4G and 5G networks security techniques and algorithms

ITU PITA Workshop on

Mobile network planning and security

Sami TABBANE

23-25 October 2019 – Nadi, Fiji Islands

Agenda

Introduction

A. 4G LTE Security

B. 5G Release 15 Security

Introduction

Security features in mobile cellular networks:

1. Access security: Authentication
2. Confidentiality: Ciphering
3. Identity protection
4. Information protection: Integrity

SECURITY DIMENSIONS DEFINED BY ITU-T

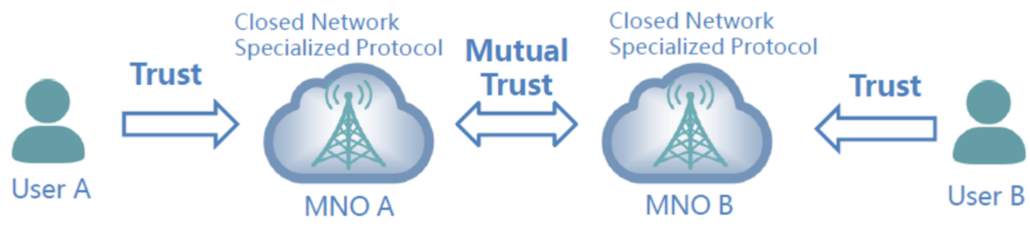
Security Dimension	Brief Explanation
Access Control	Protects against unauthorized use of network resources. It also ensures that only authorized persons or devices access the network elements, services, stored information and information flows.
Authentication	Confirms identities of communicating entities, ensures validity of their claimed identities, and provides assurance against masquerade or replay attacks.
Non-Repudiation	Provides means for associating actions with entities or user using the network and that an action has either been committed or not by the entity.
Data Confidentiality	Protects data from unauthorized disclosure, ensures that the data content cannot be understood by unauthorized entities.
Communication security	Ensures that information flows only between the authorized end points and is not diverted or intercepted while in transit.
Data integrity	Ensures the correctness or accuracy of data, and its protection from unauthorized creation, modification, deletion, and replication. It als provides indications of unauthorized activities related the data.
Availability	Ensures that there is no denial of authorized access to network resources, stored information or its flow, services and applications.
Privacy	Provides protection of information that might be derived from the observation of network activities.

ITU Recommendations

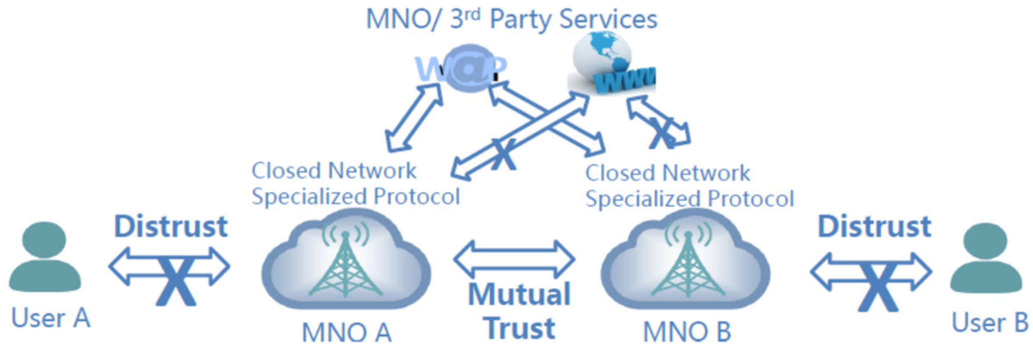
RECOMMENDATION		PUBLICATION
No.	TITLE	
X.1087	A guideline to technical and operational countermeasures for **telebiometric applications** using mobile devices	2016
X.1121	Framework of security technologies for **mobile end-to-end data communications**	2004
X.1122	Guideline for implementing secure mobile systems based on **PKI**	2004
X.1123	Differentiated security service for **secure mobile end-to-end data communication**	2007
X.1124	**Authentication** architecture for mobile end-to-end data communication	2007
X.1125	Correlative **Reacting System** in mobile data communication	2008
X.1126	Guidelines on mitigating the negative effects of **infected terminals in mobile networks**	2017
X.1127	Functional security requirements and architecture for mobile **phone anti-theft measures**	2017
X.1143	Security architecture for **message security in mobile web services**	2007
X.1147	Security requirements and framework for **Big Data analytics in mobile Internet services**	2018
X.1158	**Multi-factor authentication** mechanisms using a mobile device	2014
X.1196	Framework for the downloadable **service and content protection system** in the mobile Internet Protocol Television (**IPTV**) environment	2012
X.1247	Technical framework for countering **mobile messaging spam**	2016
X.1249	Technical framework for countering mobile **in-application advertising spam**	2019
X.tsfpp	Technical security framework for the **protection of users' personal information while countering mobile messaging spam**	[2020]
X.Suppl.30	ITU-T X.805 – Security guidelines for **mobile virtual network operators**	2017

Work item	Subject / Title	Timing
X.5Gsec-q	Security guidelines for applying quantum-safe algorithms in 5G systems	2020-03
X.5Gsec-t	Security framework based on trust relationship in 5G ecosystem	2021-03
X.5Gsec-ecs	Security Framework for 5G Edge Computing Services	2021-03
X.5Gsec-guide	Security guideline for 5G communication system based on ITU-T X.805	2021-09

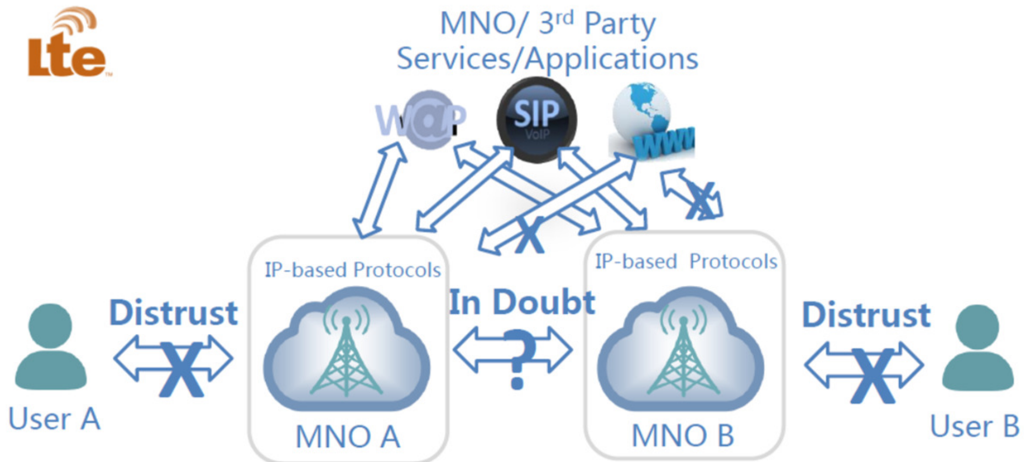
Evolution of trust models



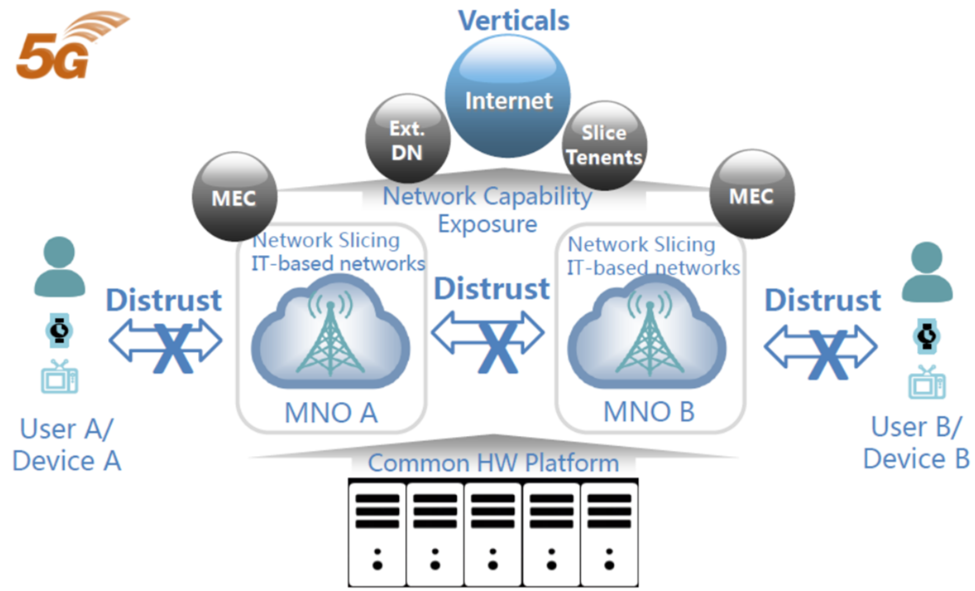
2G Trust model



3G Trust model



4G Trust model



5G Trust model

From *ITU Workshop on 5G Security (03/2018)*

A. 4G LTE Security

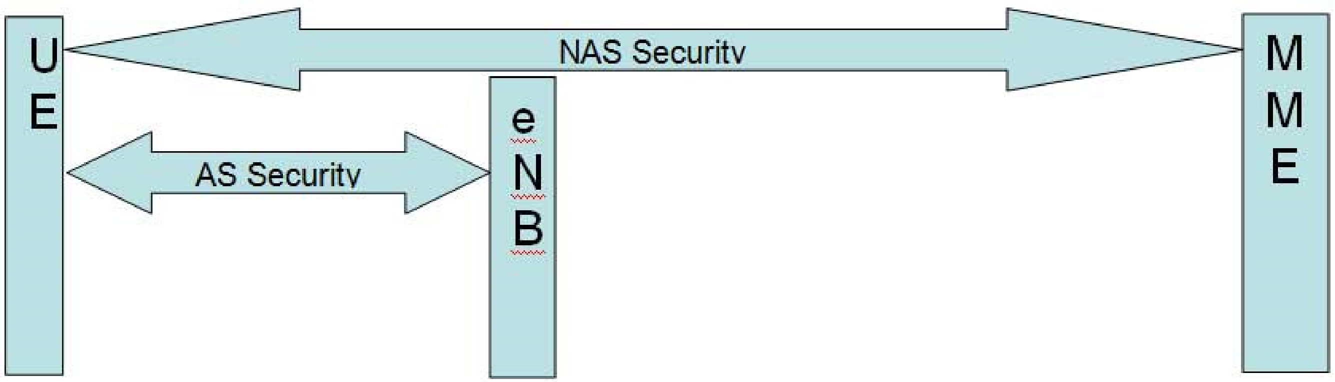
Main changes and additions in LTE / 3G:

