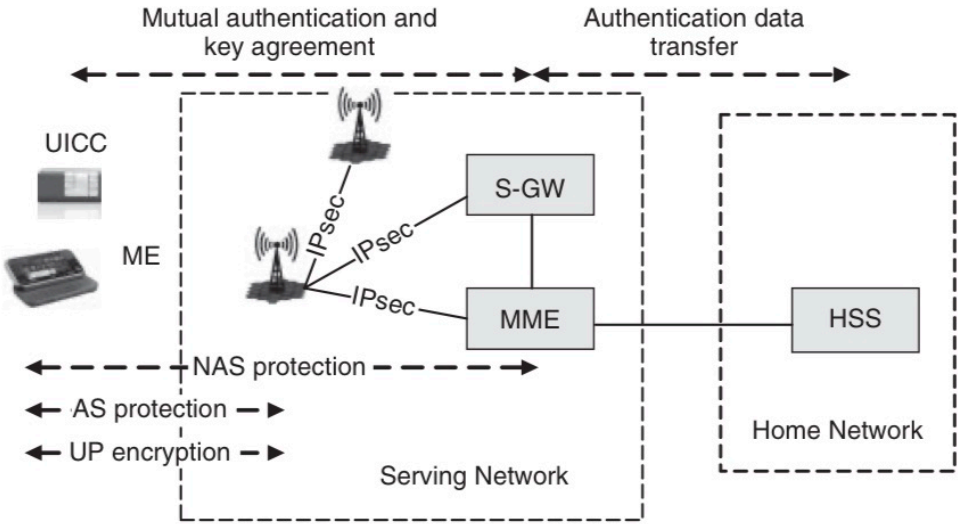
4. LTE

2.2 EPS Design Decisions

- Permanent Security Association between UE and AUC
- Reuse of 3G USIMs, but no reuse of 2G SIMs
- Delegated Authentication
  - MME requests authentication vectors from HSS, checks authentication response and distributes session keys.
- Termination of encryption and integrity protection deeper in the network
  - End-to-end encryption between UE and MME for Non-Access Stratum signaling
- Advanced Key Hierarchy
- Key Separation in Handovers
  - Problem: Key handover in case of handovers
  - MME must provide fresh keys to eNBs after handovers.

