Security Architectures of Mobile Systems

Valtteri Niemi
University of Helsinki

AMICT'2015
Petrozavodsk, 13 May

Contents

- Background and scope
- GSM
  - design decisions
    - *a priori* and *a posteriori* decisions
  - security mechanisms
- 3G
  - design decisions
  - security mechanisms
- LTE (4G)
  - design decisions
  - security mechanisms
- 5G perspectives

Background and scope

Mobile systems

- Cellular systems
  - GSM, 3G, LTE (= 4G), …
  - Standardized by ETSI, 3GPP
  - Huge global footprint
- Other wireless access technologies
  - e.g. WiFi
- Mobile apps
  - e.g. facebook
- Other technologies in mobile devices
  - Camera, GPS, accelerometer, ….
- Services
  - Communication services, e.g. Skype, Whatsapp,…
  - Location-based services
  - Cloud services
  - …..

Mobile systems

- Cellular systems
  - GSM, 3G, LTE (= 4G), …
  - Standardized by ETSI, 3GPP
  - Huge global footprint

Our scope

- Other wireless access technologies
  - e.g. WiFi
- Mobile apps
  - e.g. facebook
- Other technologies in mobile devices
  - Camera, GPS, accelerometer, ….
- Services
  - Communication services, e.g. Skype, Whatsapp,…
  - Location-based services
  - Cloud services
  - …..

Information security

- System security
  - e.g. trying to ensure that the system does not contain any weak parts.
- Application security
  - e.g. Internet banking
- Protocol security
  - e.g. how to achieve security goals by executing well-defined communication steps.
- Platform security
  - e.g. system depends on correctness of OS in all elements.
- Security primitives
  - basic building blocks on top of which all protection mechanisms are built.
  - e.g. cryptographic algorithms, but also more concrete items like a protected memory.

Information security

Our (main) scope

- System security
  - e.g. trying to ensure that the system does not contain any weak parts.
- Application security
  - e.g. Internet banking
- Protocol security
  - e.g. how to achieve security goals by executing well-defined communication steps.
- Platform security
  - e.g. system depends on correctness of OS in all elements.
- Security primitives
  - basic building blocks on top of which all protection mechanisms are built.
  - e.g. cryptographic algorithms, but also more concrete items like a protected memory.

Design of a secure system

- Threat analysis
  - list all possible threats against the system, regardless of difficulty or cost
- Risk analysis
  - weight of threats estimated
  - both probability of the attack and potential damage taken into account
- Requirements capture
  - based on risk analysis, decide what kind of protection is required for the system
- Design phase
  - build actual protection mechanisms to meet requirements
  - Existing building blocks, e.g. security protocols, are identified, possibly new mechanisms are developed, and a security architecture is created
- Security analysis
  - carrying out an evaluation of the results independently of the previous phase
- Reaction phase
  - reaction to all future security breaches cannot be planned beforehand → original design should allow enhancements

Design of a secure system

- Threat analysis
  - list all possible threats against the system, regardless of difficulty or cost
- Risk analysis
  - weight of threats estimated
  - both probability of the attack and potential damage taken into account
- Requirements capture
  - based on risk analysis, decide what kind of protection is required for the system
- Design phase
  - build actual protection mechanisms to meet requirements
  - Existing building blocks, e.g. security protocols, are identified, possibly new mechanisms are developed, and a security architecture is created
- Security analysis
  - carrying out an evaluation of the results independently of the previous phase
- Reaction phase
  - reaction to all future security breaches cannot be planned beforehand → original design should allow enhancements

Our (main) scope

Communication security

- *Authenticity*
  - Verifying the identities of the communicating parties
- *Confidentiality*
  - Limit the intelligibility of the communication just to parties involved
- *Integrity*
  - If all messages sent by the party *A* are identical to the ones received by the party *B* and vice versa, then integrity of the communication has been preserved
- *Non-repudiation*
  - For message sent by *A,* this implies that *A* cannot later deny sending of it
- *Availability*
  - This is an underlying pre-requisite for communication: a channel must be available

Communication security

Our (main) scope

- *Authenticity*
  - Verifying the identities of the communicating parties
- *Confidentiality*
  - Limit the intelligibility of the communication just to parties involved
- *Integrity*
  - If all messages sent by the party *A* are identical to the ones received by the party *B* and vice versa, then integrity of the communication has been preserved
- *Non-repudiation*
  - For message sent by *A,* this implies that *A* cannot later deny sending of it
- *Availability*
  - This is an underlying pre-requisite for communication: a channel must be available

GSM

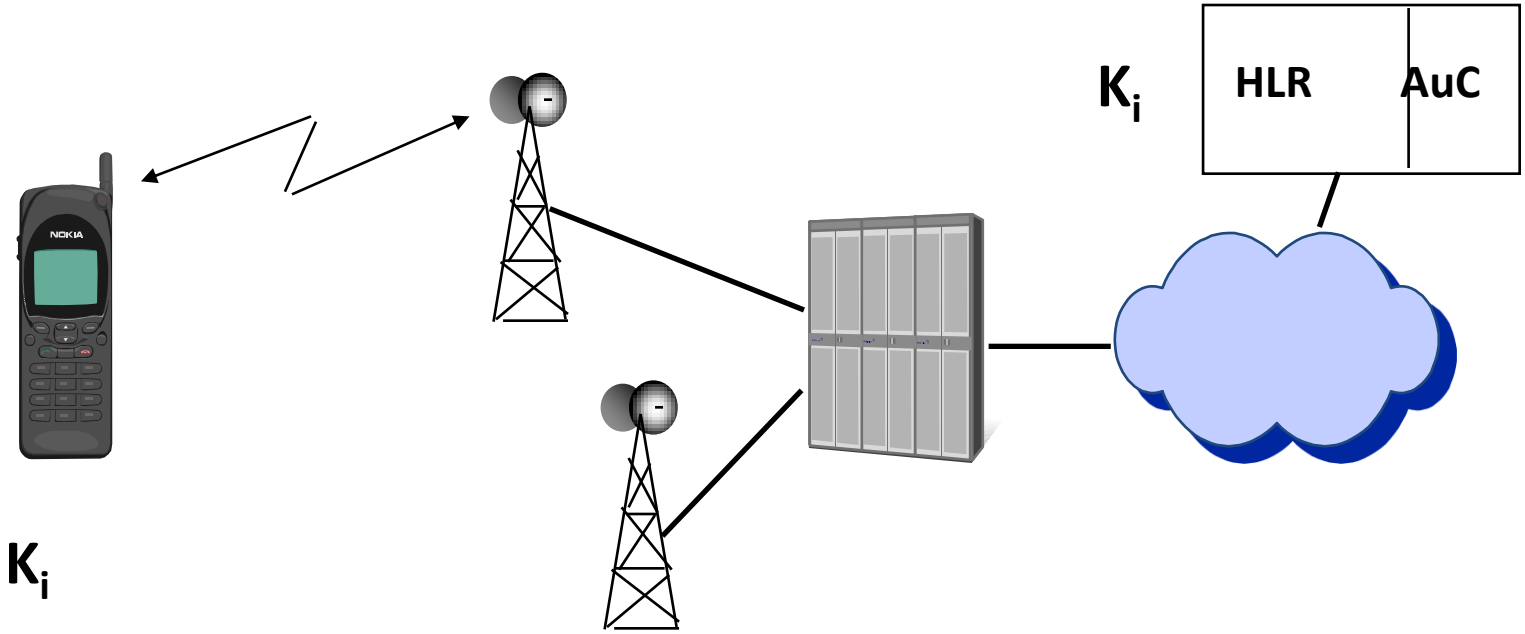
Landscape at the time of design

- Stakeholders: European ***national*** telecom operators
- Target: ***supplement*** for fixed networks (in Europe)
- Use case: voice calls
- Tight ***export control*** of crypto

a priori design decisions for GSM security

- GSM aimed to be ***as secure as the fixed*** networks to which it would be connected
- Security mechanisms should protect the system for ***20 years***

GSM access security



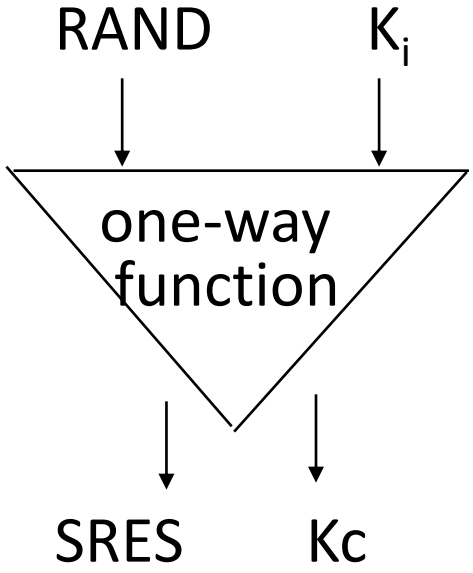
- The secret key of user i exists (and stays) only in two places:
  - in her own SIM card
  - in the Authentication Center

Trust model

- Each operator shares ***long term security association*** with its subscriber
  - Security association credentials stored in tamper-resistant identity module issued to subscriber (called the SIM or UICC)
- Operators may enter ***roaming agreements*** with other operators → a certain ***level of trust*** exists between the respective domains

Authentication of user i

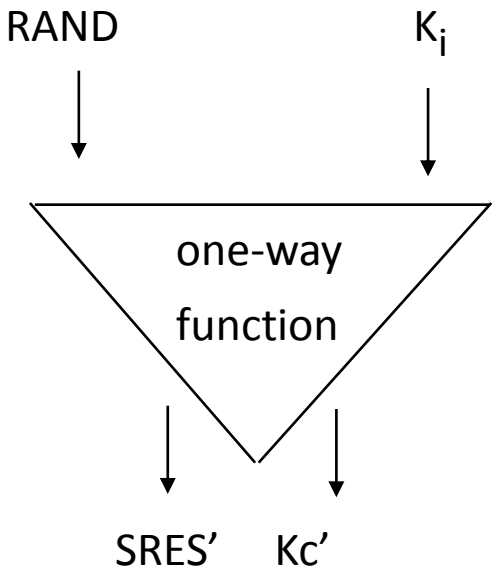
- Authentication Center chooses a random number RAND and computes



- The triple (RAND, SRES, Kc) is sent to the MSC/VLR.
- MSC/VLR sends RAND to the phone.
- The one-way function of computing SRES/Kc is called **A3/A8.** These are ***operator-specific*.**

Authentication cont'd

- The SIM card computes



and sends the output SRES' to the MSC/VLR.

- If SRES = SRES', then the call is accepted.

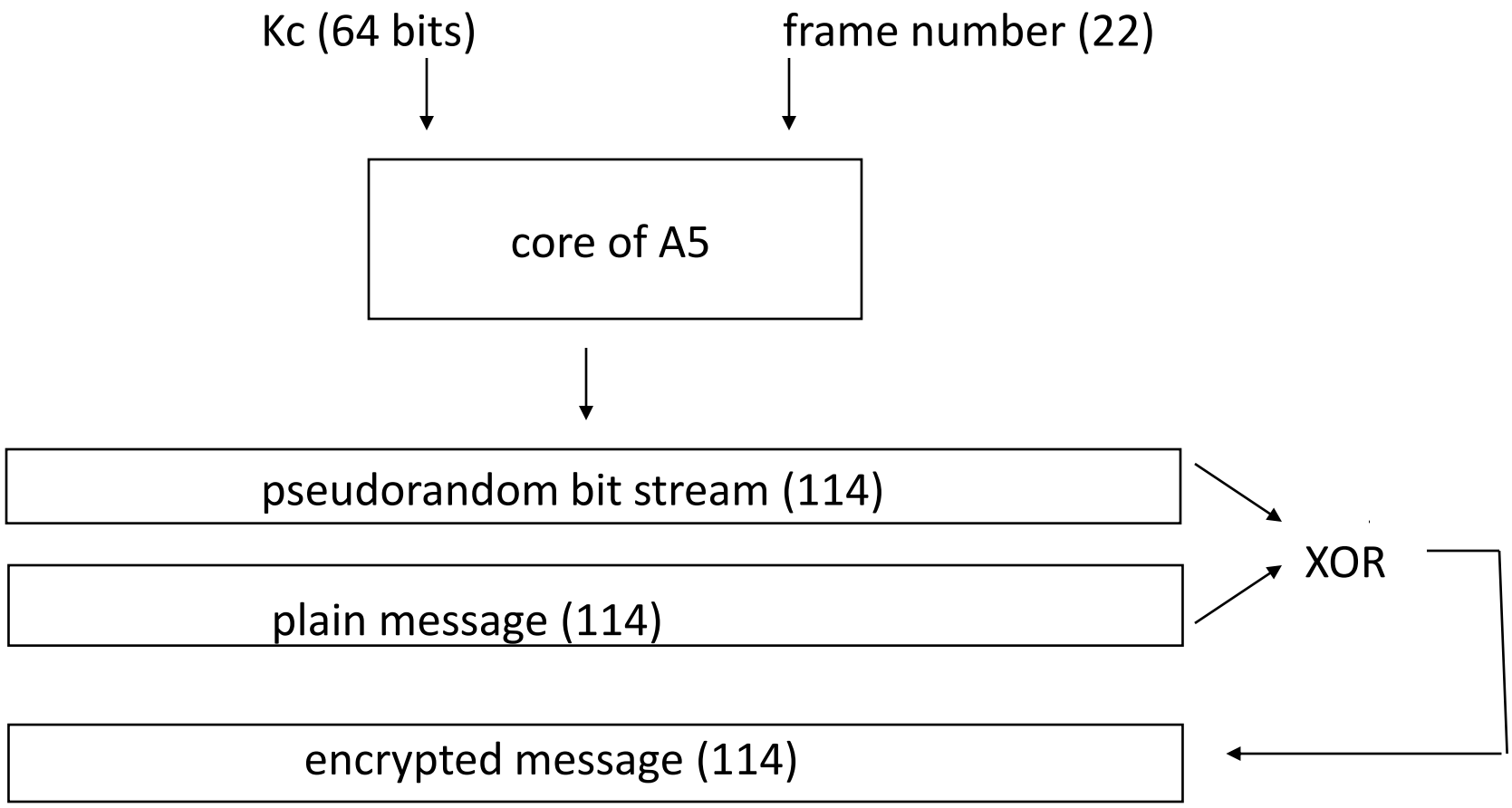
Encryption of the call

- During the authentication a secret key is exchanged:

  $$Kc = Kc'$$

  by which all calls/signalling are ***encrypted between the phone and the base station*** until the next authentication occurs.
- The encryption algorithm is called A5. The first two versions A5/1 and A5/2 were standardized but the specs are confidential and managed by GSM Association. Later, a third version A5/3 was created and is publicly available. All make use of **64-bit** keys Kc.
- Nowadays there is also a **128-bit** key algorithm A5/4.
  - Deployment of this is more difficult than in A5/3 case because longer keys require changes in many parts of the system