- Introduction of a **hierarchical key system** in which keys can be changed for different purposes (e.g., HO),
- **Separation** of the security functions for the NAS,
- Introduction of the concept of **forward security**: limits the security issues when a disclosed key is used

Security Aspects and parameters in LTE

Main characteristics

- Re-use of UMTS ***Authentication and Key Agreement*** (AKA)
- Use of **USIM** required (GSM SIM excluded)
- Extended **key hierarchy**
- **Longer keys**



Security distribution

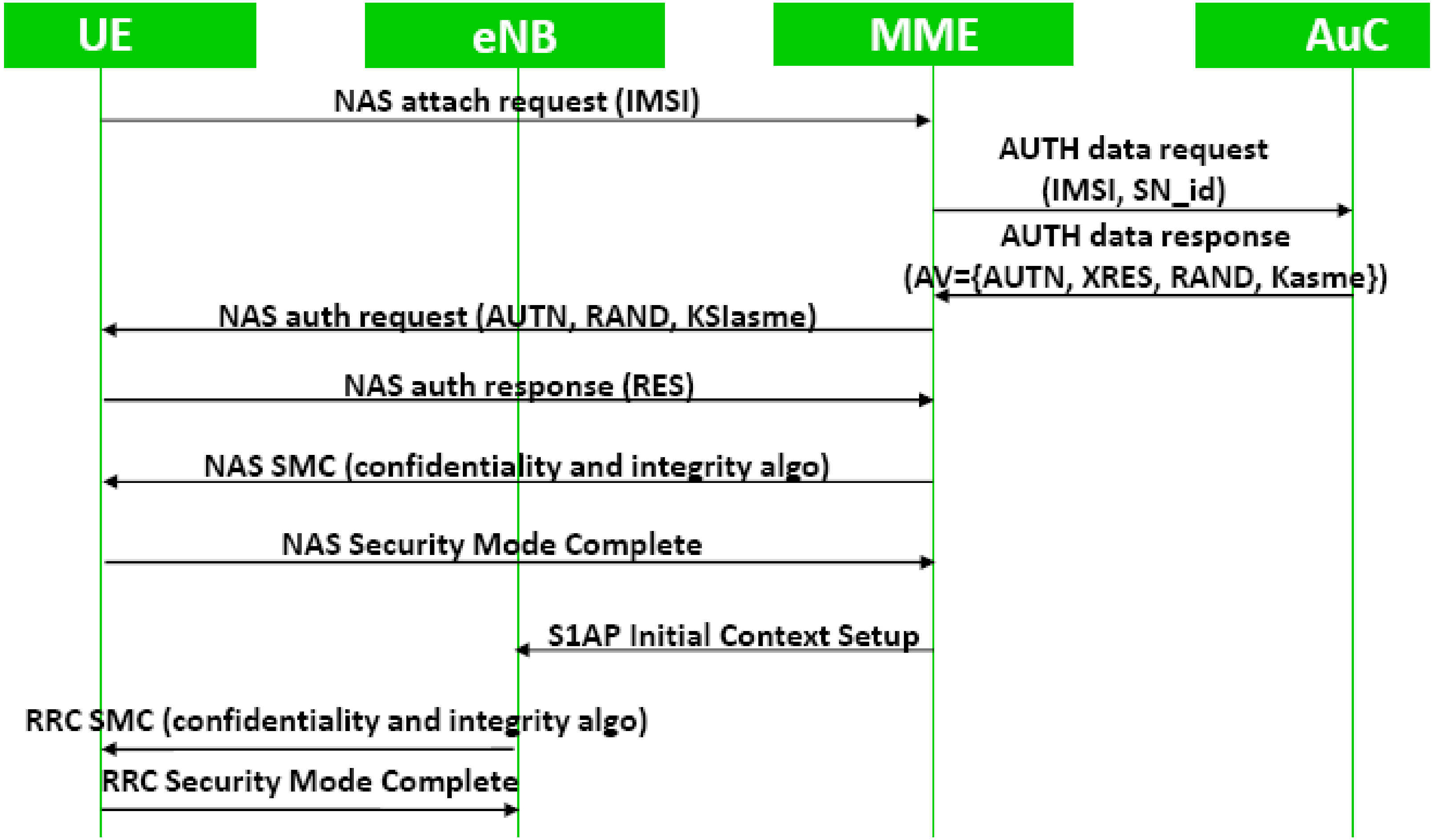
Access security

ASME

- **Access Security Management Entity** (ASME) is assumed by the MME.
- It receives the top-level keys in an access network from the HSS or HLR.
- The MME invokes the AKA procedures by requesting authentication vectors to the HE (Home environment). The HE sends an authentication response back to the MME that contains a fresh authentication vector, including a base-key named KASME

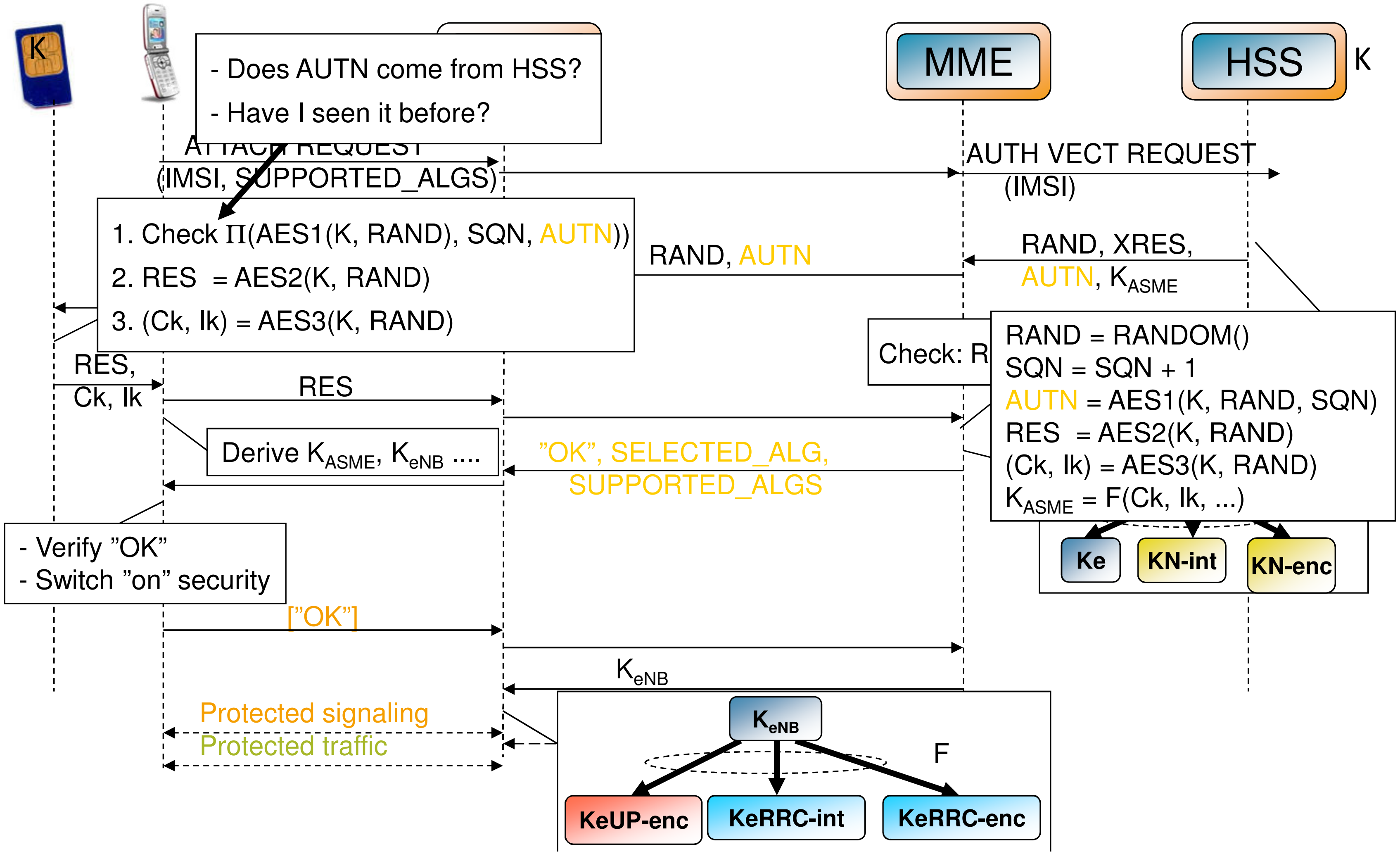
Authentication and Key Agreement Algorithm