4. LTE

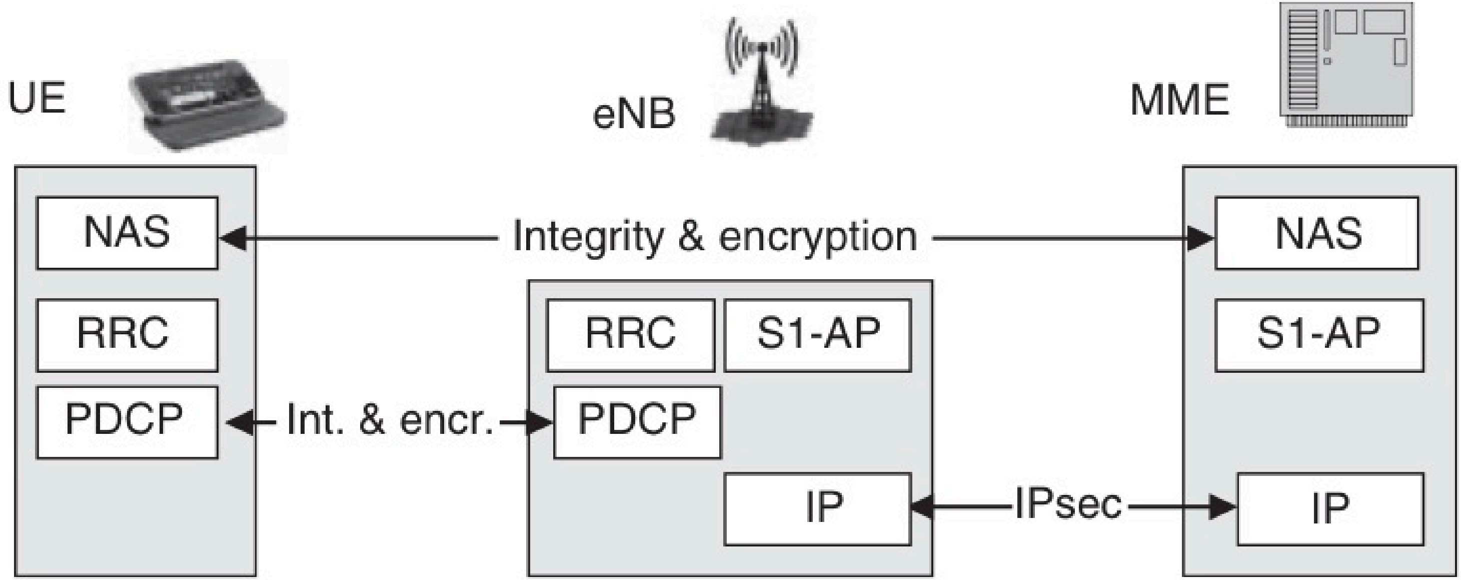
3.1 EPS Security Architecture



- MME triggers AKA protocol with UE (= ME + UICC).
- MME and UE share key K_{ASME} to derive keys for encryption and authentication for signaling and data
- Another key is derived for eNB