Structure of A5 stream cipher

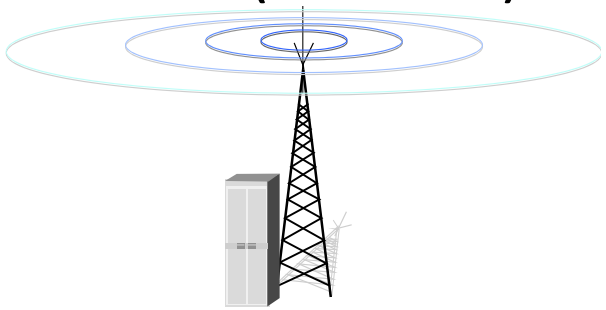


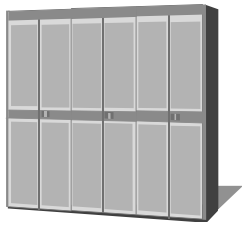
GSM security protocol

MS (SIM)
IMSI, **Ki**

MSC/VLR
(and BTS)

HLR
{{IMSI,**Ki**}}





IMSI / TMSI

IMSI

RAND

RAND, XRES, **Kc**

Kc

SRES

SRES=XRES ?

encrypted TMSI

a posteriori design decisions for GSM security

- ***Active attacks*** which involve impersonating a network element were intentionally ***not addressed***
- ***Authentication*** based on ***what you have:*** smart card
- ***Specs*** of cryptoalgorithms kept ***confidential***

Example of a ***reactive*** design decision

Barkan–Biham A5/2 Attack (from 2003)

Exploited weaknesses in cryptographic algorithms:

- A5/2 can be broken very fast

… and exploited also other legacy features in the GSM security system:

- A5/2 was a mandatory feature in terminals
- Call integrity based only on encryption
- Same Kc is used in different algorithms
- Attacker can force the victim MS to use the same Kc by RAND replay

An example attack: Decryption of strongly encrypted call

- Catch a RAND and record a call encrypted with Kc and A5/3
- Replay the RAND and tell the MS to use A5/2
- Analyse Kc from the received encrypted uplink signal
- Decrypt the recorded call with Kc

Countermeasure

- Withdrawal of A5/2 from all 3GPP terminals

GPRS security

- Similar to GSM security
- SGSN takes the role of MSC/VLR for authentication
- Encryption terminates also in SGSN
  - Embedded in Logical Link Layer (LLC)
  - Counter: frame number (22 bits) replaced by LLC counter (32 bits)
  - Algorithms:
    - GEA1 (confidential, weakest)
    - GEA2 (confidential)
    - GEA3 (publicly available)
    - GEA4 (Rel-9 addition; first to use 128-bit keys instead of 64-bit keys)

3G

Landscape at the time of design

- GSM became phenomenal success story
- Stakeholders: national operators, private challenger operators, regulators
- Target: truly global system

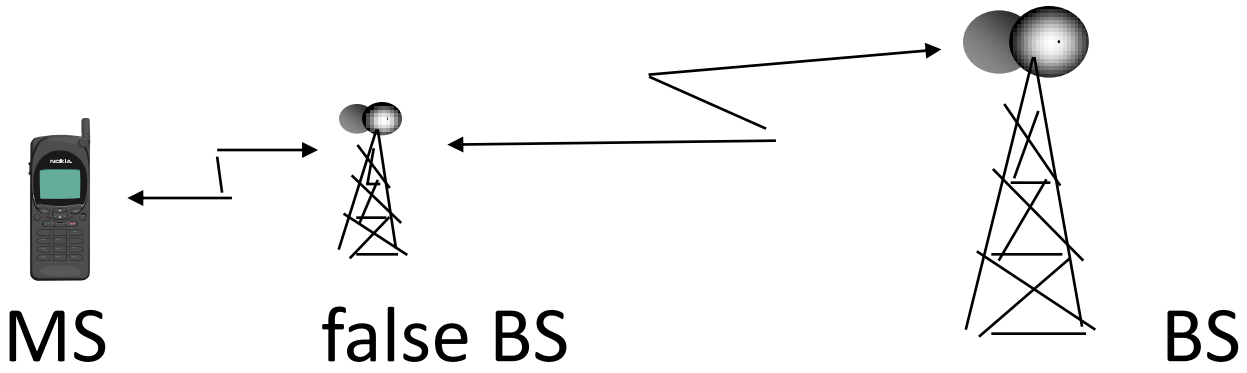
a priori design decisions for 3G security

- Move ***useful*** 2G security features to 3G
- Add countermeasures against ***real*** weaknesses in 2G

- Main *security characteristics* in GSM (= 2G) :
  - User authentication & radio interface encryption
  - SIM used as security module
  - Operates without user assistance
  - Requires minimal trust in serving network
- Main *weaknesses* in GSM:
  - Active attacks are possible (false BS etc.)
  - Authentication data (e.g. cipher keys) sent in clear inside one network and between networks
  - Cipher keys too short (if 64 bits)
  - Secret algorithms do not create trust

Active attack

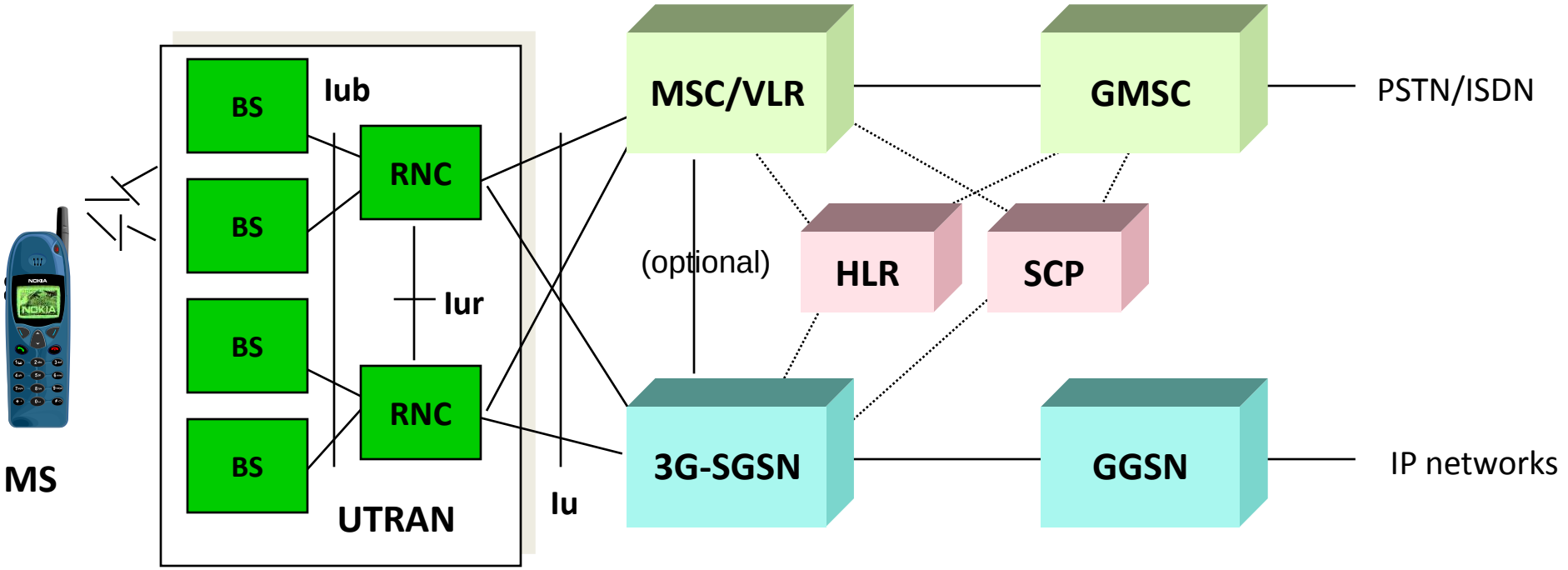
- A ***false*** element masquerades
  - as a base station towards terminal
  - as a terminal towards network
- Objectives of the attacker:
  - eavesdropping
  - stealing of connection
  - manipulating data



Design decisions for 3G architecture

- ***New radio*** interface and radio access network architecture
- ***Core*** network architecture ***inherited*** from GSM/GPRS

3G system architecture



Encryption & integrity

Transport of auth data

Execution of authentication

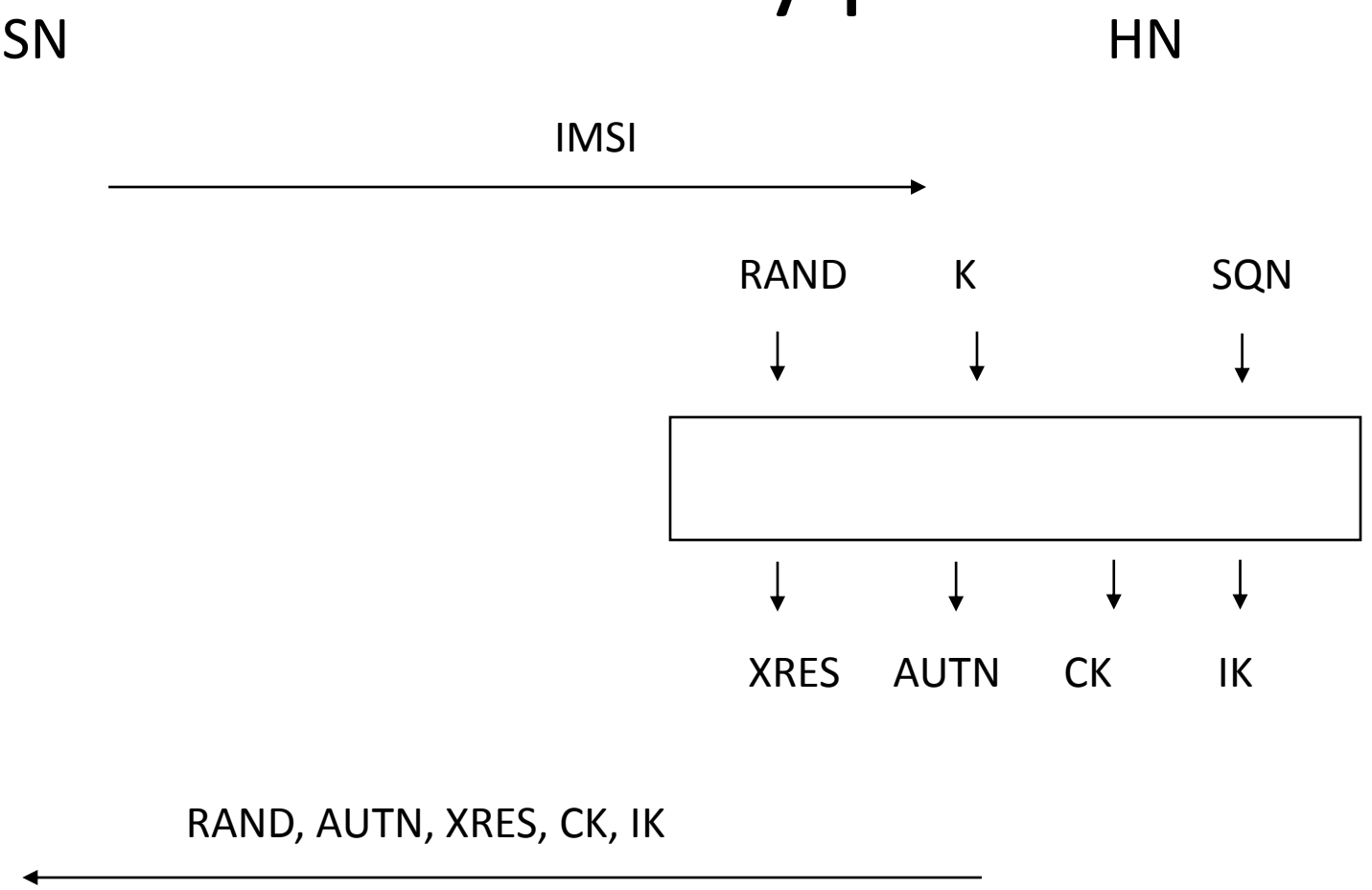
Mutual authentication

- There are three entities involved:
  - Home network HN (AuC)
  - Serving network SN (VLR/SGSN)
  - Mobile station MS (USIM)
- Executed whenever SN decides