AKA procedure



Authentication and Ciphering procedure

LTE: Initial Attach



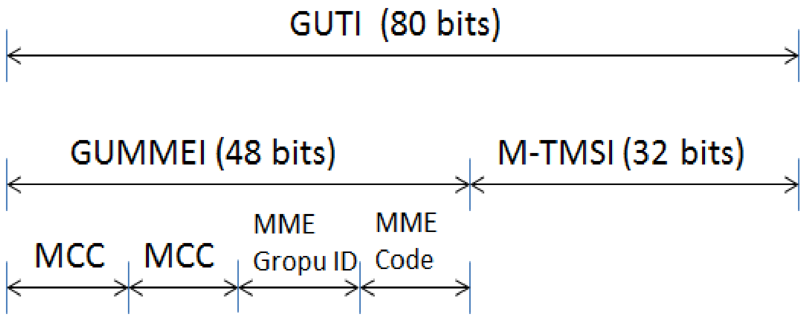
User identity privacy

- ***International Mobile Subscriber Identity*** (IMSI) allocated to each mobile subscriber in every (GSM, UMTS, and EPS) system.
- VLRs, SGSNs and MMEs may allocate ***Temporary Mobile Subscriber Identities*** (X-TMSI) for subscriber identity confidentiality.
- An MS may be allocated three TMSIs through the:
  - VLR (TMSI)
  - SGSN (P-TMSI)
  - **MME (S-TMSI, M-TMSI, part of GUTI, *Globally Unique Temporary UE Identity*).**

Temporary Mobile Subscriber Identity (TMSI) structure and coding is chosen by agreement between operator and ME manufacturer in order to meet local needs.
TMSI = 4 bytes.

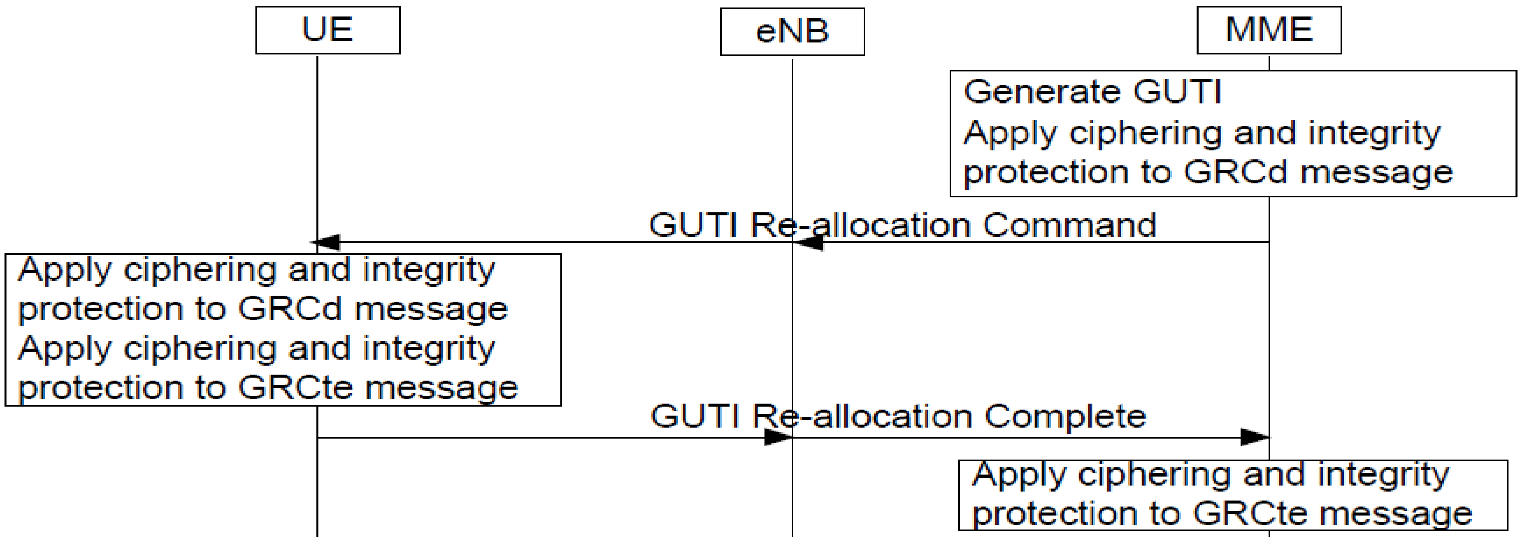
Globally Unique Temporary UE Identity (GUTI): unambiguous identification of the UE that does not reveal the UE or the user's permanent identity in the *Evolved Packet System* (EPS). It allows the identification of the MME and network.

GUTI = ***GUMMEI*** + ***M-TMSI***, where
GUMMEI = MCC + MNC + MME Identifier
MME Identifier = MME Group ID + MME Code
MCC and MNC shall have the same field size as in earlier 3GPP systems.
M-TMSI shall be of 32 bits length.
MME Group ID shall be of 16 bits length.
MME Code shall be of 8 bits length.



GUTI for UE identity protection

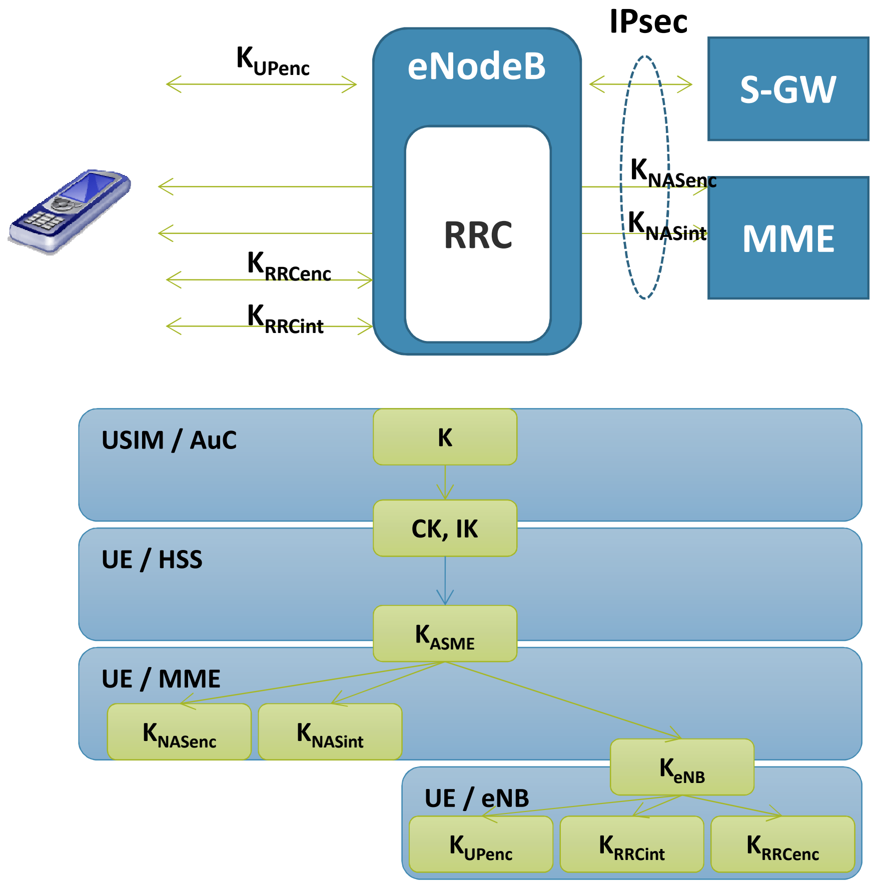
- **Temporary identity** used instead of the permanent identity IMSI.
- GUTI may be transferred from the **MME to the UE** via:
  - *Attach Accept* message as an answer to an Attach Request message,
  - *Tracking Area Update Accept* message as an answer to a Tracking Area
  - *Update Request* message,
  - *GUTI Re-allocation Command* message.



User data confidentiality and integrity

Security Aspects and parameters in LTE

- Security concerns:
  - UE **authentication** (USIM: 128 bits key);
  - Internal signaling protection (**integrity**), signaling and traffic **encryption**;
  - **Signaling encryption for RRC and NAS**.
- Safety is enhanced by protecting all entities
  - Hierarchical protection (UE, eNB, ASME, HSS, AuC);
  - Transport security on all interfaces.



ASME: Access Security Management Entity

- Encryption is performed at the ***eNodeB***.
- MSPs (*Mobile Services Provider*) to support encryption within the transport network, especially if using third-party backhaul transport providers or public Internet transport.
- ***IPSec tunneling*** between the eNodeB and the security gateway used to secure data and provide QoS to manage the security centrally.