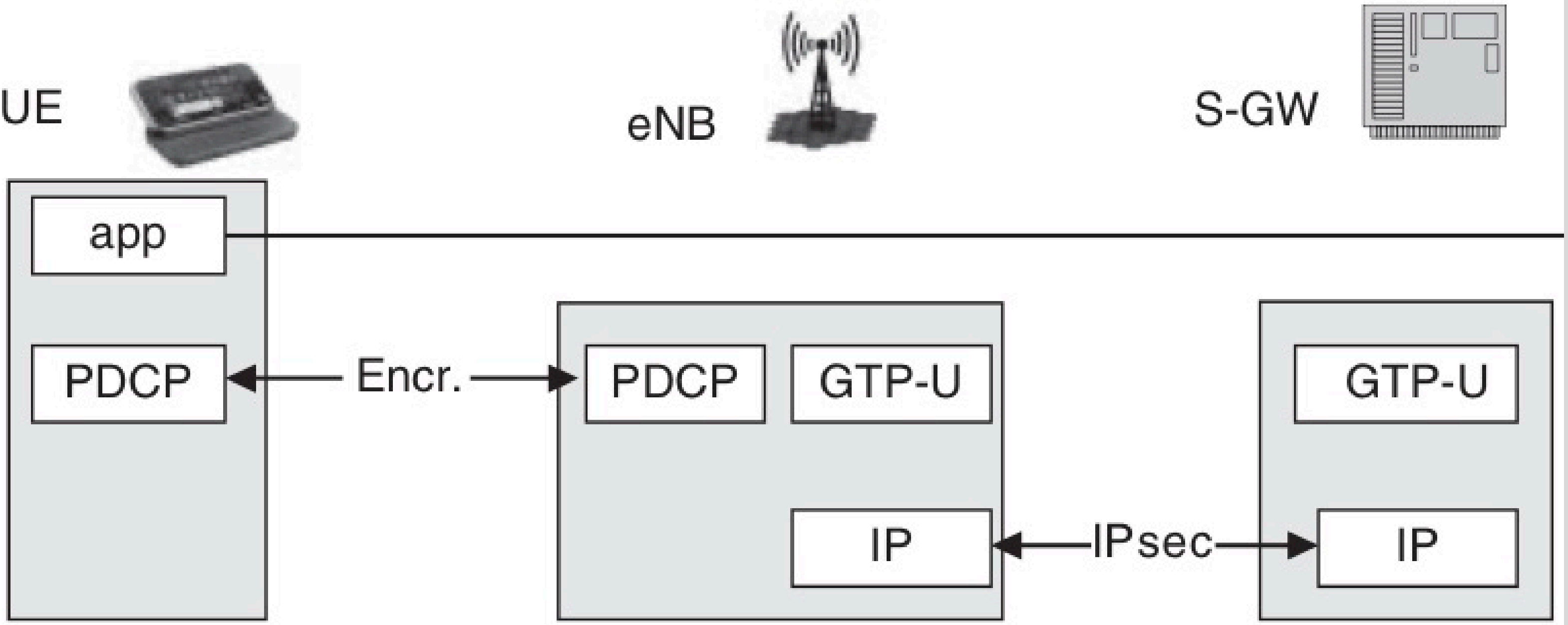
4. LTE

3.2 EPS Signaling Plane Protection



4. LTE

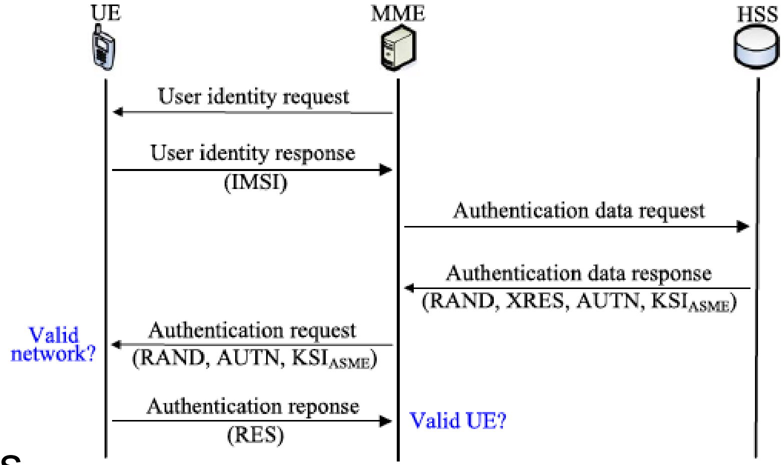
3.3 Data Plane Protection



4. LTE

4.1 EPS Authentication and Key Agreement

- Identification
  - User identification based on IMSI using Globally Unique Temporary UE Identity (like TMSI)
  - Transmission of IMSI after activation of NAS security
- AKA procedure
  - Generation of EPS authentication vectors
  - Mutual authentication of SN and UE
  - Keys are bound to SN
  - Distribution of authentication data inside SN

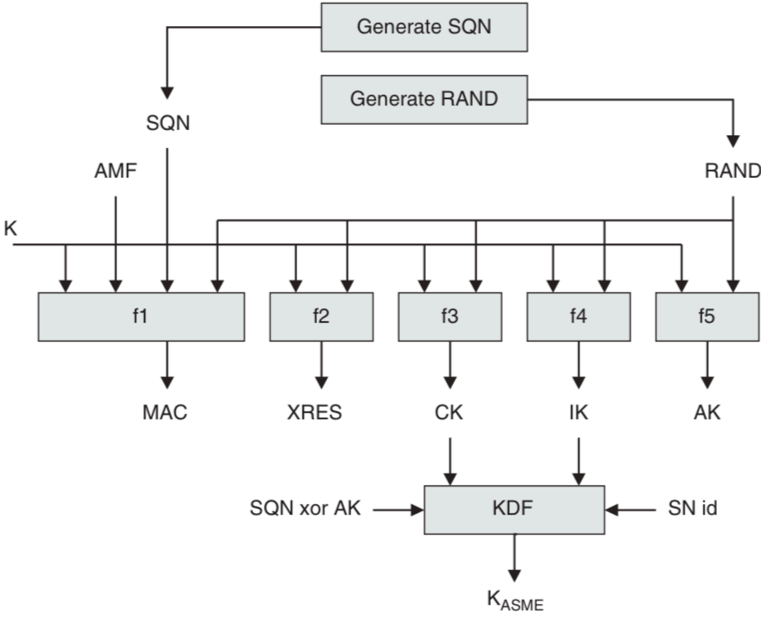


UNIVERSITÄT BERN

4. LTE

4.2 Authentication Vector Generation in HSS

- Sequence Number
- expected Response
- 128-bit random number
- K_{ASME}: local master key
- Access Security Management Entity
- Cipher Key
- Integrity Key
- Anonymity Key
- Authentication Management Field
- Key Derivation Function
- Authentication Token