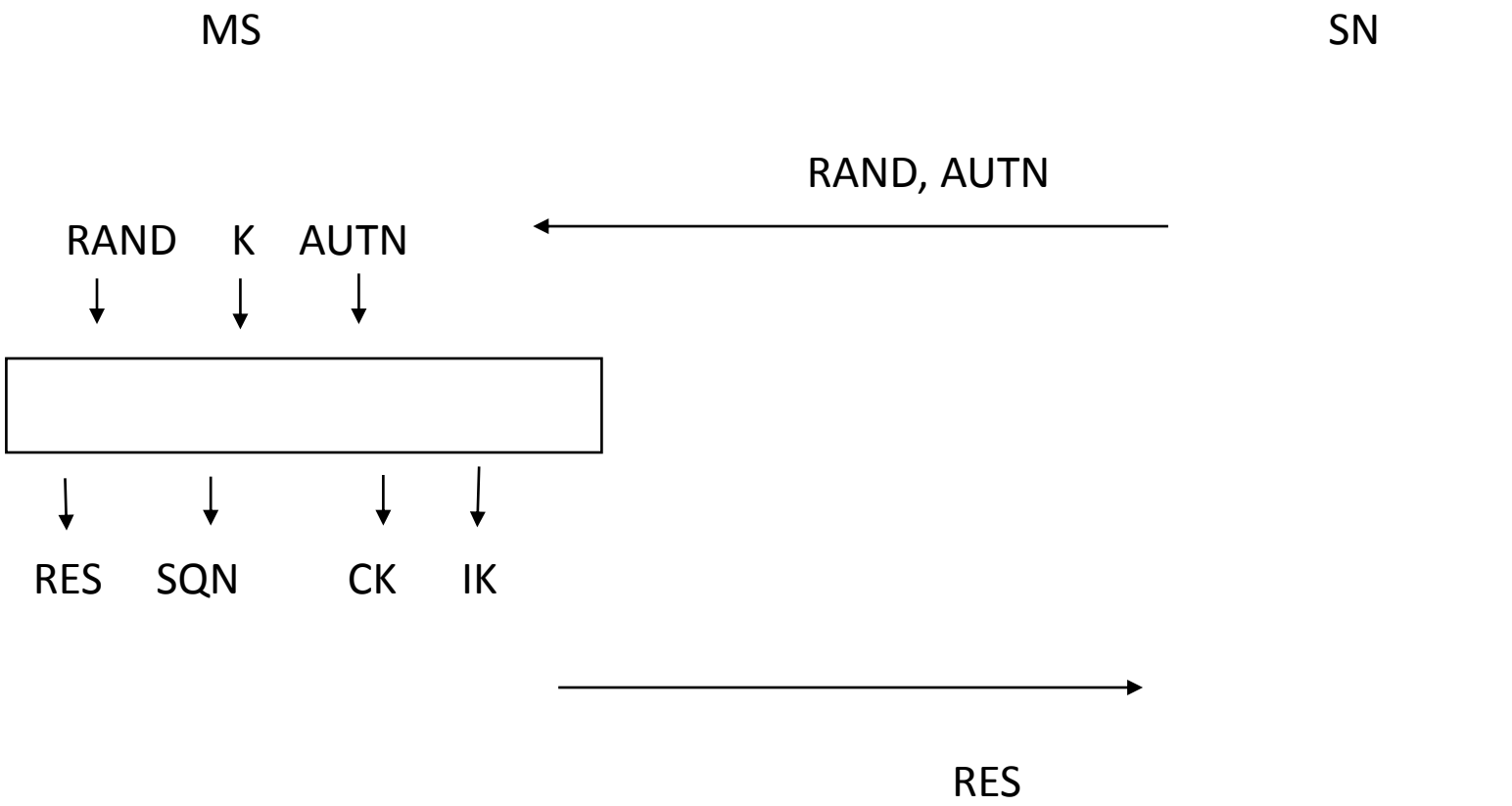
- The idea: SN checks MS's identity (as in GSM) and MS checks that SN has *authorization* from HN
- A *master key K* is shared between MS and HN
- GSM-like *challenge-response* in *user-to-network* authentication
- Network proves its authorization by giving a token AUTN which is protected by K and contains a sequence number SQN

- Each operator may use its *own algorithms* for authentication
- At the same time keys for ciphering and integrity checking are derived
- Ciphering and integrity checking are performed in MS and in RNC and these are independent of the authentication mechanism

Generation of security parameters



3G Authentication & key agreement

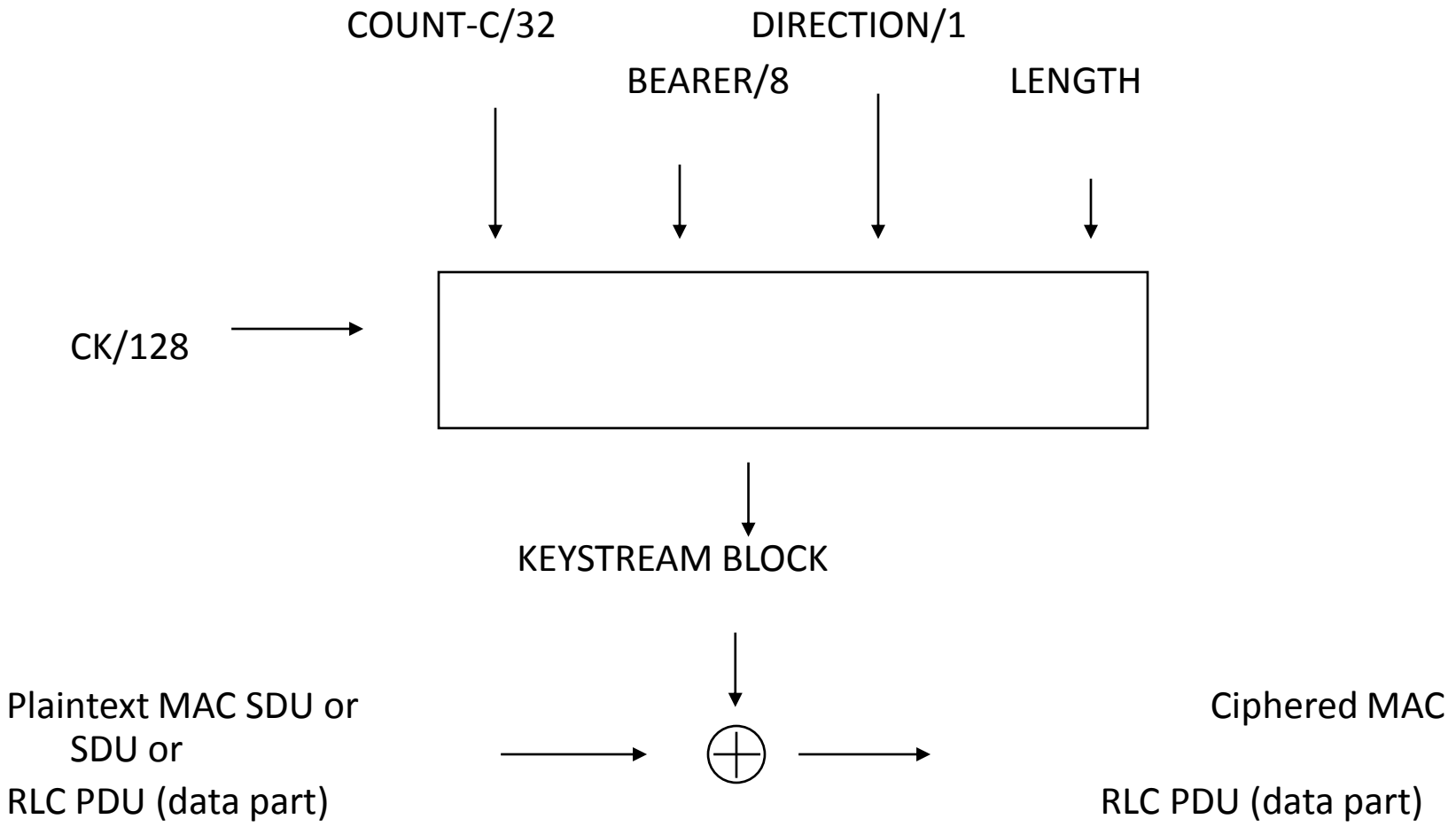


3G ciphering mechanism

- Between UE and RNC
- Stream cipher like in GSM and GPRS
- Key length 128 bits
- Key lifetime could be limited

- ***Design decision:*** First algorithm UEA1 based on KASUMI block cipher
  - AES did not exist yet
  - Public specifications (although under export control)

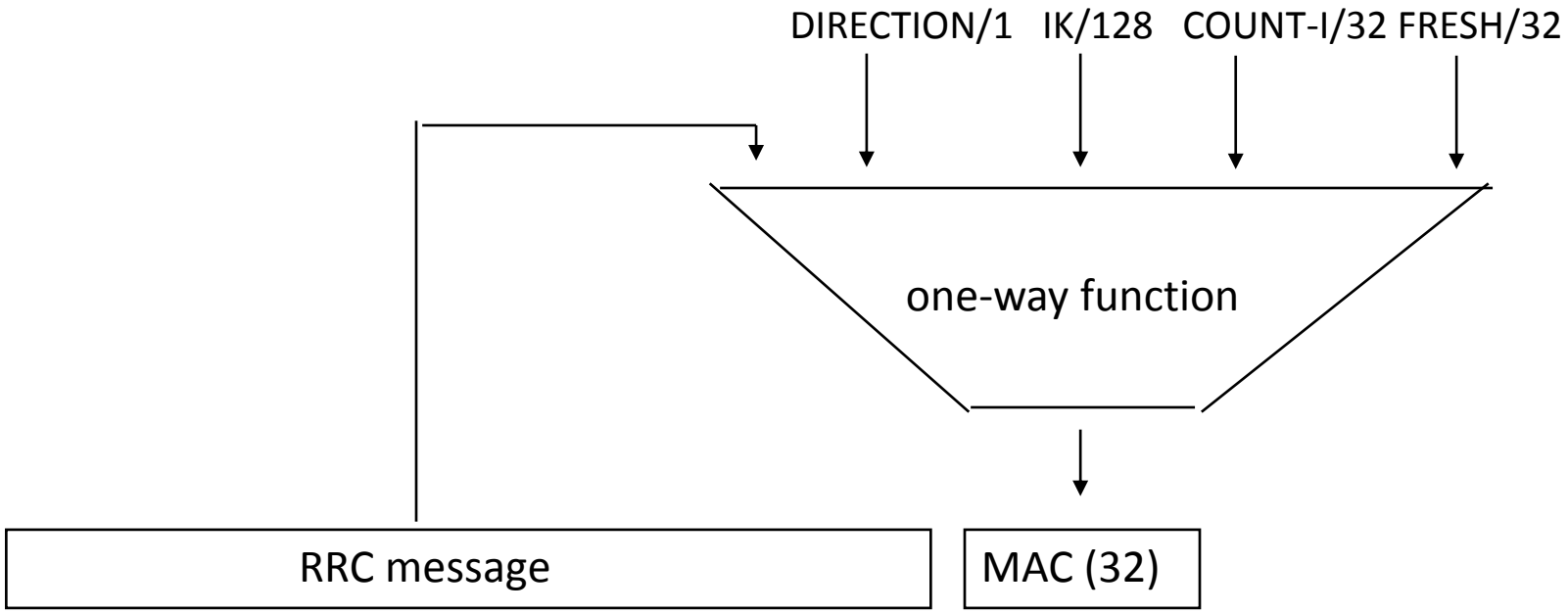
3G Ciphering algorithm



Integrity protection

- Purpose: to authenticate *individual* RRC signaling messages
- Almost all RRC messages are integrity protected

Integrity mechanism



For UIA1: the one-way function is based on KASUMI block cipher

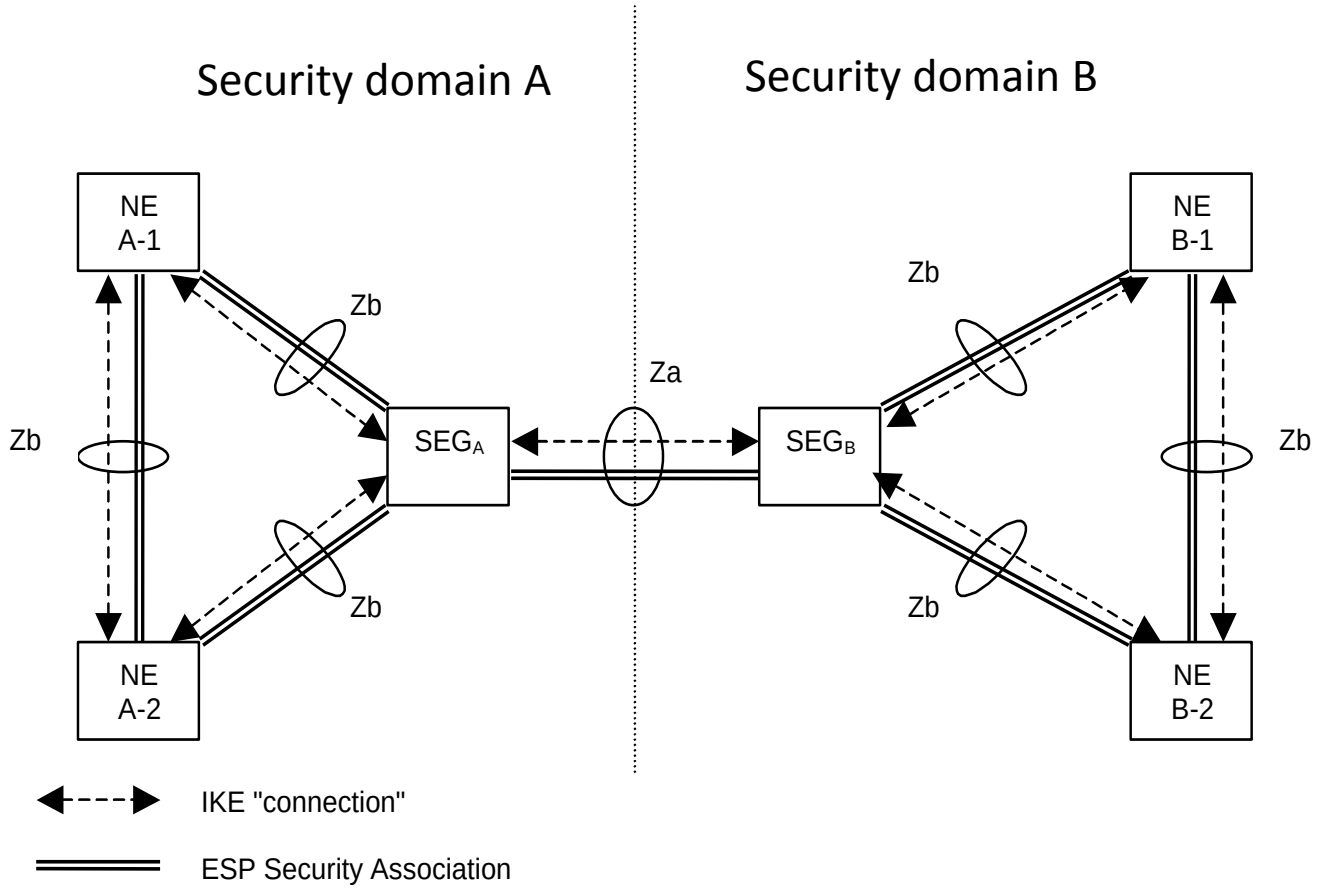
a posteriori design decision for 3G

- GSM SIM is sufficient for access to 3G
  - SIM not aware of mutual authentication
  - Generates 64-bit keys

Second set of cryptoalgorithms based on SNOW3G

- These are called UEA2 and UIA2
- Added in 3GPP release 7 (in 2006)
- SNOW3G is a stream cipher

Network domain security (based on IPsec)



Status of 3G security today

- 3G security resilient against security analyses
- No significant attacks known on cryptographic algorithms
- No false base station attacks seem possible
- 3G security seems still sufficient for 3G networks

LTE = 4G

4G: What and why?

- LTE offers ***higher data rates***, up to several Gb/sec
  - Multi-antenna technologies
  - New transmission schema based on OFDM
  - Signaling/scheduling optimizations
- "flat" ***IP-based architecture***
  - Two network nodes for user plane
  - Simplified protocol stack
  - Optimized inter-working with legacy cellular, incl. CDMA
  - Inter-working with non-3GPP accesses, incl. WiMAX

4G: What and why?