NAS security

- NAS messages, **UE** and **MME** scope .
- NAS message communication between UE and MME are ***Integrity*** protected and ***Ciphered*** with extra NAS security header.

AS security

- RRC and user plane data, **UE** and **eNB** scope .
- PDCP layer in UE and eNB side responsible for ciphering and integrity.
- RRC messages integrity protected and ciphered but U-Plane data is only ciphered.

Different Security algorithms (integrity/ciphering)

- **Integrity** (**EIA**: EPS Integrity Algorithm)
  - **“0000”** EIA0 Null Integrity Protection algorithm
  - **“0001”** 128-EIA1 SNOW 3G
  - **“0010”** 128-EIA2 AES
- **Ciphering** (**EEA**: EPS Encryption Algorithm)
  - **“0000”** EEA0 Null ciphering algorithm
  - **“0001”** 128-EEA1 SNOW 3G based algorithm
  - **“0010”** 128-EEA2 AES based algorithm

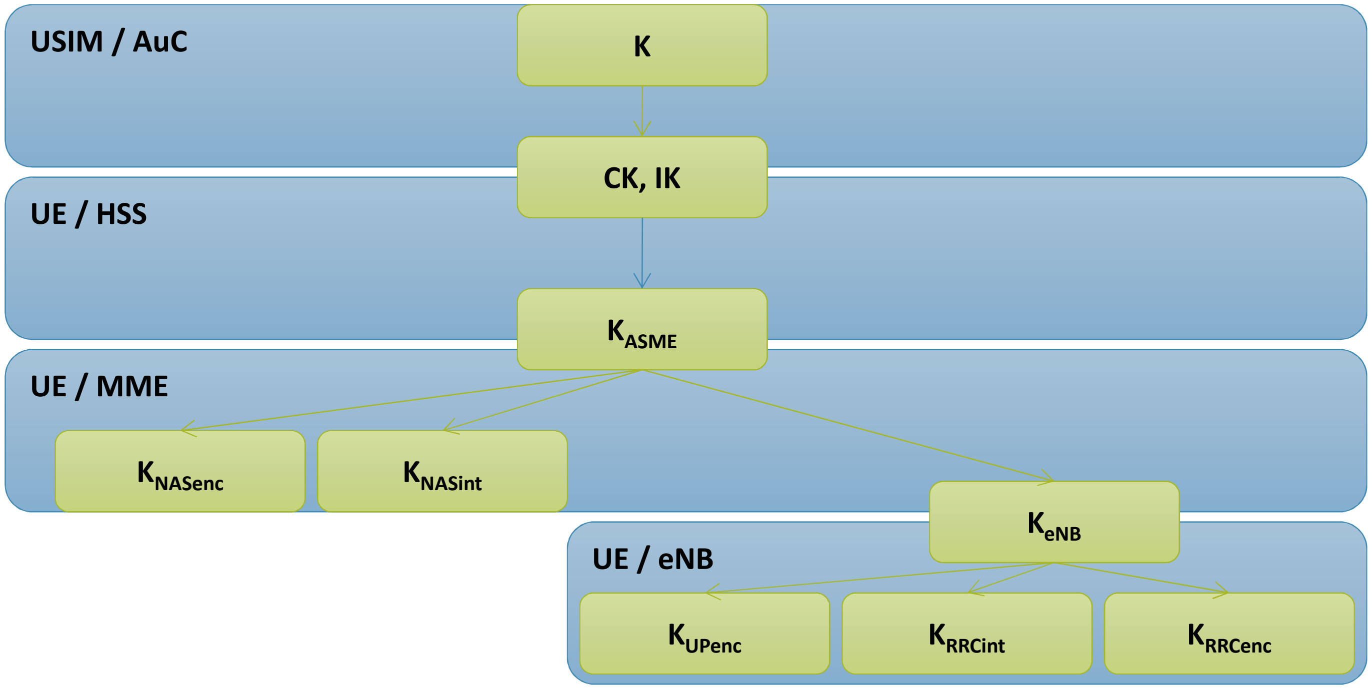
Key/parameters distribution in LTE nodes

	UE	eNB	MME	HSS/Au
Pre Shared keys	UE Security Key (K)			UE Security Key
	AMF			AMF
	OP			OP
Generated keys				SQN
				RAND
Derived Auth vectors	IK			IK
	CK			CK
				AK
	RES			XRES
	XMAC			MAC
				AUTN
Derived Keys	KASME		KASME	
	Knas-int		Knas-int	
	Knas-enc		Knas-enc	
	KeNB	KeNB		
	Krrc-int	Krrc-int		
	Krrc-enc	Krrc-enc		
	Kup-enc	Kup-enc		

AMF (Authentication Management Field) – **SQN** (Sequence Number)

Key hierarchy

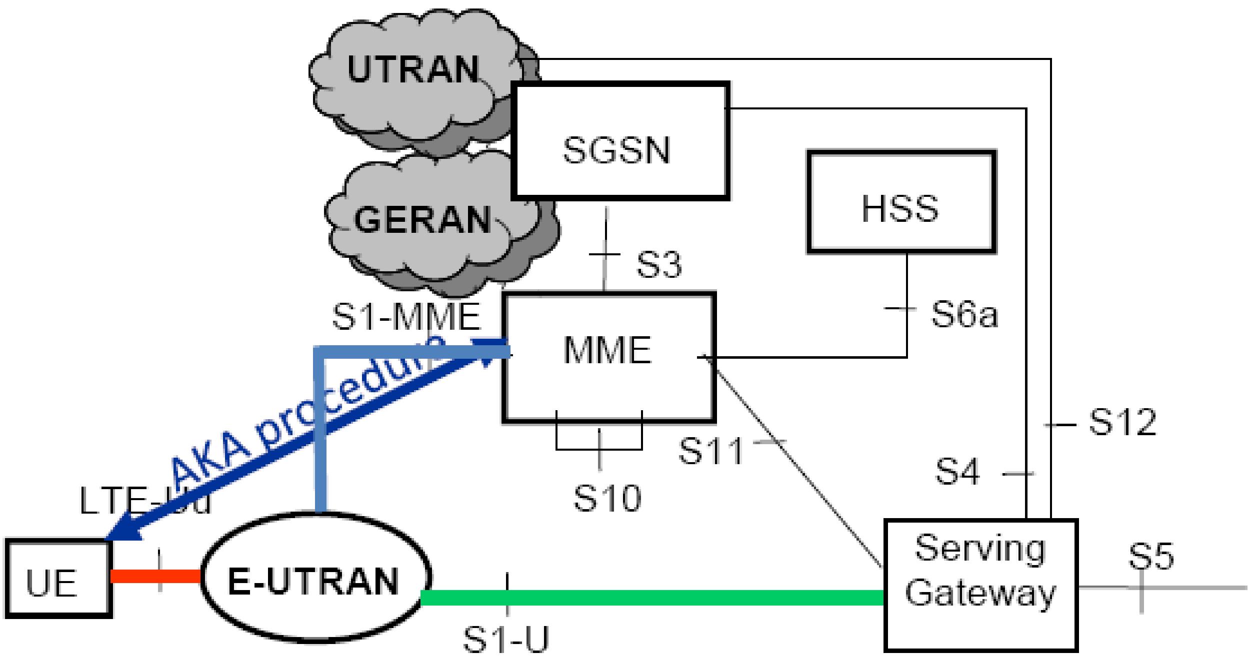
- Faster handovers and key changes, independent of AKA
- Added complexity in handling of security contexts