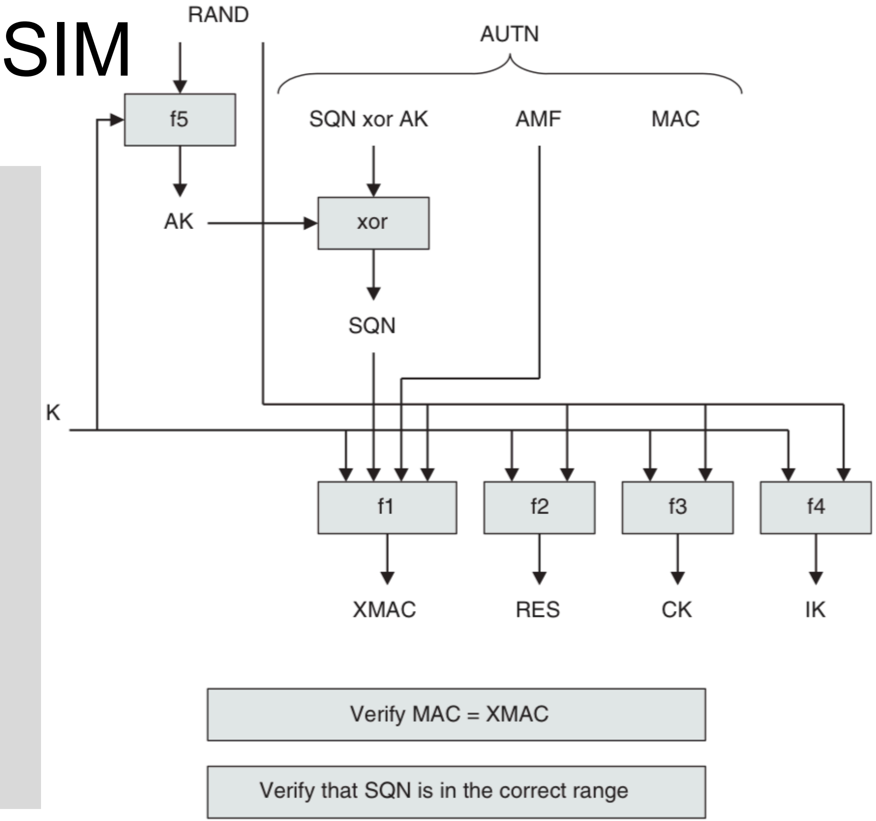
AUTN := SQN xor AK || AMF || MAC

UMTS AV := RAND || XRES || CK || IK || AUTN

EPS AV := RAND || XRES || K_{ASME}|| AUTN

4. LTE

4.3 User Authentication in USIM



4. LTE

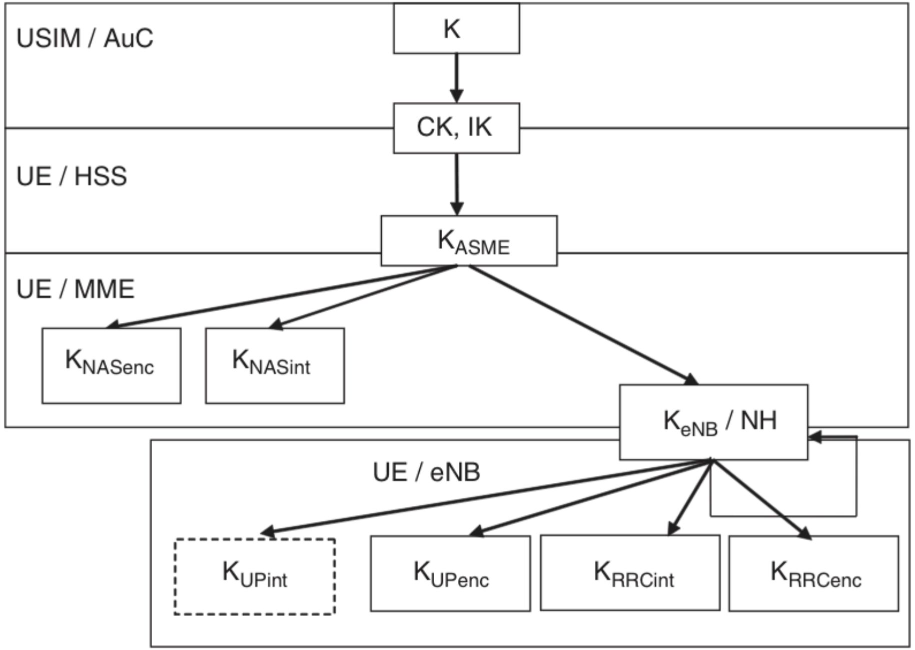
5. Distribution of Authentication Data inside SNs

- GUTI is used for signaling
- Problem
  - A new MME (due to reattachment or mobility) does not know GUTI.
- Solution
  - Translation of GUTI into IMSI by old MME or request it from UE
  - Exchange of authentication data
    - Transfer of EPS security context and EPS Authentication Vector between MMEs of the same SN
    - Transfer of EPS security context (includes SN ID) between MMEs of trusted SNs

4. LTE

6. Key Hierarchy

- Cryptographic Keys are derived from intermediate key K_{ASME}.
- K_{ASME} is generated at UE and distributed from HSS to MMEs.
- K_{ASME} is less exposed and always kept in the core network.
- K_{ASME} does not have to be renewed often.



4. LTE

7. Security Contexts

= security parameters, cryptographic keys, and algorithm identifiers

- EPS NAS context to protect signaling between MME and UE
  - K_{ASME}, UE security capabilities, NAS uplink and downlink COUNT
- EPS AS context to protect radio link between UE and eNB
  - Cryptographic keys at AS level

- partly stored at USIM
- can be transferred from one MME to another,
  even in different networks,
  or from MME to eNB.

4. LTE

8.1 General Handover Options

UE and eNB share keys,
new eNB also must share a key.