LTE = Long Term Evolution (of radio networks)

- Technical terms:
  - E-UTRAN = Evolved UTRAN (LTE radio network)
  - EPC = Evolved Packet Core (4G core network)
  - EPS = Evolved Packet System (= RAN + EPC)

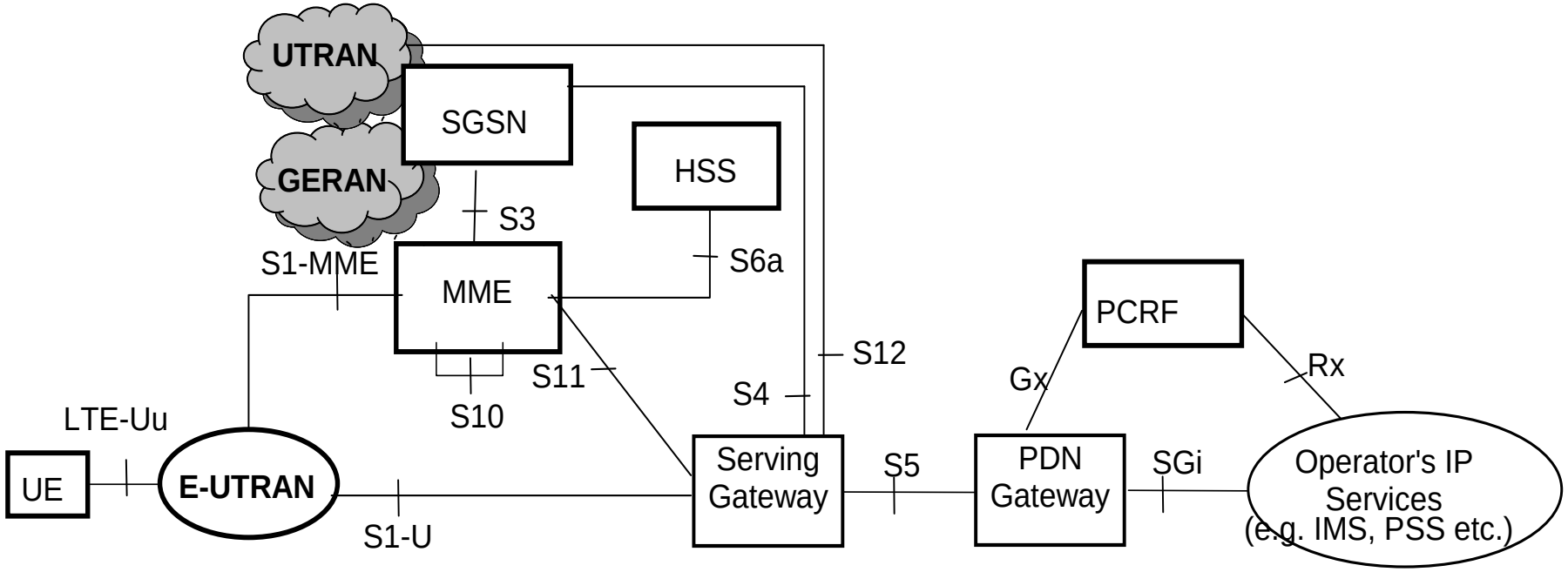
LTE : designed by whom?

3GPP TSG SA : stage 2 specifications for LTE/SAE
3GPP TSG RAN: stage 3 specs for LTE
3GPP TSG CT: stage 3 specs for SAE

LTE/SAE is included in 3GPP *Release 8* specifications

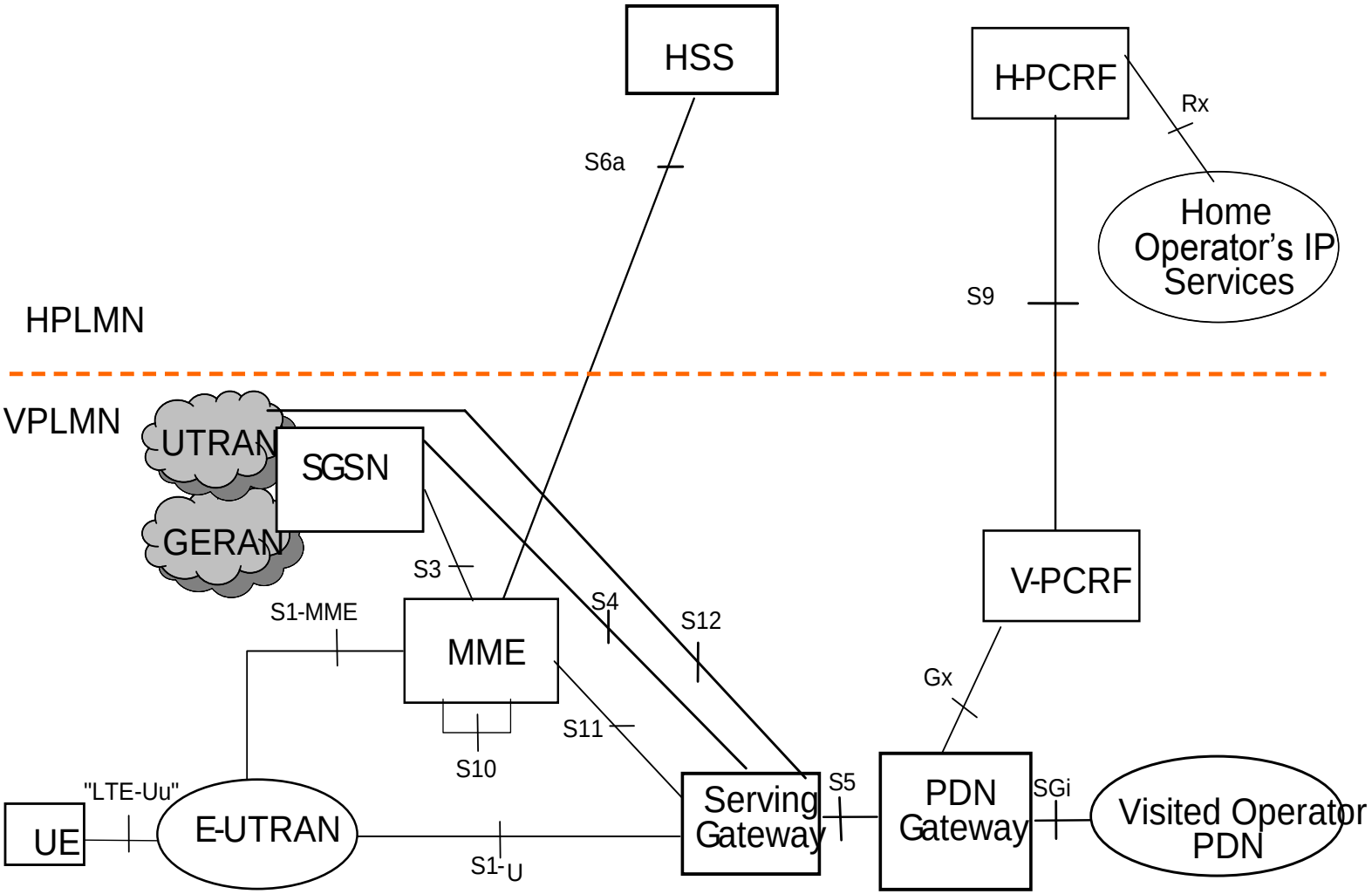
Security design by 3GPP TSG SA Working Group 3 (SA3)

EPS architecture (non-roaming case)



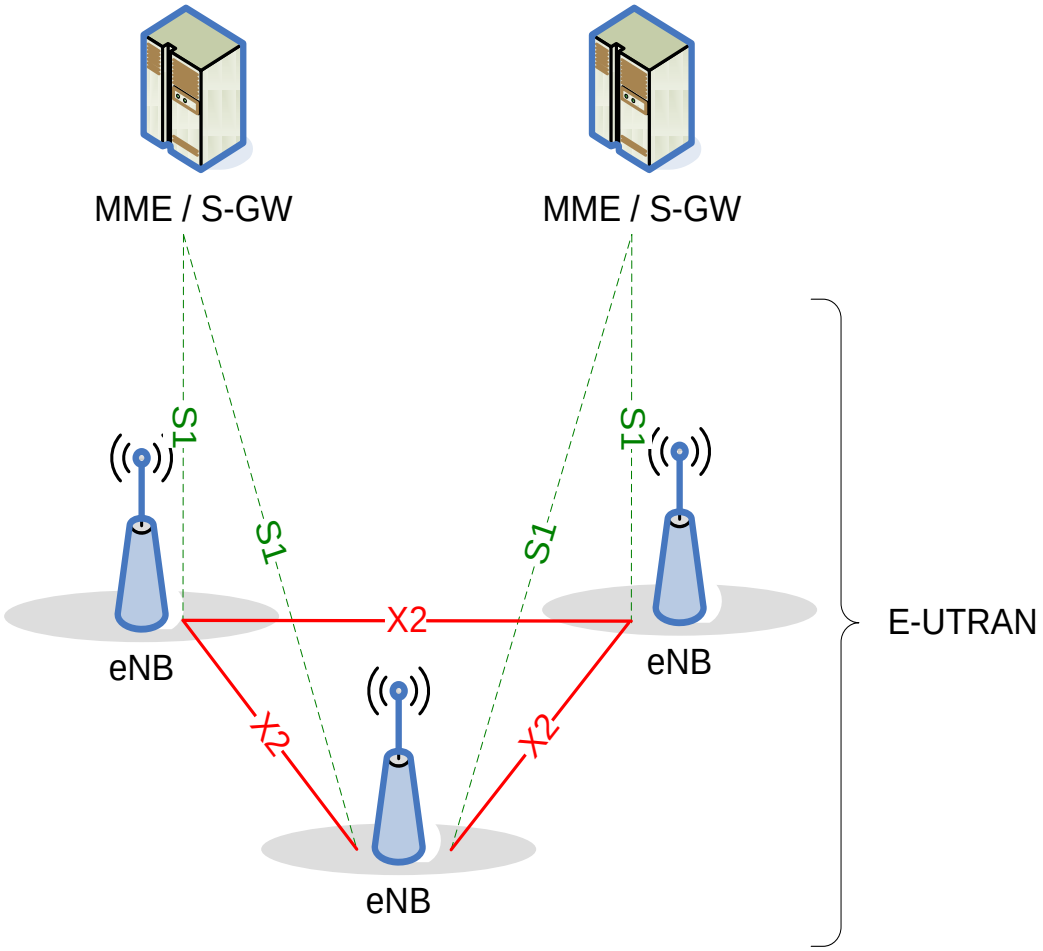
From 3GPP TS 23.401

EPS architecture (one of the roaming variants)