ASME: Access Security Management Entity

Security Aspects and parameters in LTE

Security aspects in LTE



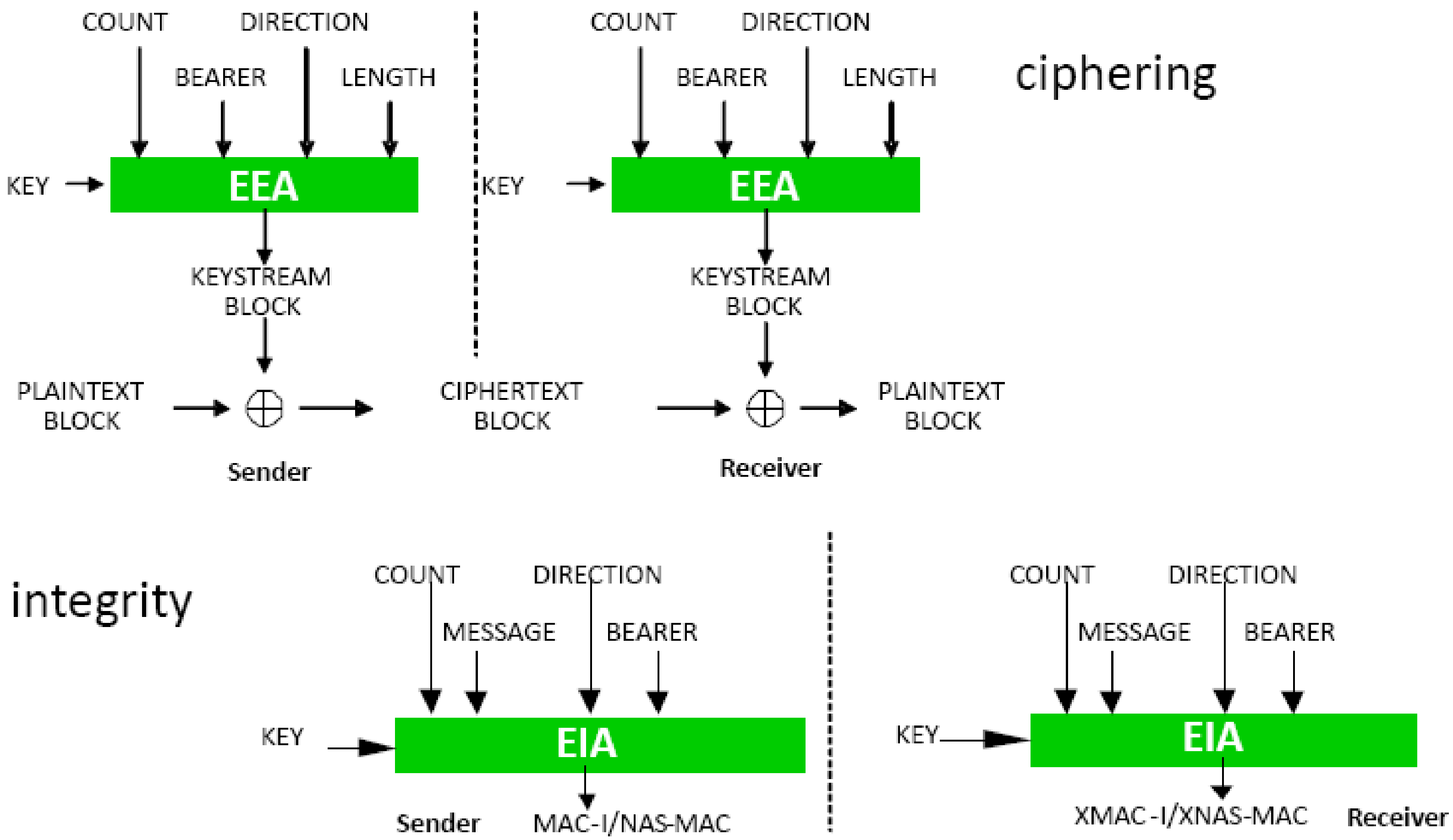
Confidentiality and integrity for signalling and confidentiality for user plane (RRC & NAS)

Confidentiality and integrity for signalling only (NAS)

Optional user plane protection (IPsec)

Security Aspects and parameters in LTE

LTE Ciphering and Integrity Algorithms



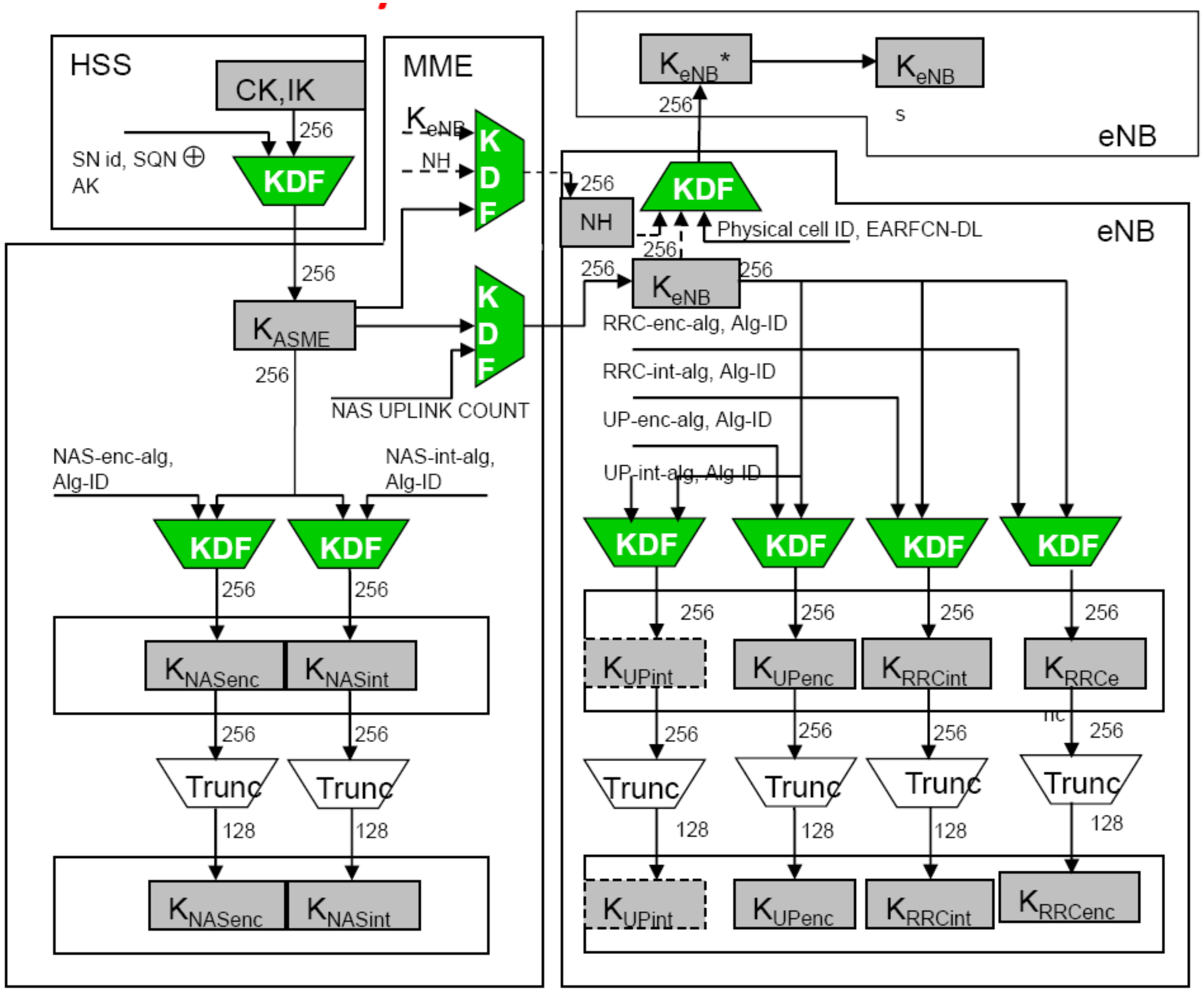
- Security keys for AS (*Access Stratum*)
  - User data and control
  - Different from those used in EPC.
- eNodeB keys:
  - K_{eNB}: Derived by the UE and the MME from K_{ASME} (*'Master Key'*) and issued by the MME in eNodeB
  - K_{eNB}: used to derive the AS traffic keys and handover key $K_{eNB}{}^{*}$
  - $K_{eNB}{}^{*}$: Derived from the UE and the source from eNodeB K_{eNB} or valid NH (Next Hop) ⇨ During the handover, the terminal and the target eNodeB derive a new $K_{eNB}{}^{*}$ from K_{eNB}

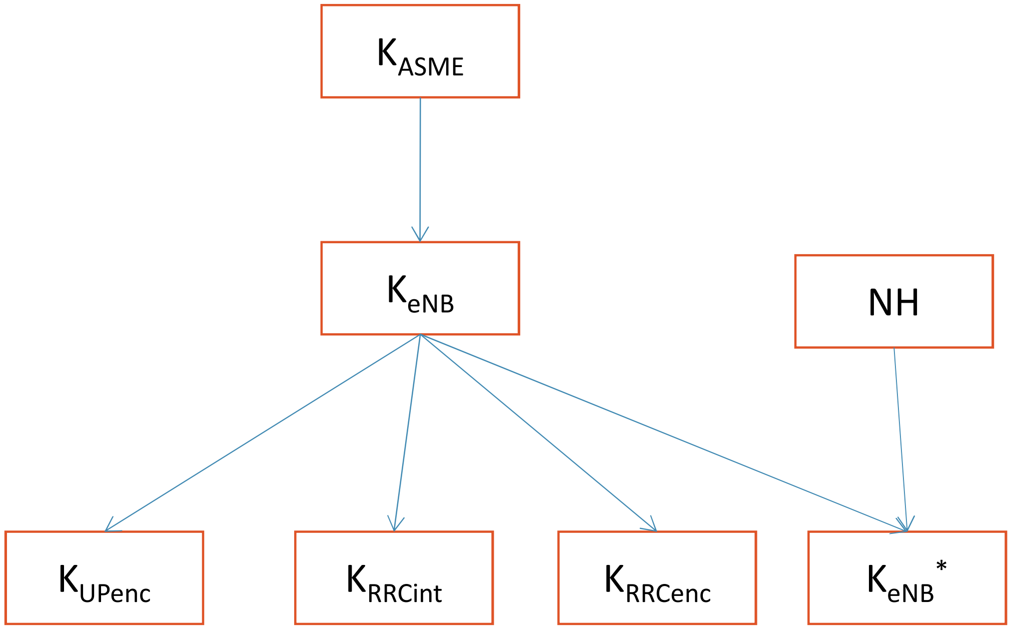
Security Aspects and parameters in LTE

- K_{UPenc}: Derived from K_{eNB} and used to **encrypt the user plane**
- K_{RRCint}: Derived from K_{eNB} and used to ensure **the integrity of RRC message**
- K_{RRCenc}: Derived from K_{eNB} and used to **encrypt RRC messages**
- Next Hop (NH): Intermediate key used to derive K_{eNB}^* during **intra-LTE handover security**
- The NCC (*Next Hop Chaining Counter*) determines if the next K_{eNB}^* must be based on a current K_{eNB}^* or fresh NH:
  - If no fresh NH available ⇨ target PCI (*Physical Cell Identity*) + K_{eNB}
  - Fresh NH ⇨ Target PCI + NH