- Options how to transfer keys
  - **Delegated authentication**, e.g., from HSS to MME by deriving a key from root key.
  - **Key request** from base station to Key Distributor
  - **Pre-distribution** of base station specific keys from KD to base stations
  - **Optimistic access**: UE uses preliminary ticket to get access prior to final authentication
  - **Pre-authentication**:
    UE authenticates to multiple base stations through a single base station and pre-establishes keys
  - **Session Keys Context** contains multiple session keys encrypted for each base station and is moved between them.

4. LTE

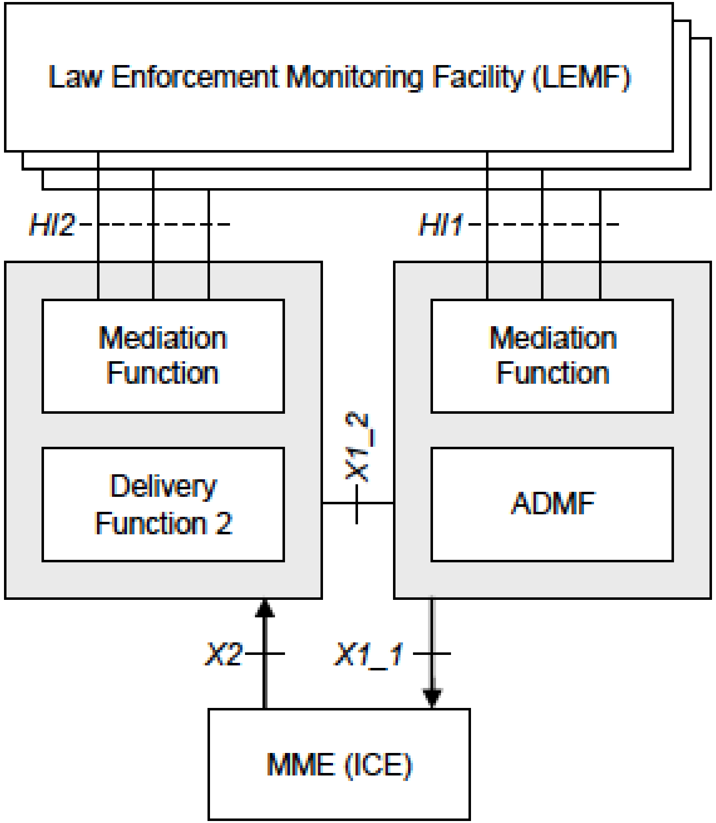
8.2 LTE Key Handling in Handovers

- MME is informed before/after S1/X2 handover.
- MME can provide fresh key material to target eNB before/after S1/X2 handover.
- LTE provides backward key separation, i.e., source base station uses a one-way Key Derivation Function for the target base station specific key.
  → target base station can not deduce source base station key