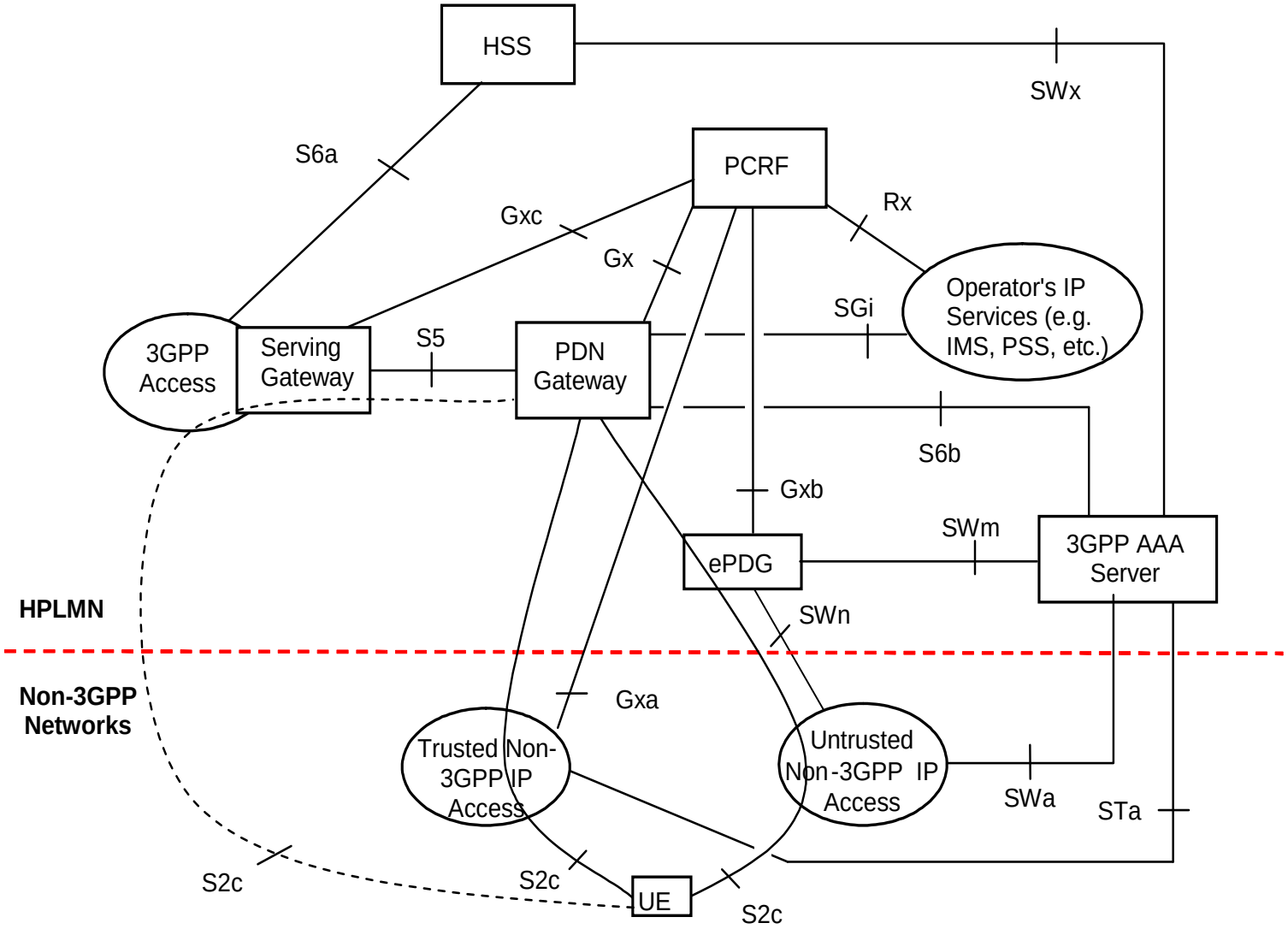
From TS 23.401

E-UTRAN architecture



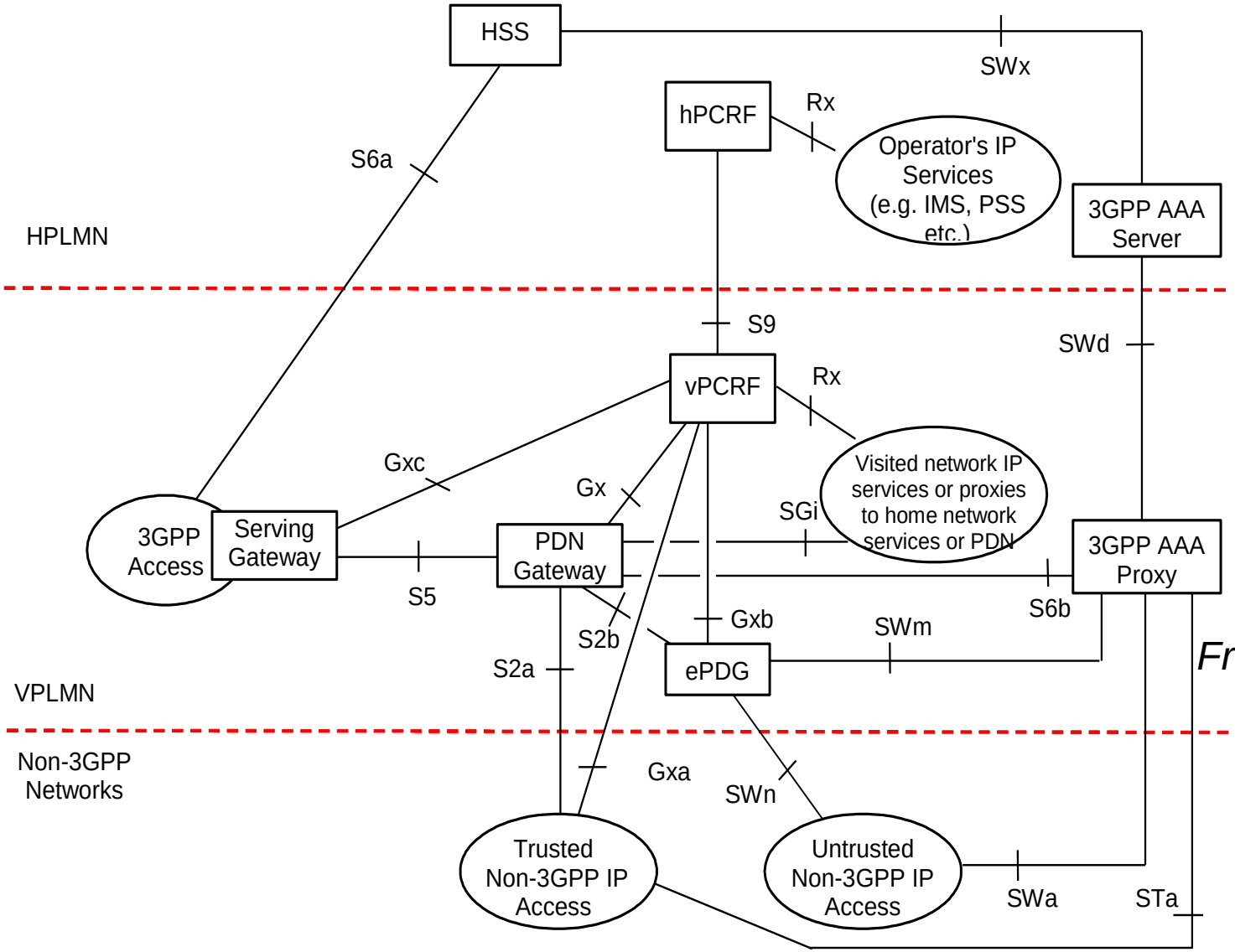
From 3GPP TS 36.300

EPS archi with non-3GPP access (non-roaming)



From TS 23.402

Roaming case (one variant)



From TS 23.402

LTE Security

Implications of 4G architecture on security

- Flat architecture:
  - All ***radio*** access ***protocols terminate in*** one node: ***base station***
  - ***IP*** protocols also ***visible in base station***
- Security implications due to
  - ***Architectural design*** decisions
  - ***Interworking*** with legacy and non-3GPP networks
  - Allowing ***base station*** placement ***in untrusted locations***
  - New business environments with ***less trusted networks*** involved
  - Trying to ***keep*** security ***breaches*** as ***local*** as possible
- As a result (when compared to 3G):
  - ***Extended Authentication*** and Key Agreement
  - More complex ***key hierarchy***
  - More complex ***interworking security***
  - Additional ***security for base stations***

Major design decisions for EPS security (1/2)

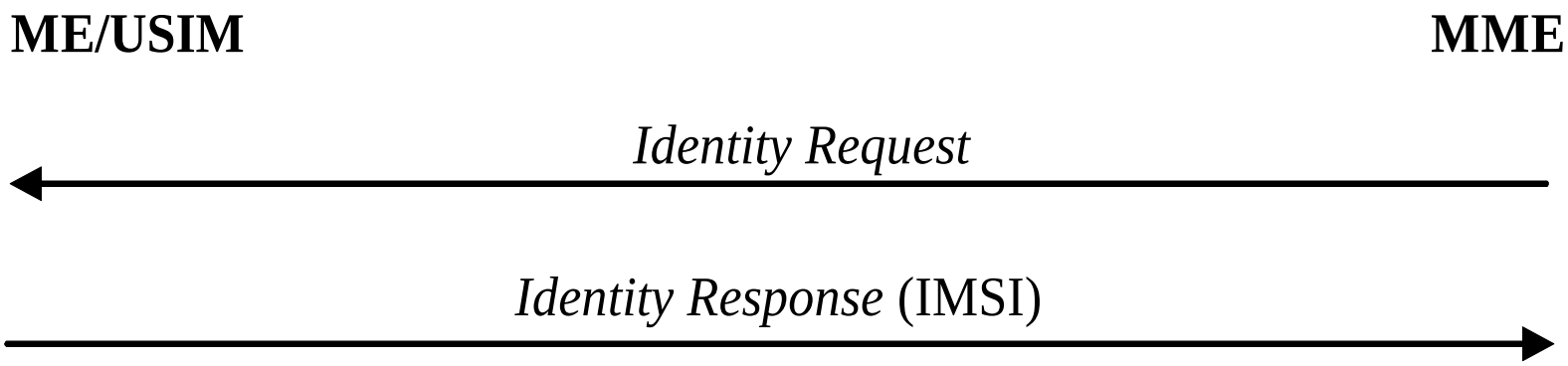
- Permanent security association
  - Inherited from GSM and 3G
- Interfaces in UE and HSS/HLR
  - ME-USIM interface is fully standardized but HSS-AuC is not
- Reuse of 3G USIMs
- ***No*** reuse of 2G SIMs in EPS
- Delegated authentication
  - Inherited from GSM and 3G
- Reuse of 3G AKA
- Cryptographic network separation
- Serving network authentication

Major design decisions for EPS security (2/2)

- Termination point for encryption and integrity protection
  - Flat architecture required moving to base station site
- New key hierarchy in EPS
- Key separation in handovers
- Homogeneous security for heterogeneous access networks
- User identity confidentiality ***not*** protected against active attackers
- ***Other „NOT“ – decisions:***
  - ***No integrity protection for user plane on radio interface***
  - ***No (cryptographic) non-repudiation of charging***

Identity confidentiality in EPS (1/2)

- Mechanism ***inherited from GSM*** and 3G
- User's permanent identity (IMSI) is sent to the network ***only if*** network cannot identify the UE otherwise



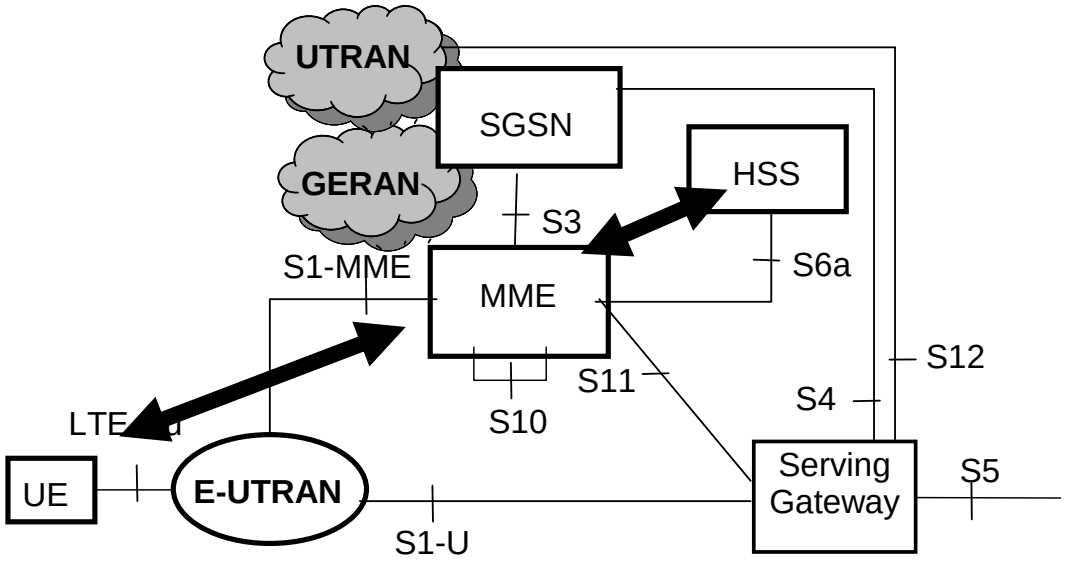
From 33.401

Identity confidentiality in EPS (2/2)

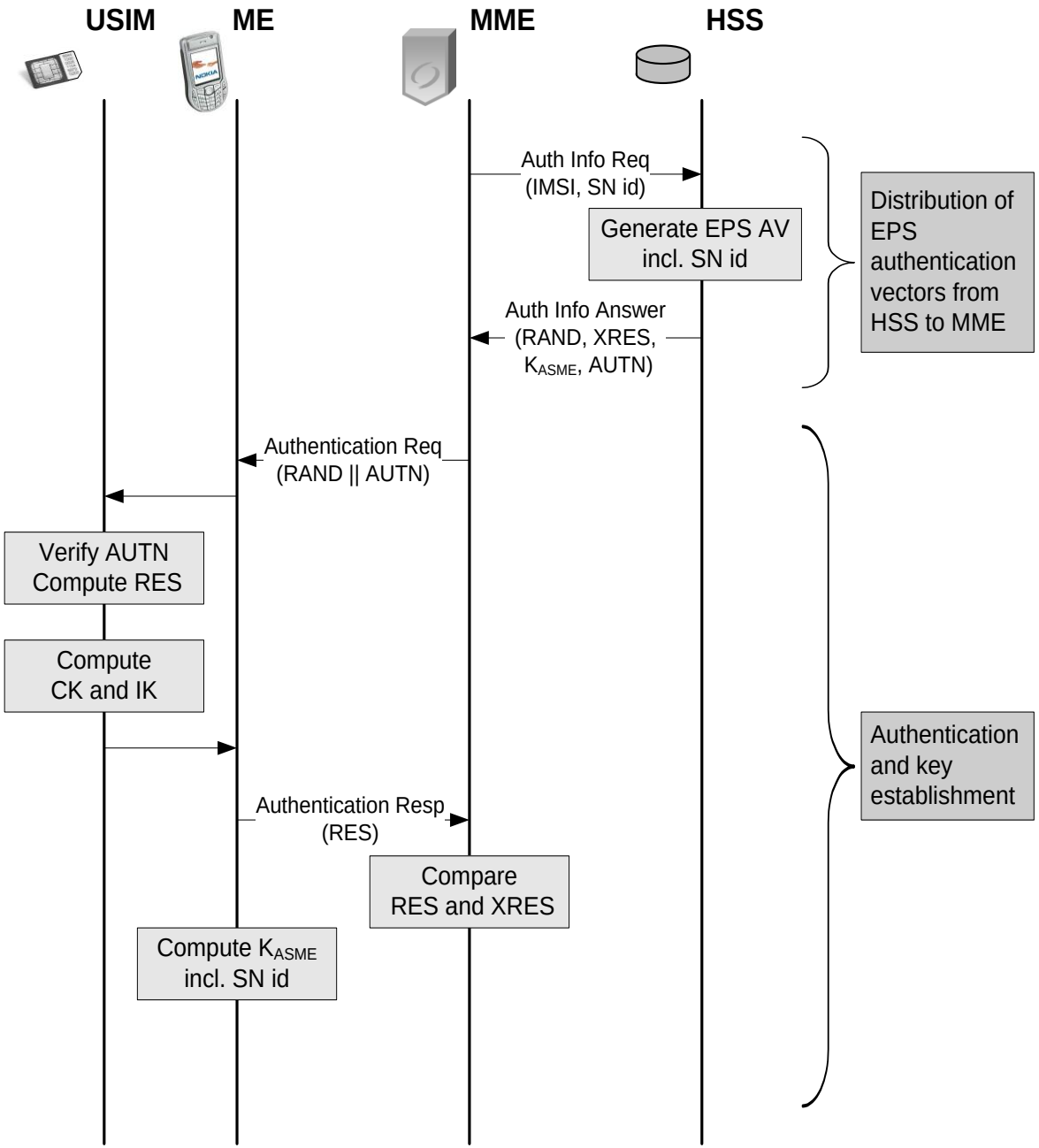
- Network assigns a temporary identity for the UE
- It is sent to the UE in encrypted message