Security Aspects and parameters in LTE

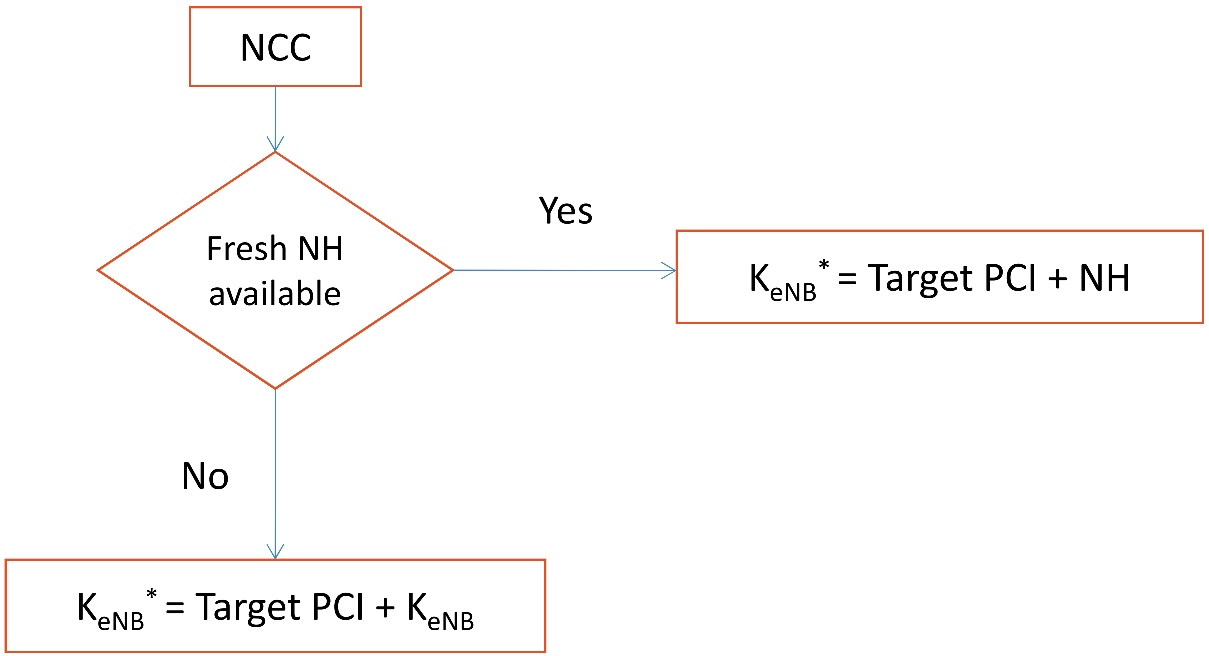
Keys derivation scheme





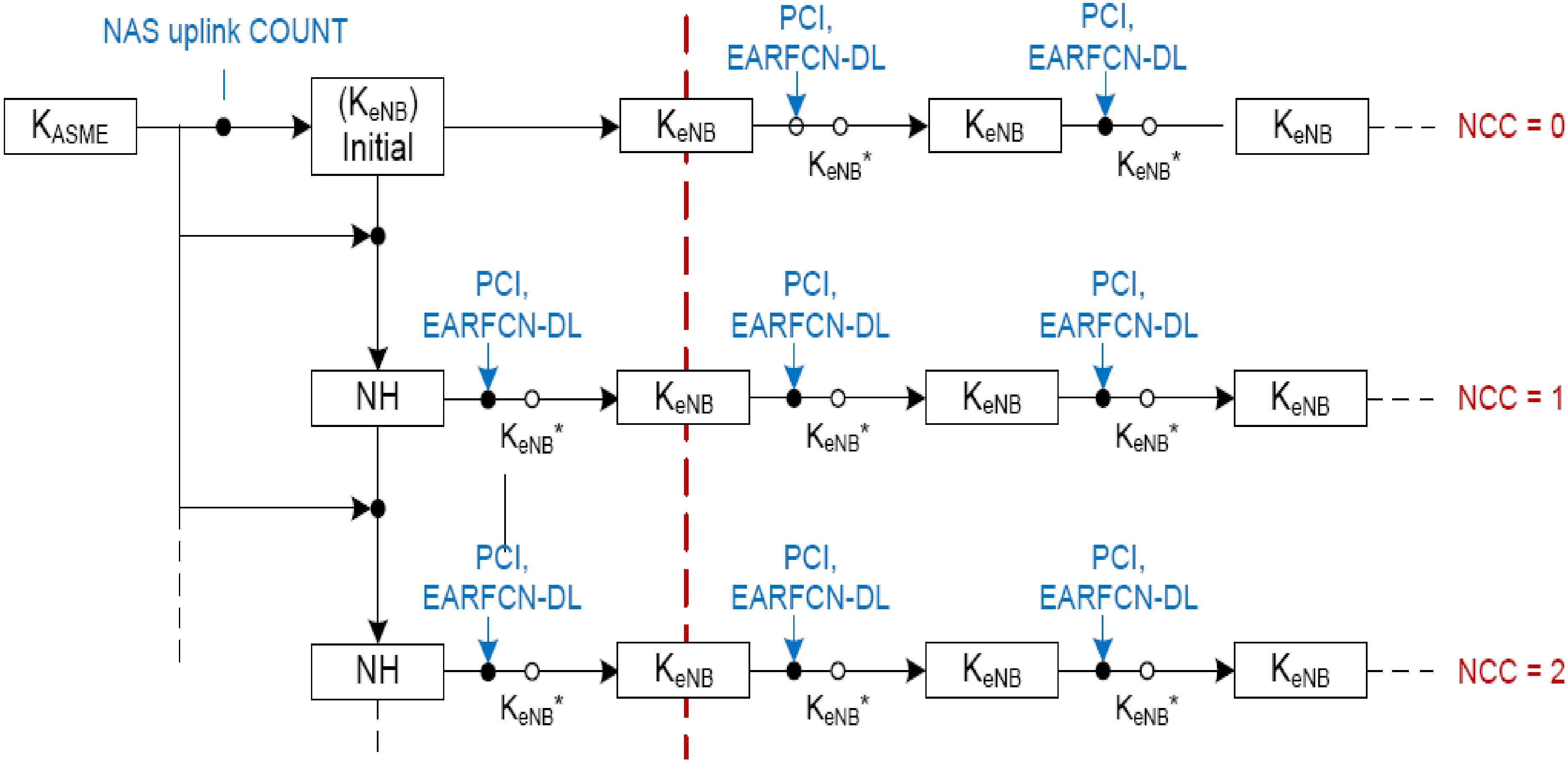
Different Keys Scheme

Security Aspects and parameters in LTE



K_{eNB}^{*} determination

Handover key chaining

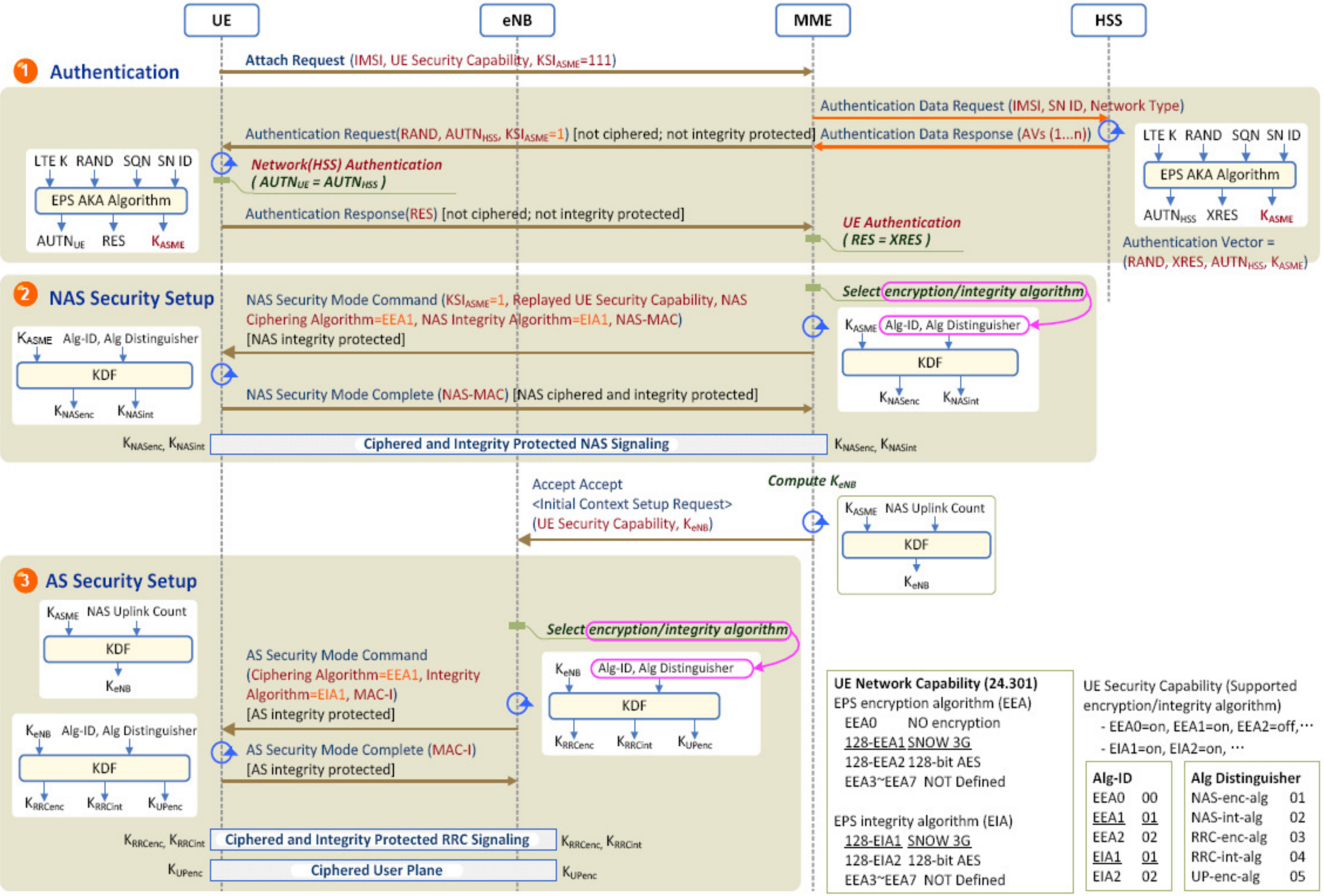