4. LTE

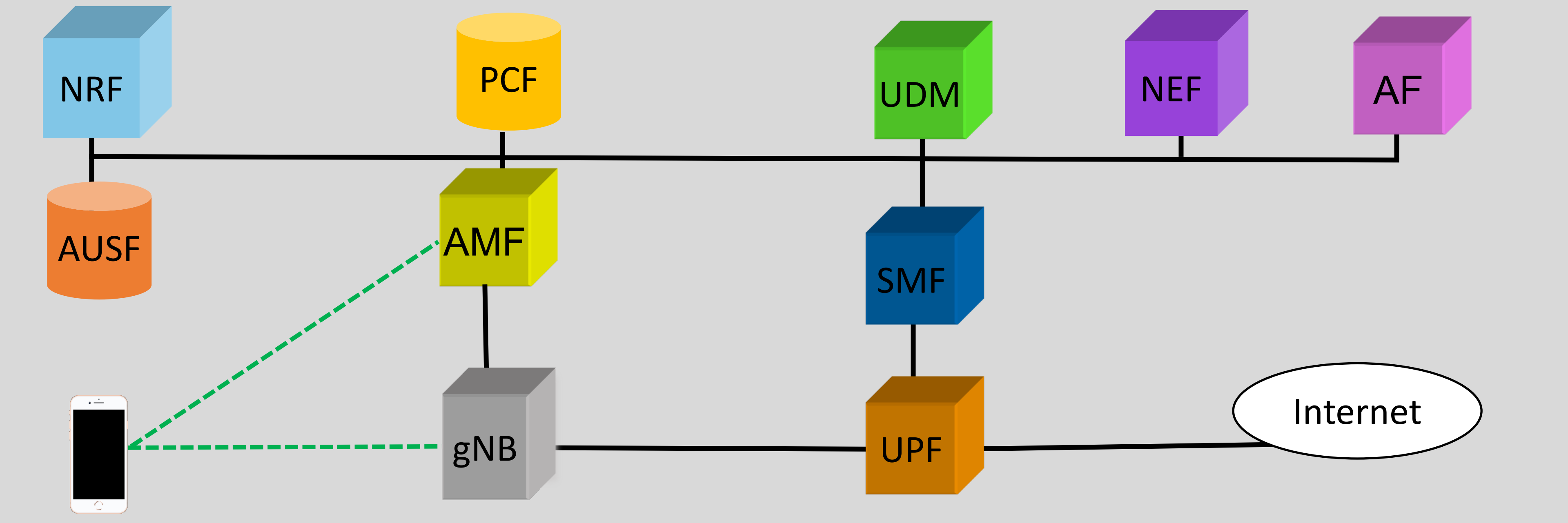
9. Lawful Interception

- Authorized and official access to private communications
- can also be implemented at HSS and S-GW / P-GW
- Administration Function



5. 5G

1.1 Service-Based Network Architecture



5. 5G

1.2 Network Architecture Components

- Access and Mobility Management Function
  - handles mobility procedures.
  - terminates NAS signalling.
  - mobility management
- Authentication Server Function
  - supports UE authentication.
- Network Exposure Function
  - provides an interface for outside applications to communicate with the 3GPP network.
- Network Repository Function
  - provides registration & discovery functionality so that Network Functions can discover each other.
- Network Slice Selection Function
  - assists in the selection of suitable network slice instances for users.

5. 5G

1.3 Network Architecture Components

- Policy Control Function
  - supports unified policy framework to govern network behaviour
  - provides policy rules to Control Plane function(s) and to enforce them
- Session Management Function
  - supports the establishment, modification and release of a data session
  - configuration of traffic steering policies at the UPF
  - IP address allocation and policy enforcement.
- Unified Data Management
  - Access authorization based on subscription data, e.g., roaming restrictions
  - UE's Serving NF Registration Management
  - Support to service/session continuity, e.g., by keeping SMF assignment of ongoing sessions.
- User Plane Function
  - serves as the anchor point for intra/inter Radio Access Technology mobility, packet routing, traffic reporting
  - handles user plane Quality of Service.

5. 5G

2.1 Features

- New Radio
  - Millimeter waves
  - Directional transmission
  - Beam-forming
  - Positioning
  - Multiple Input Multiple Output
- New Services
  - e.g., massive Machine Type Communications, Internet of Things
- Softwarization
  - Network Function Virtualization
    - Hypervisors
    - Application-level protocols such as HTTP
  - Network Slicing
  - Edge Computing
  - Software-Defined Networking
    - Centralized management & monitoring

5. 5G

2.2 Mobile Edge Protection

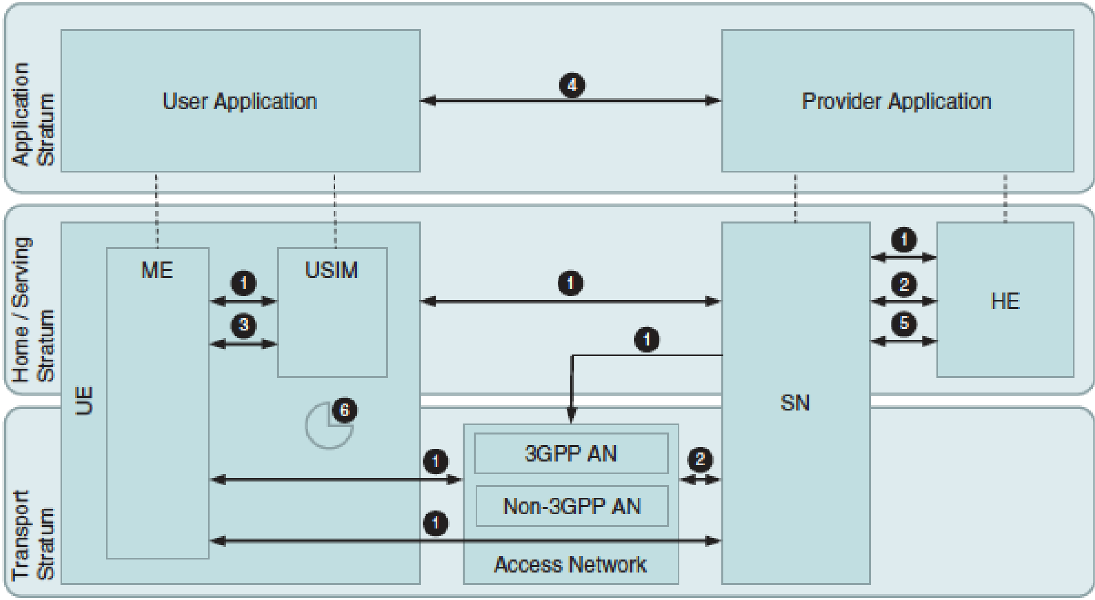
- Protection of cached data and authentication vectors

- Protection of virtualized computing environments
  - Isolation might help.
  - But resources must be protected.