Authentication and key agreement

Authentication and key agreement

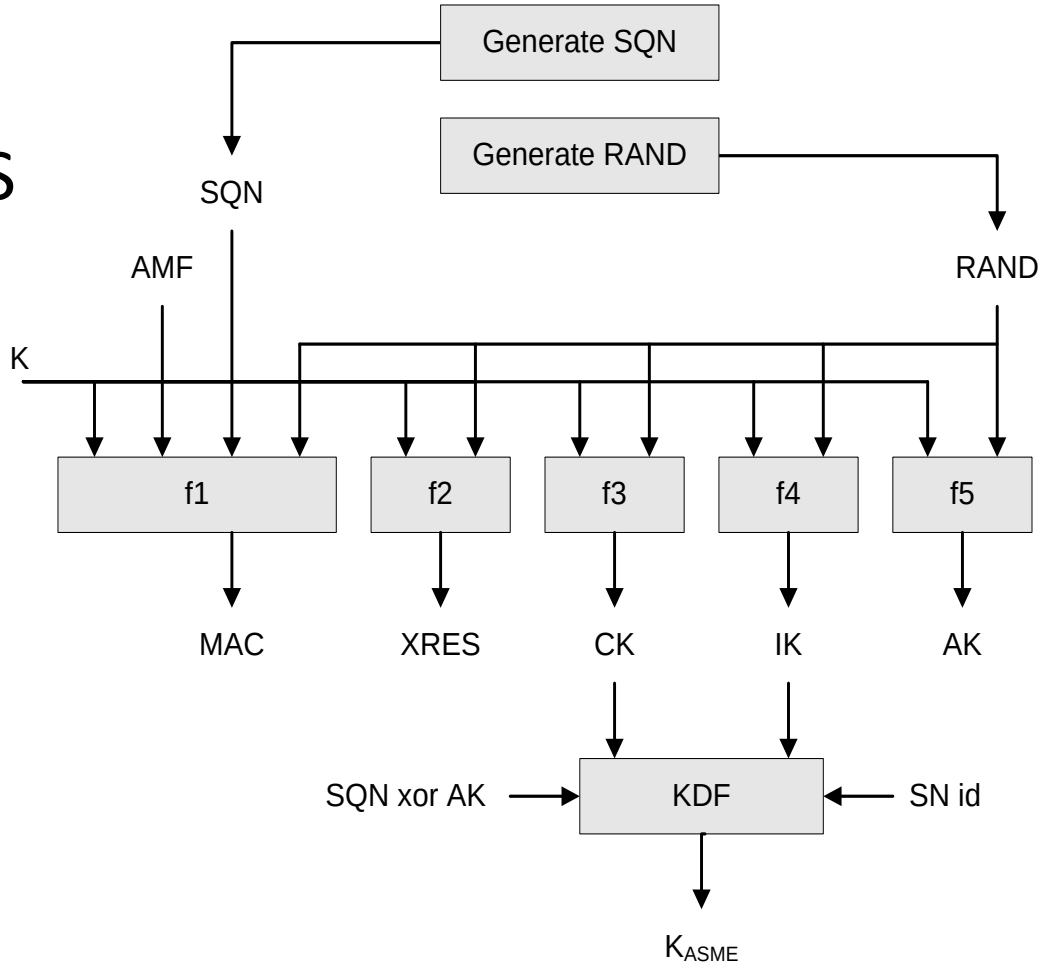


- HSS generates authentication data and provides it to MME
- Challenge-response authentication and key agreement procedure between MME and UE



From "LTE security"

Generation of UMTS and EPS AV's



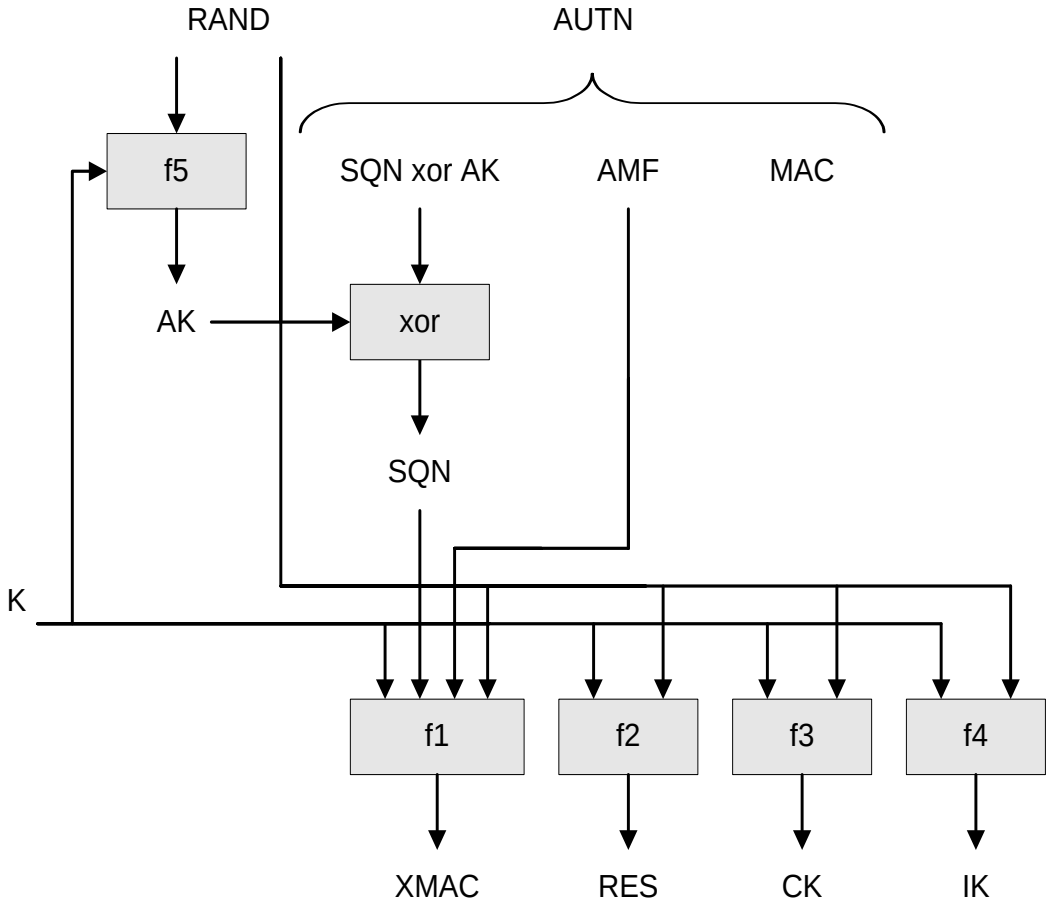
From "LTE security"

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

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

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

Verification in USIM



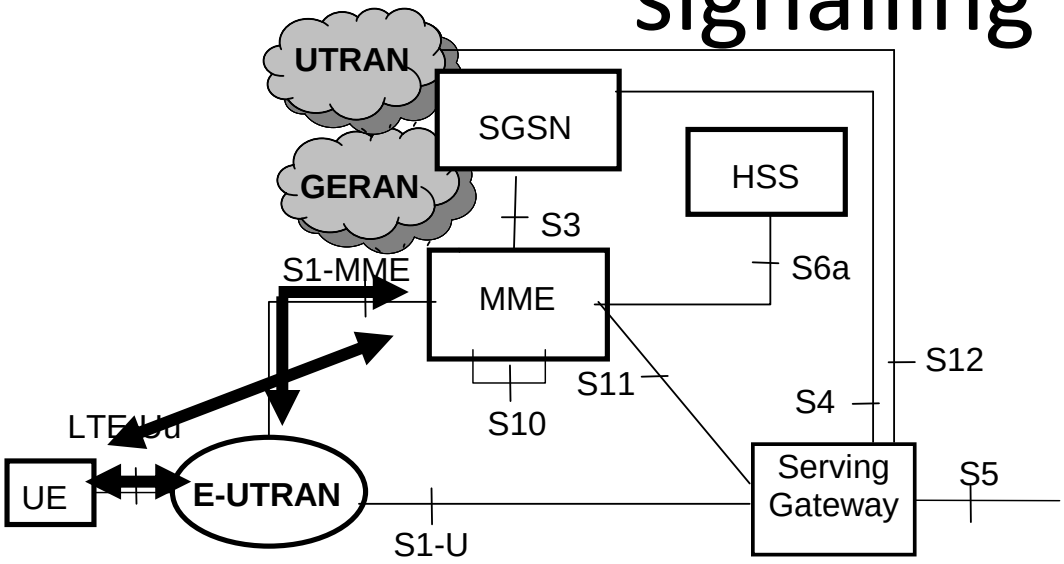
Verify MAC = XMAC

Verify that SQN is in the correct range

From "LTE security"

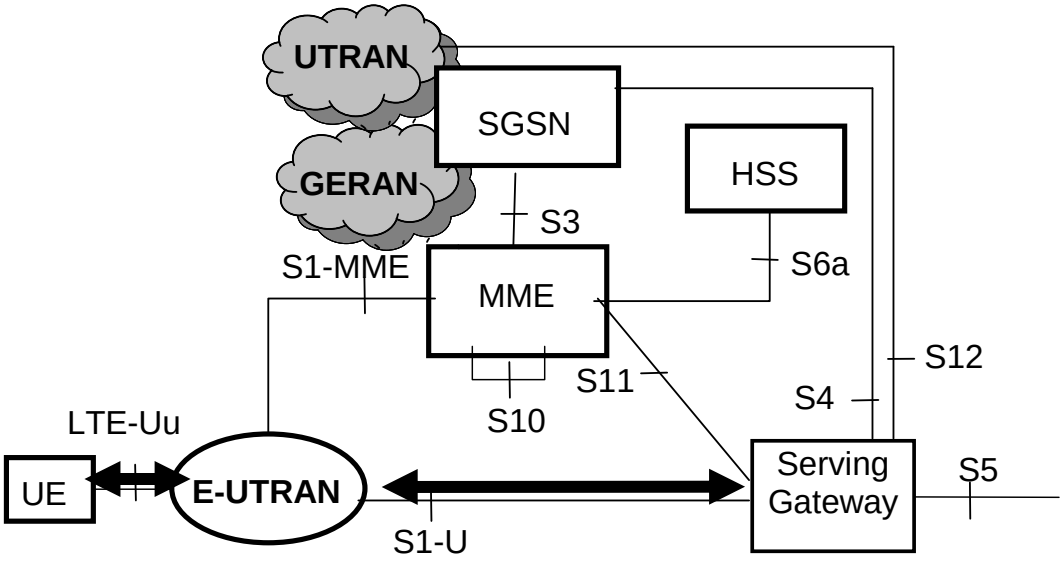
LTE Data protection

Confidentiality and integrity of signalling



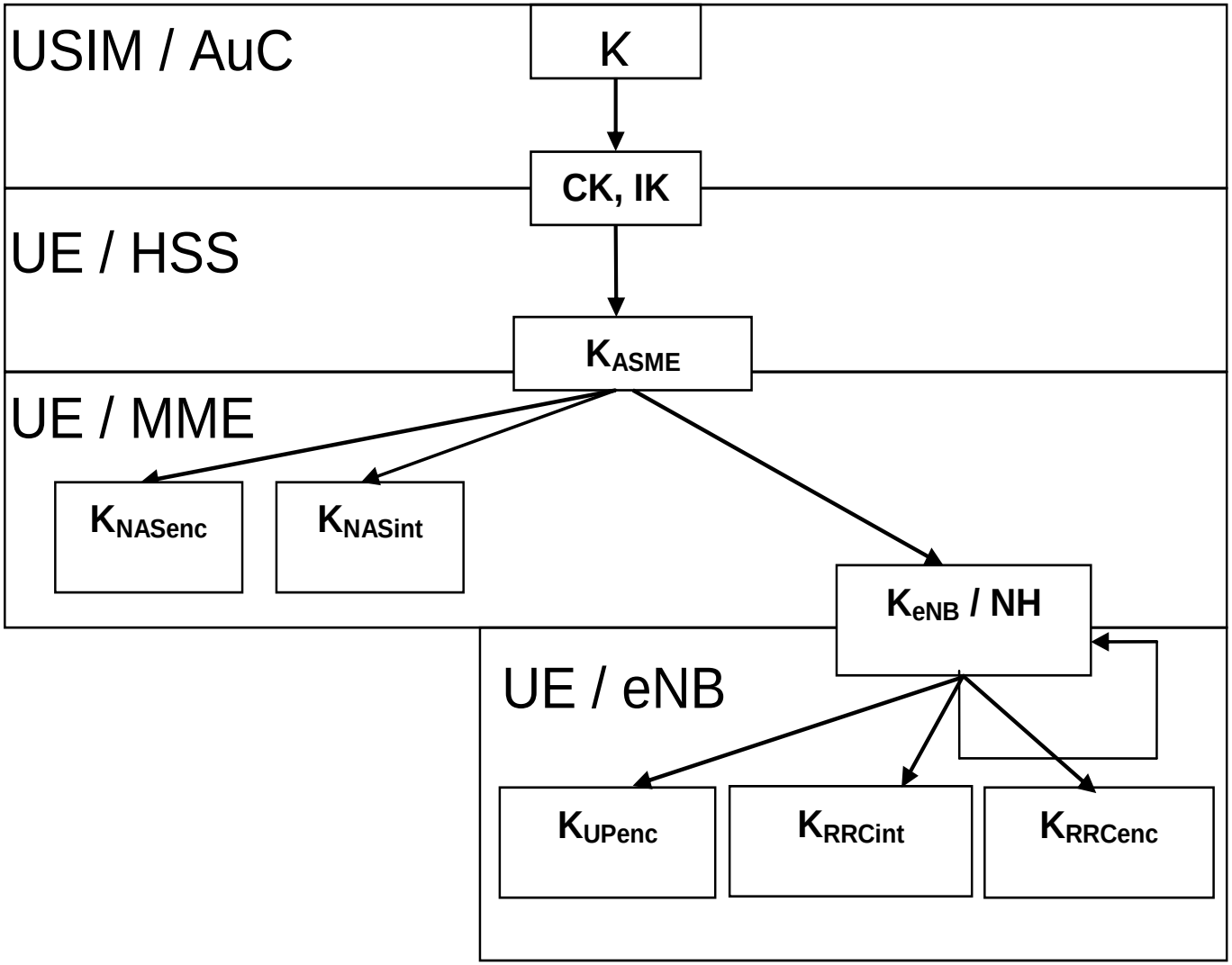
- RRC signalling between UE and E-UTRAN
- NAS signalling between UE and MME
- S1 interface signalling
  - protection is not UE-specific
  - optional to use