NCC: Next Hop Chaining Counter

Synthesis

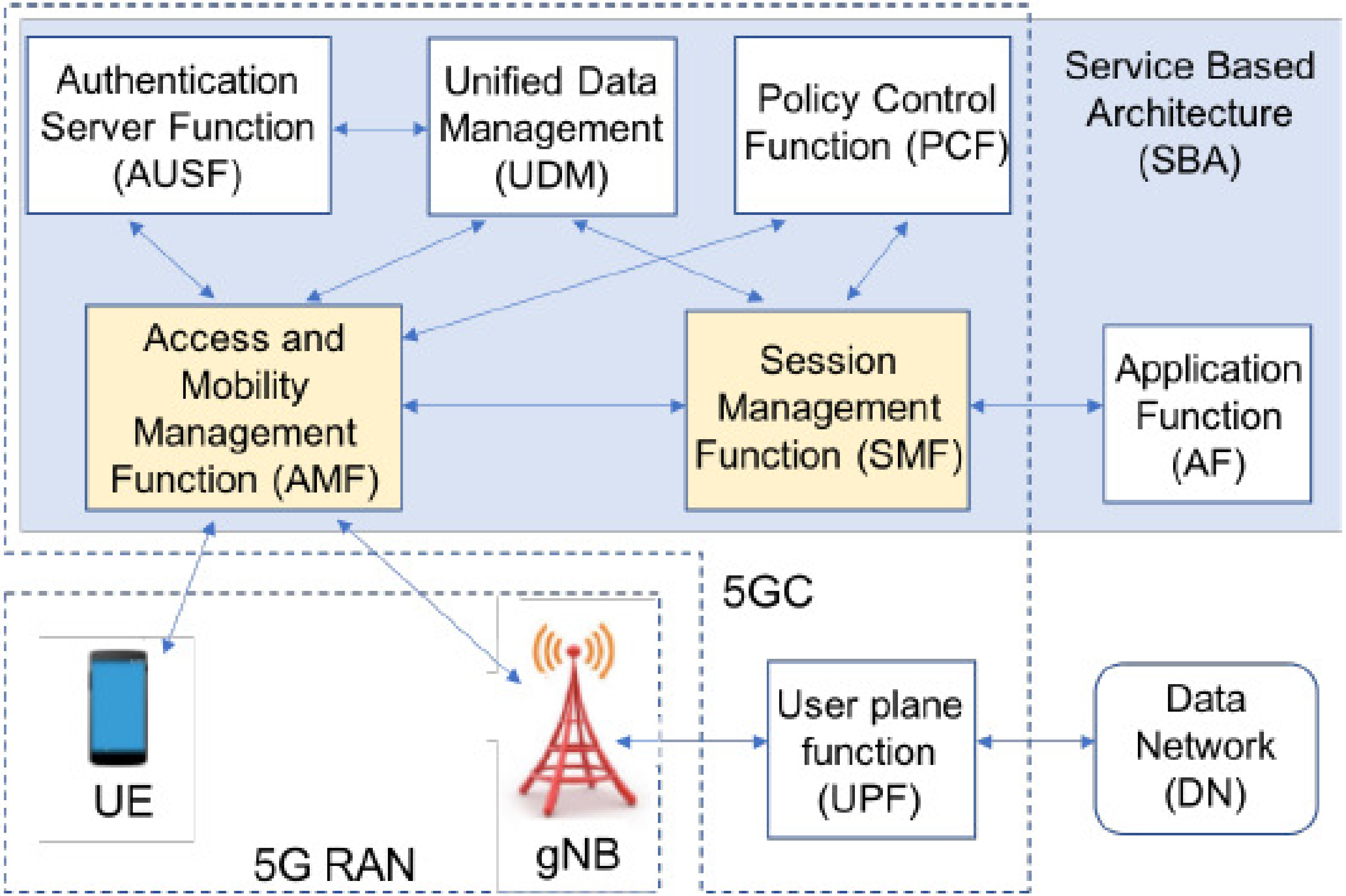
Security Aspects and parameters in LTE

Security related message flow

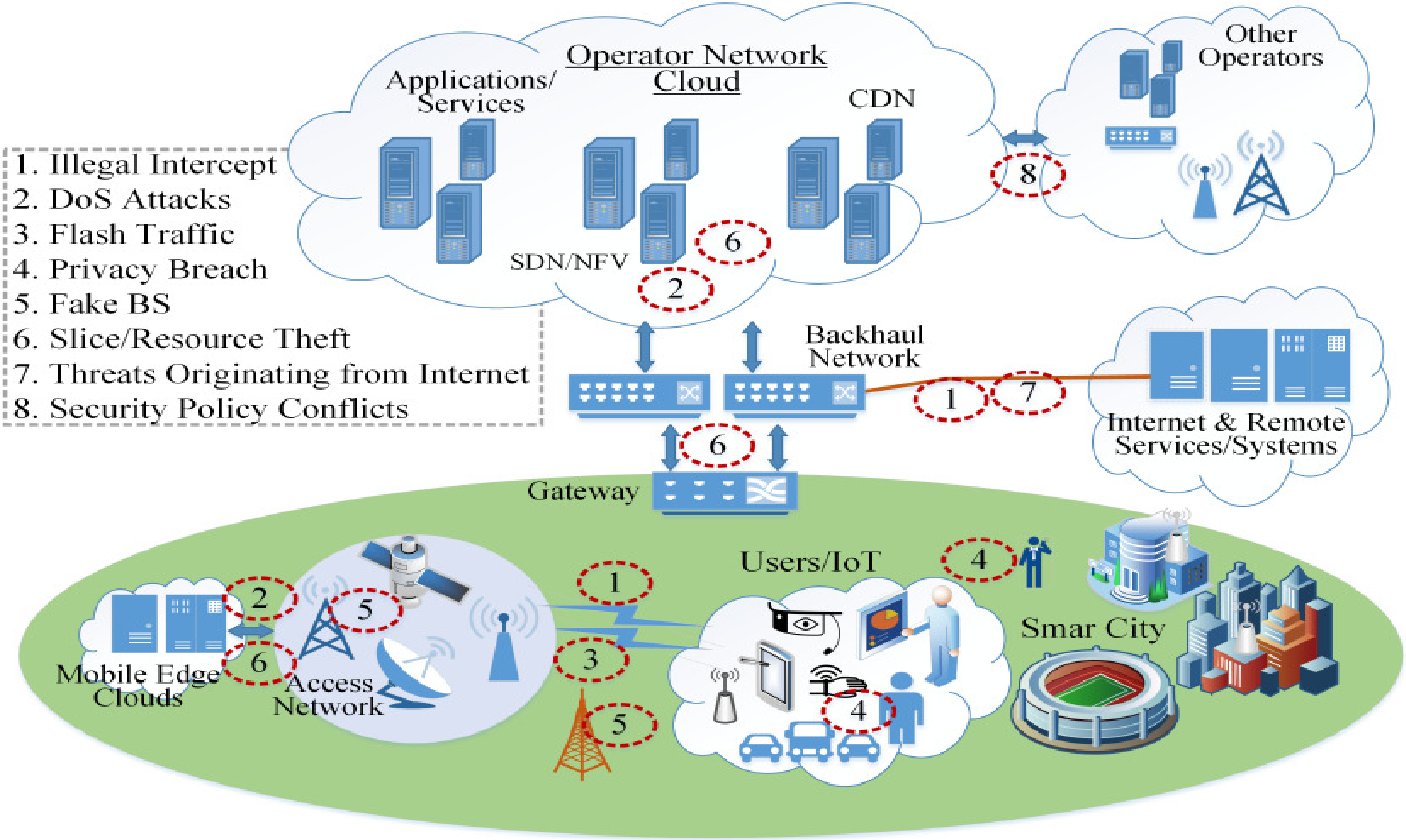


B. 5G Release 15 Security

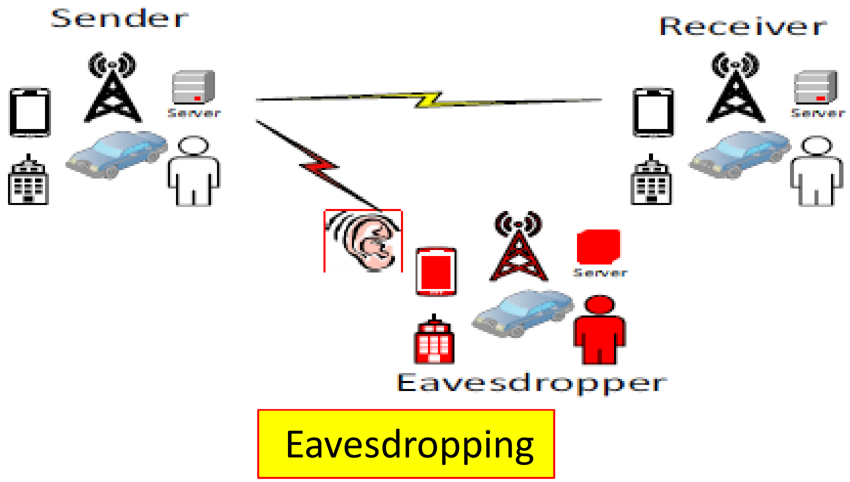