5. 5G

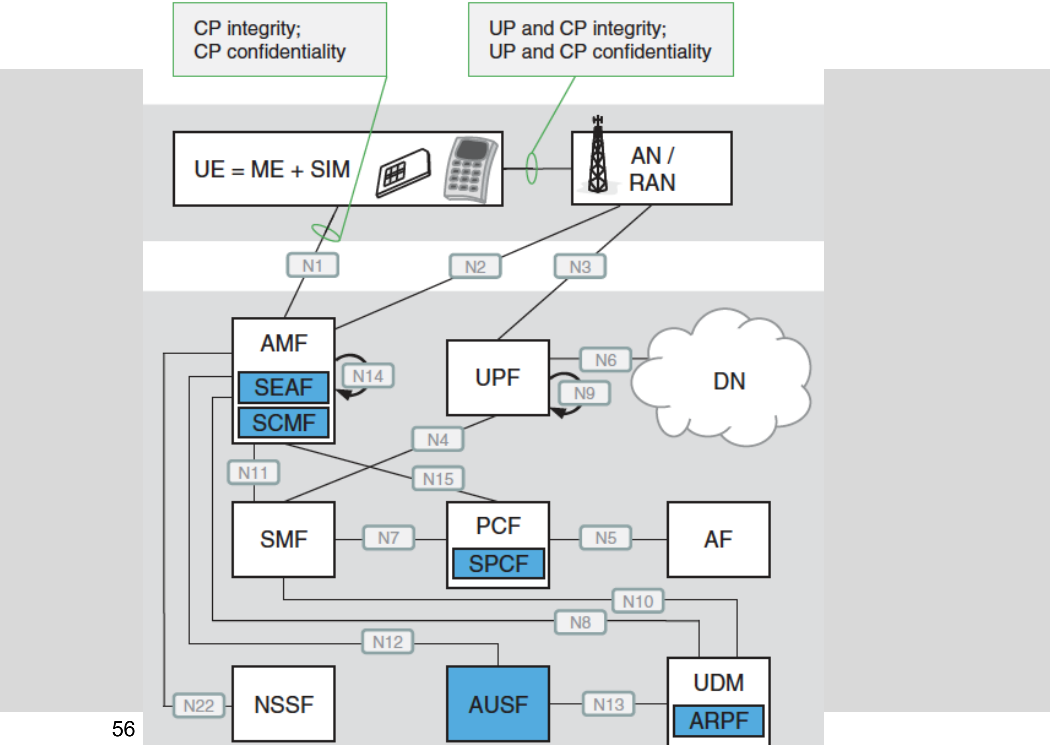
3. 3GPP System Security Architecture

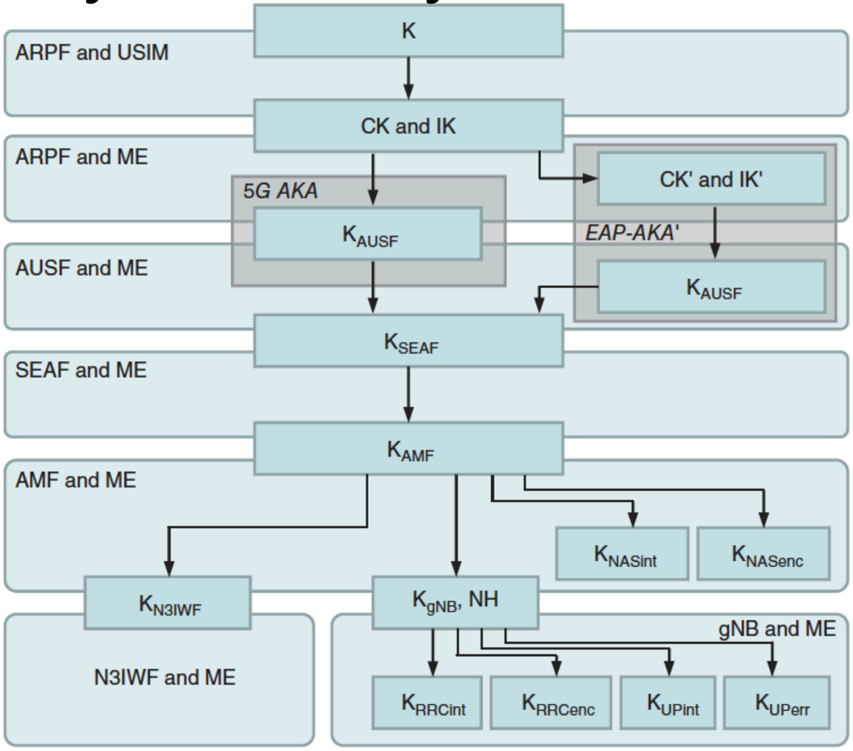
1. **Network access security** features for UE to authenticate and access services securely. These features protect the radio interface and deliver security context from SN to UE.
2. **Network domain security** features to securely exchange user data and signalling.
3. **User domain security** features secure user access to ME.
4. **Application domain security** features for applications to exchange messages securely.
5. **Service-based architecture domain** security features include network element registration, discovery, authorization security, and protection for the service-based interfaces.
6. **Visibility and configurability of security** features to inform user if a security feature is in operation.