User plane confidentiality

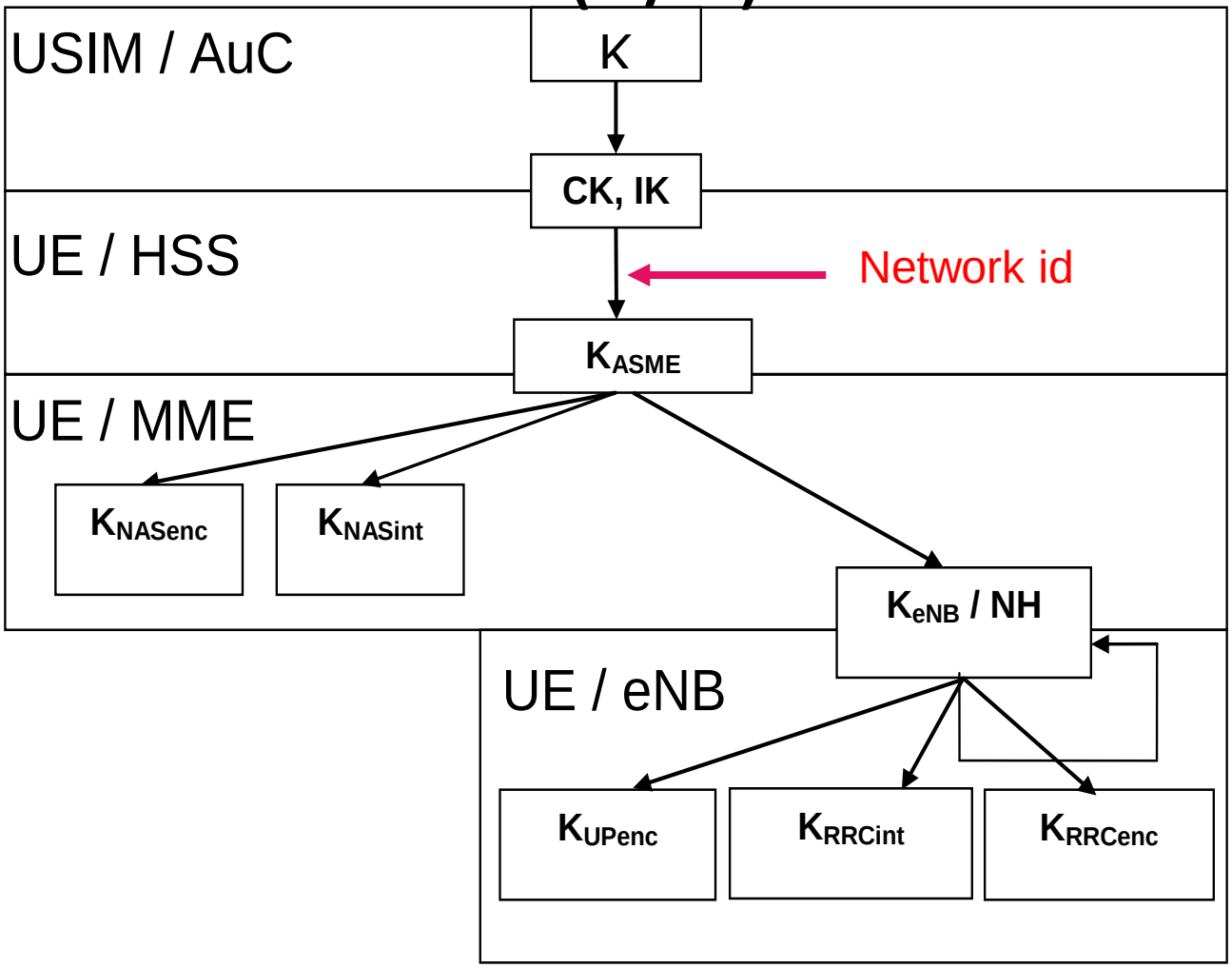


- S1-U protection is not UE-specific
  - (Enhanced) network domain security mechanisms (based on IPsec)
  - Optional to use
- Integrity is not protected for various reasons, e.g.:
  - performance
  - limited protection for application layer

LTE Key hierarchy



Cryptographic network separation (1/2)



Cryptographic network separation (2/2)

- Authentication vectors in EPS are specific to the serving network
  → AV's usable in EPS cannot be used in GERAN or UTRAN
- AV's usable for UTRAN/GERAN access cannot be used for E-UTRAN access
  – Solution by a "***separation bit***" in AMF field
- On the other hand, Rel-99 USIM is sufficient for EPS access
  → It is the ***ME*** that has to check the "separation bit" (when accessing E-UTRAN)

LTE crypto-algorithms

Crypto-algorithms

- Two sets of algorithms from Day One
  - If one breaks, we still have one standing
  - Should be as different from each other as possible
  - ***AES*** and ***SNOW 3G*** chosen as basis → ETSI SAGE has specified/chosen modes
- A third algorithm set added for Release 11
  - The base algorithm ***ZUC*** is of Chinese origin and usable in China
- Rel-99 USIM is sufficient → master key 128 bits
  - All keys used for crypto-algorithms are 128 bits but included possibility to add 256-bit keys later (if needed)
- Deeper key hierarchy → (one-way) key derivation function needed
  - ***HMAC-SHA-256*** chosen as basis

Caveat: Security of algorithm capability negotiation

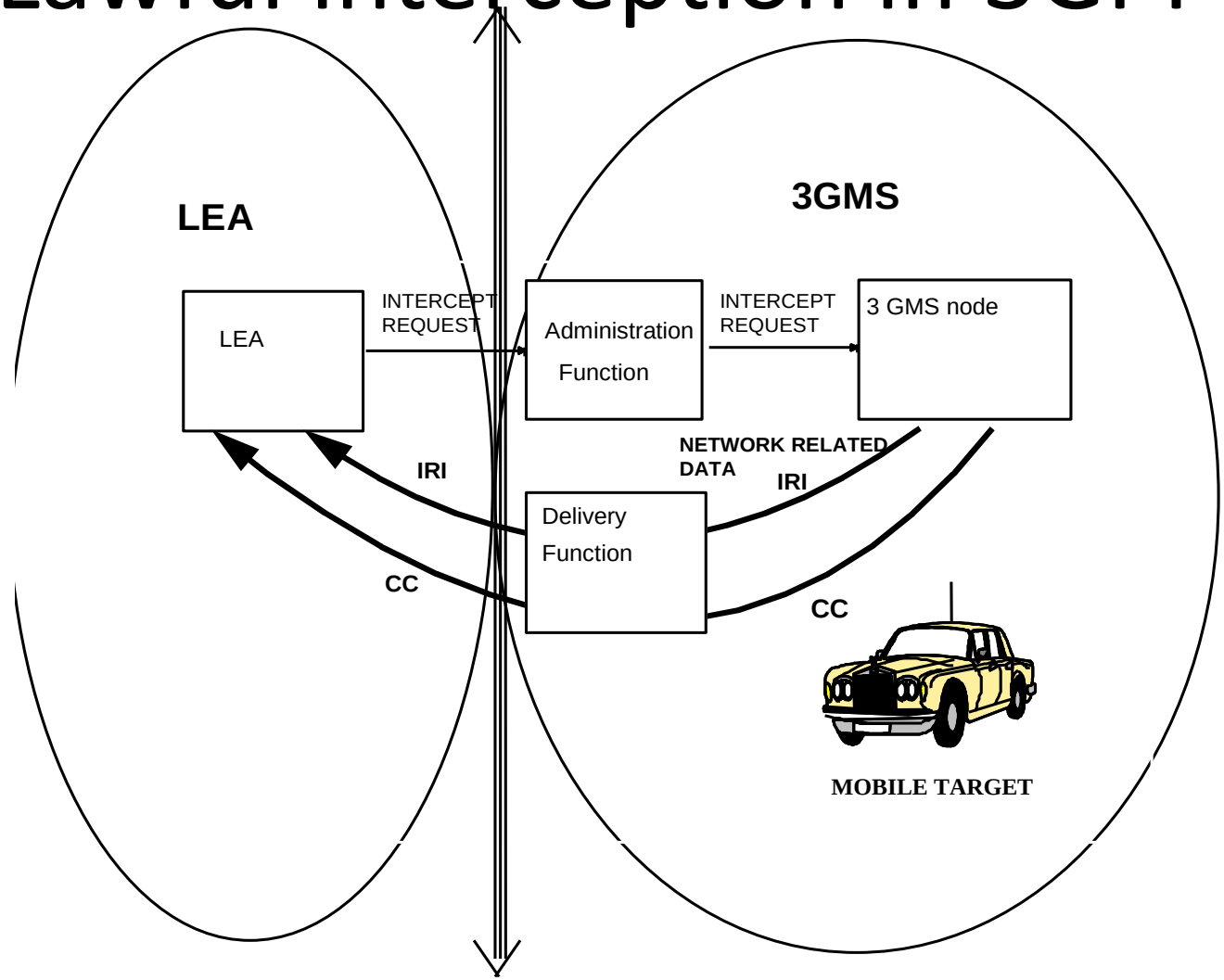
- Algorithm ***capabilities*** exchanged ***first without protection***
- Capabilities ***re-exchanged and verified*** once integrity protection is turned on

  → all integrity algorithms should resist real-time attacks in the beginning of the connection

- If this is not the case anymore, broken algorithm has to be withdrawn completely from the system
  - In the same way as A5/2 is withdrawn from GSM

Lawful interception

Lawful interception in 3GPP



a priori design decision

- Interfaces for lawful interception are standardized like any other interfaces in the system
  - All specs are public

LI specifications

- Requirements in TS 33.106 (11 pages)
- Architecture, functions, information flows in TS 33.107 (129 p.)
- Description of the Handover Interfaces, incl. ASN1, in TS 33.108 (189 p.)

When LI is invoked: examples

- A circuit switched call is requested originated from, terminated to, or redirected by the target
- Location information related to the target facility is modified by the subscriber attaching or detaching from the network, or if there is a change in location
- An SMS transfer is requested - either originated from or terminated to the target
- A data packet is transmitted to or from a target

What is intercepted ?

- CC = Content of Communications
  - Intercepted from media plane entities, e.g. in EPS: Serving Gateway
- IRI = Intercept Related Information
  - E.g. in the case of *Attach:*
    - *Observed MSISDN*
    - *Observed IMSI*
    - *Observed ME Id*
    - *Event Type*
    - *Event Time*
    - *Event Date*
    - *Network Element Identifier*
    - *Location Information*
    - *Failed attach reason*
    - *Etc.*

Base station security

Configuration of base station

- Communication between the remote/local ***O&M systems*** and the ***eNB mutually authenticated***.
- The eNB shall be able to ensure that ***software/data change*** attempts are ***authorized***
- ***Confidentiality and integrity*** of software transfer towards the eNB ensured.
- etc.

Secure environment inside eNB

- ***Secure storage*** of sensitive data, e.g. long term cryptographic secrets and vital configuration data.
- The ***secure*** environment shall support the ***execution of sensitive functions***, e.g. en-/decryption of user data.
- The ***secure*** environment shall support the execution of sensitive parts of the ***boot*** process.
- ***Only authorised access*** shall be granted to the secure environment.
- etc.

Security aspects typically not standardized

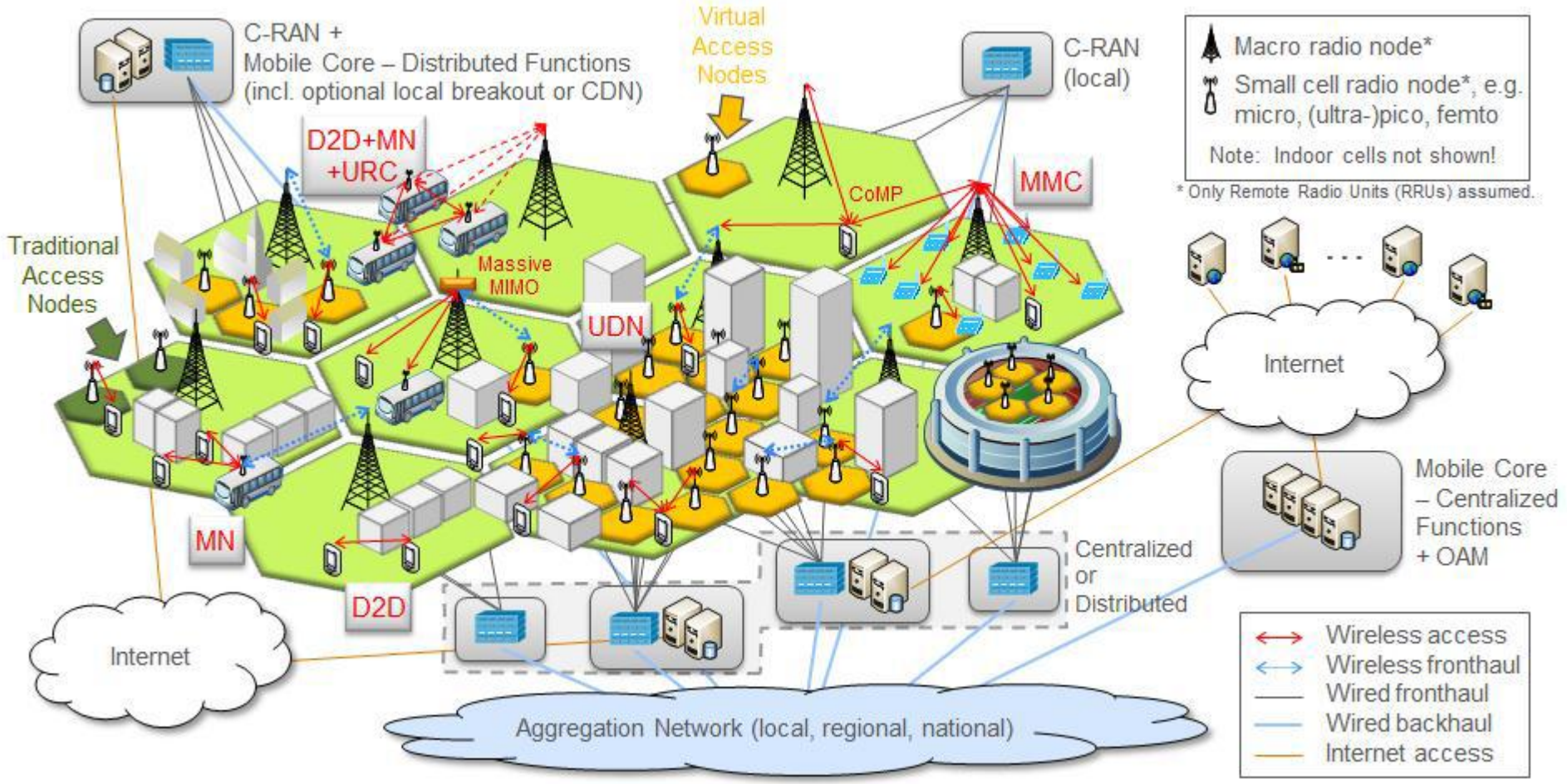
- Product implementations
  - Secure SW development
  - HW security
  - Security testing and audits
- Organizational aspects
  - Organization of security in a corporation (e.g. mobile operator)
  - Security awareness
  - Emergency response (CERT)
- Operational aspects
  - Anti-virus, vulnerability scanning
  - Firewalls
  - Intrusion detection and prevention
  - Fraud management systems

Perspectives to 5G

5G targets (according to METIS)

- 1000 x higher mobile data volume per area
- 10 to 100 x higher number of connected devices
- 10 to 100 x higher typical user data rate
- 10 x longer battery life for low power machine communications
- 5 x reduced End-to-End latency

5G architecture (according to METIS)



5G key technologies

- Cloud computing
- Software-defined networking
- Network function virtualization
- (Direct) device-to-device communications
- Machine-to-machine communications

Some 5G security challenges

- Isolation of functions in virtualized environment
- All issues with SDN and Cloud Computing
- Potential lack of infra support in device-to-device communications
- Potential lack of human intervention in machine-to-machine communications

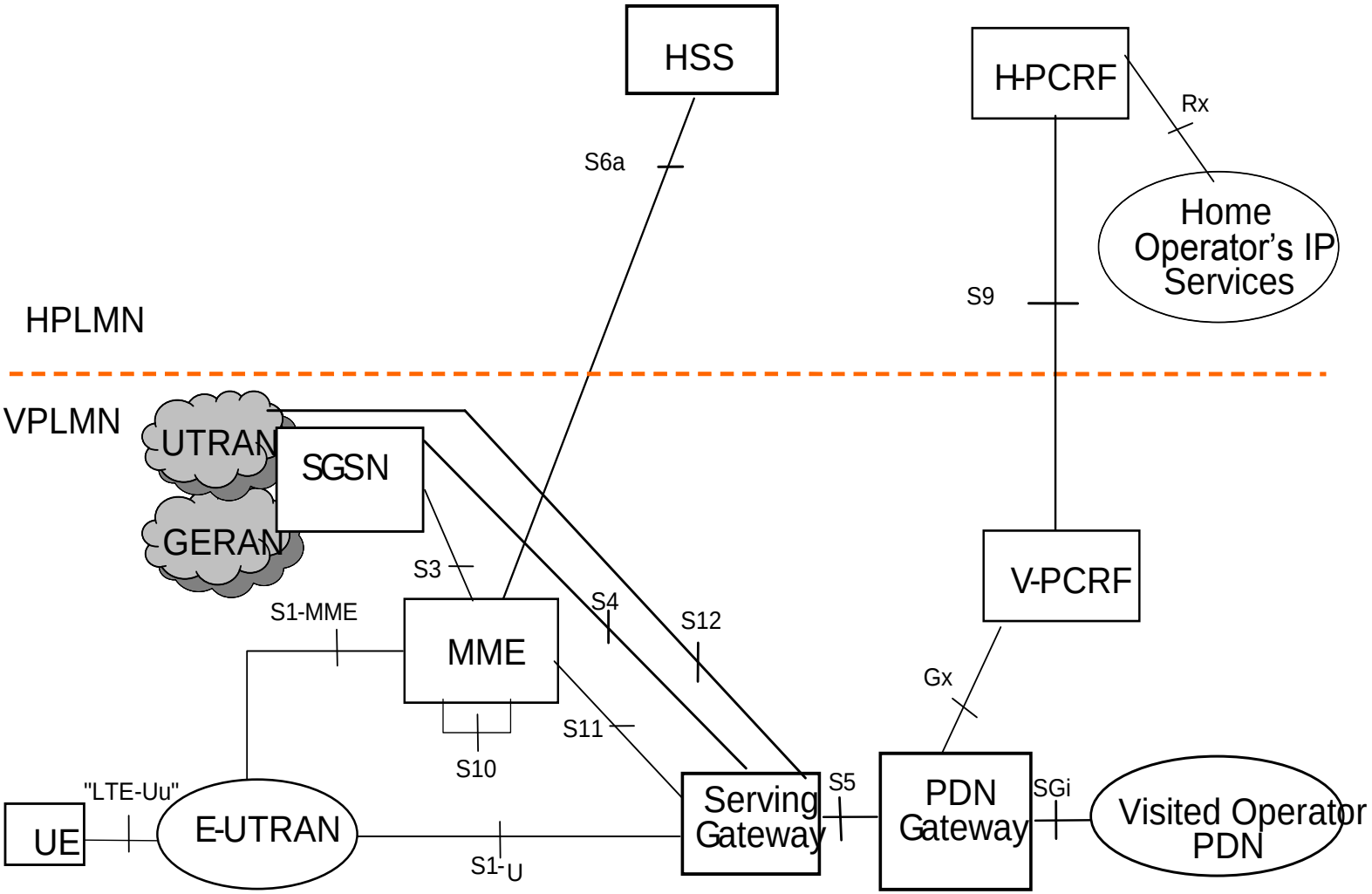
About SDN security 1/2

- 5G SDN protocols expected to be based on OpenFlow
- OpenFlow developed by ONF (Open Networking Foundation)
  - Wireless and Mobile WG
  - Security discussion group
- Lots of research still needed for SDN security

About SDN security 2/2

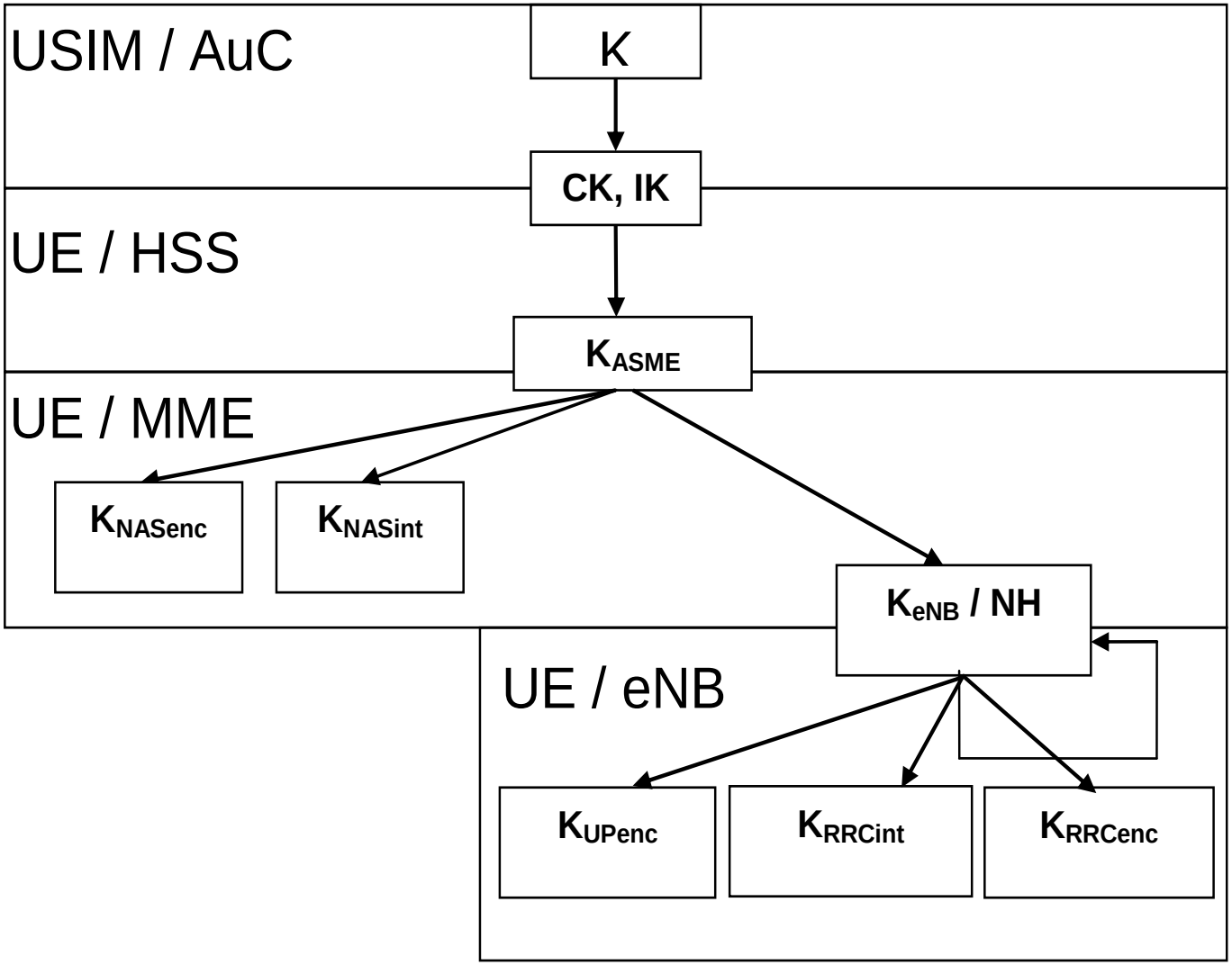
- Some generic security issues:
  - Lack of built-in security in OpenFlow protocols
  - Centralized control may create single-point-of-failure
- SDN helps in solving security issues:
  - Flexible reaction to identified threats and vulnerabilities; easier to upgrade the network
  - Data mining and machine learning could be a built-in feature in the security architecture

4G architecture (one of the roaming variants)

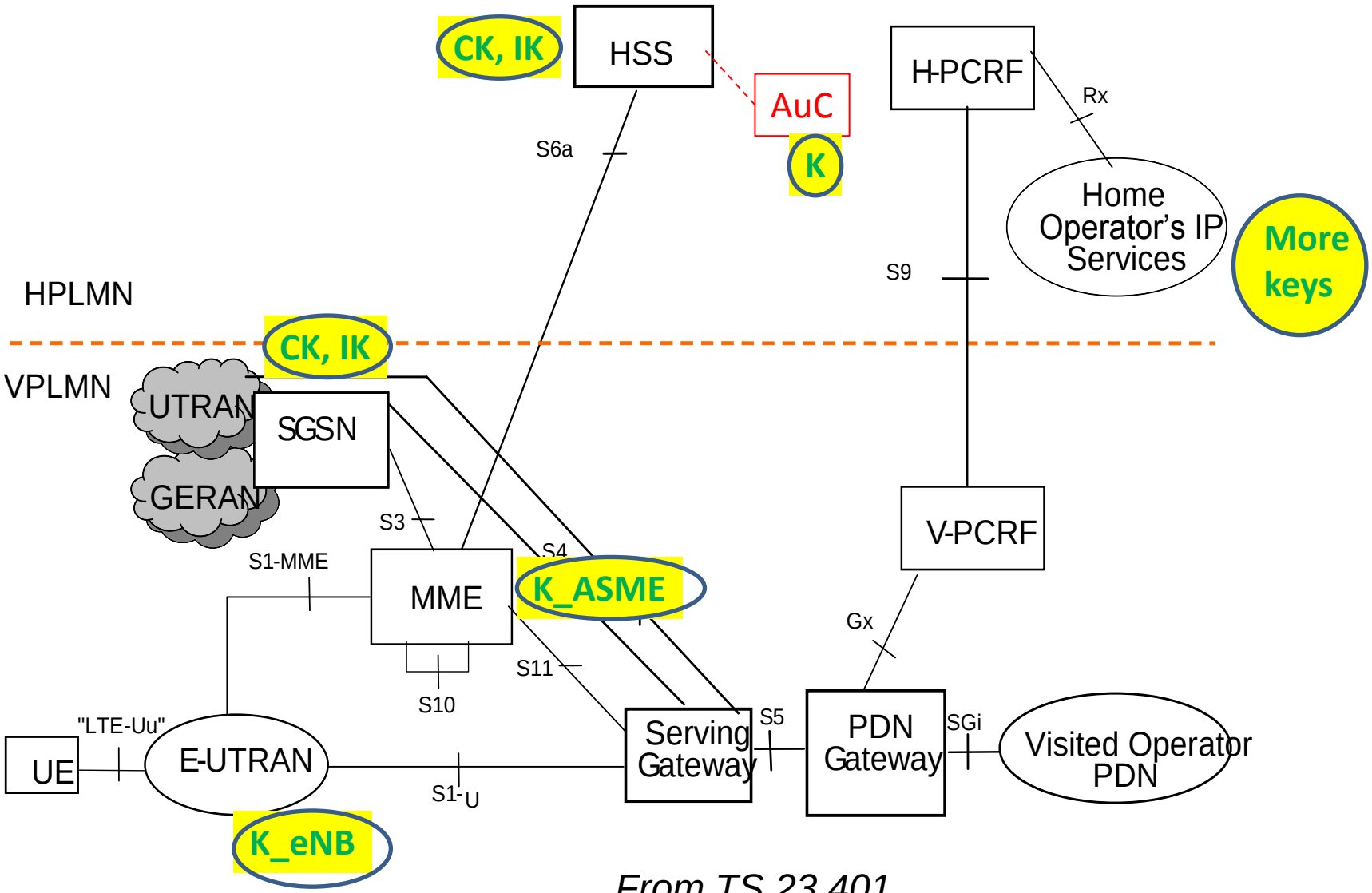


From TS 23.401

LTE Key hierarchy



4G architecture (one of the roaming variants)



From TS 23.401

LTE keys

- There are many keys distributed all over the 4G network
  - In the previous slide, only keys specific to one user were shown
  - Many more keys shared between network elements
- If defining network functionality with SDN, how to guarantee access to correct keys (and only those) ?

5G keys 1/2

- Until 3G, (user-specific) keys were derived in
  - SIM/UICC on terminal side
  - AuC on network side
- In 4G, many more keys are derived in
  - ME on terminal side
  - In many network elements
- Does the trend continue in 5G ?

5G keys 2/2

- SDN paradigm enables ”easy” addition of new network functionalities
- New functionalities must be secure
  - How to guarantee that the security architecture is also flexible enough ?
  - How to enable access to the correct keys in a dynamic architecture ?
  - How to generate new keys if there are no ”correct” keys available ?
- Security may easily become a burden in development of dynamic network architectures

NFV and Cloud

- Regardless of SDN, 5G networks follow the Cloud paradigm
- Network functions are virtualized, and run on top of general-purpose hardware

ETSI NFV

- Published
  - Security Problem Statement
  - (draft) Security and Trust Guidance
- ETSI NFV and ONF are strategic partners

NFV security issues 1/2

- How to isolate network functions from each other ?
  - For example: function 1 should use Key set 1; function 2 should use Key set 2 but both functions are run on the same hardware
- Assume network function is moved from one physical machine to another – how to arrange access to the keys accordingly?
- Hypervisor vulnerabilities could have drastic impact on big parts of the network
- How to authenticate virtual functions ?

NFV security issues 2/2

- Legacy networks (3G, 4G) need to interoperate with virtualized network functions
  - Legacy network does not ”understand” that its counterpart is a virtual machine → legacy may act based on wrong assumptions → virtual network function may become a good platform for attacks against legacy networks
- Platform security is a key enabler
  - Access control
  - Secure boot, secure crash,
  - …