5. 5G

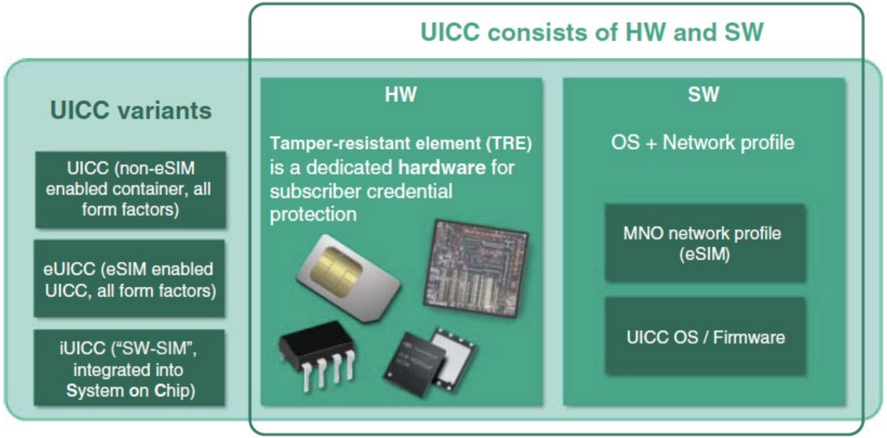
4. Security Architecture and Key Hierarchy





5. 5G

5. Universal Integrated Circuit Card Evolution



UICC consists of HW and SW

UICC variants

- UICC (non-eSIM enabled container, all form factors)
- eUICC (eSIM enabled UICC, all form factors)
- iUICC ("SW-SIM", integrated into System on Chip)

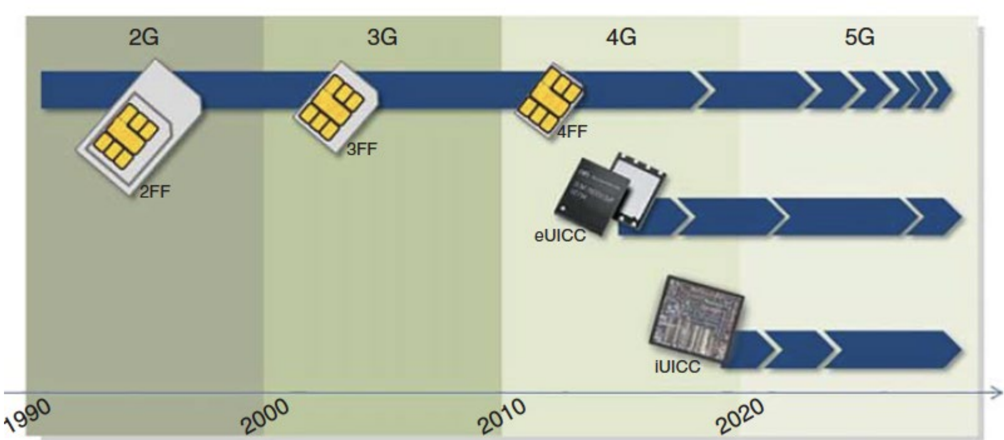
HW

Tamper-resistant element (TRE) is a dedicated **hardware** for subscriber credential protection

SW

OS + Network profile

- MNO network profile (eSIM)
- UICC OS / Firmware



Thanks a lot

for your Attentation

Prof. Dr. Torsten Braun, Institut für Informatik

Bern, 25.04.2022 – 02.05.2022