Simplified 5G reference network architecture

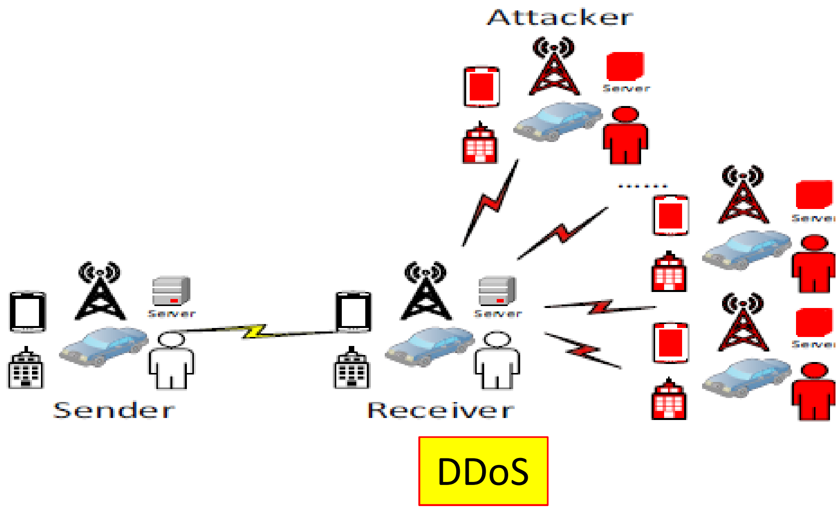


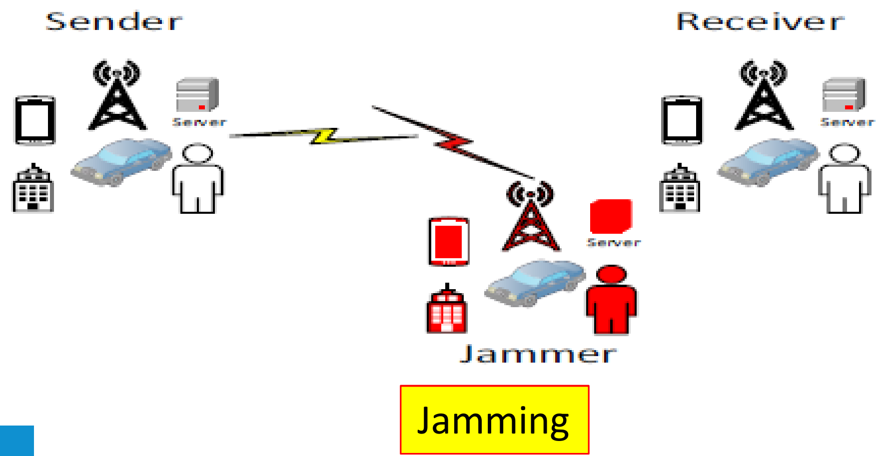
Security threat landscape in 5G networks

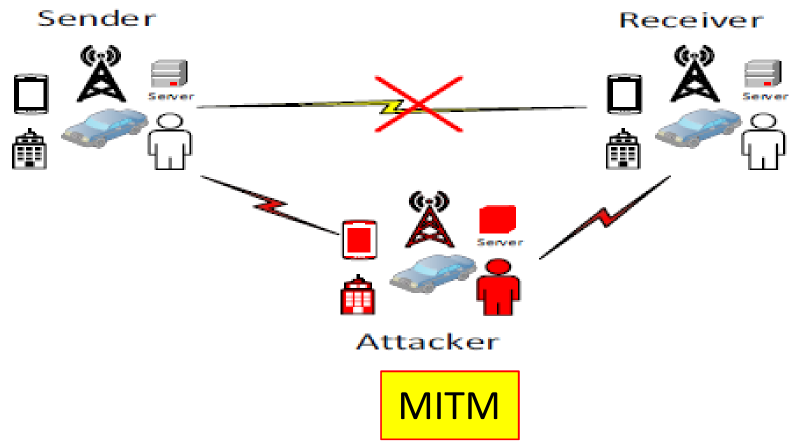


Main attacks in 5G wireless networks

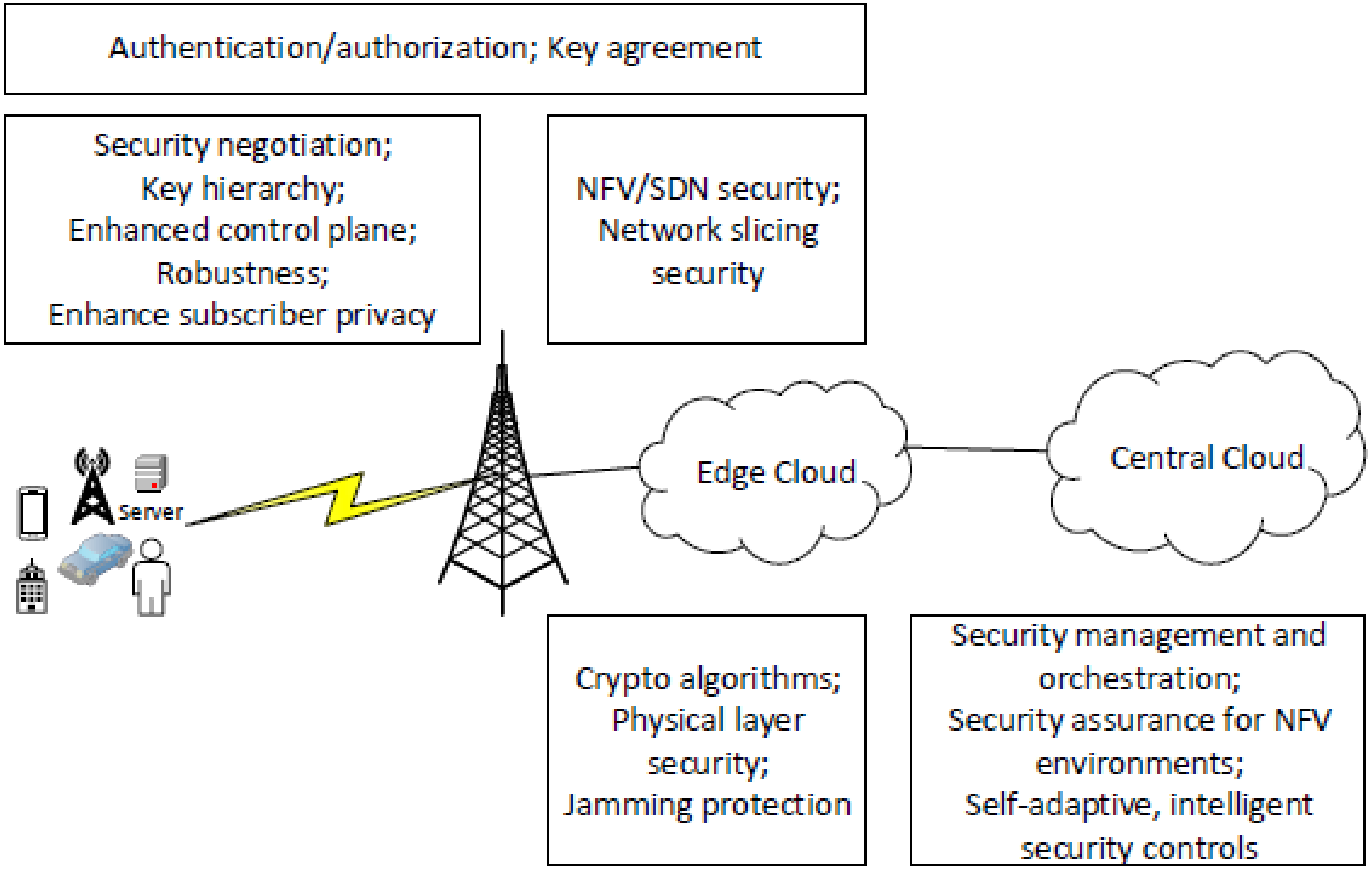








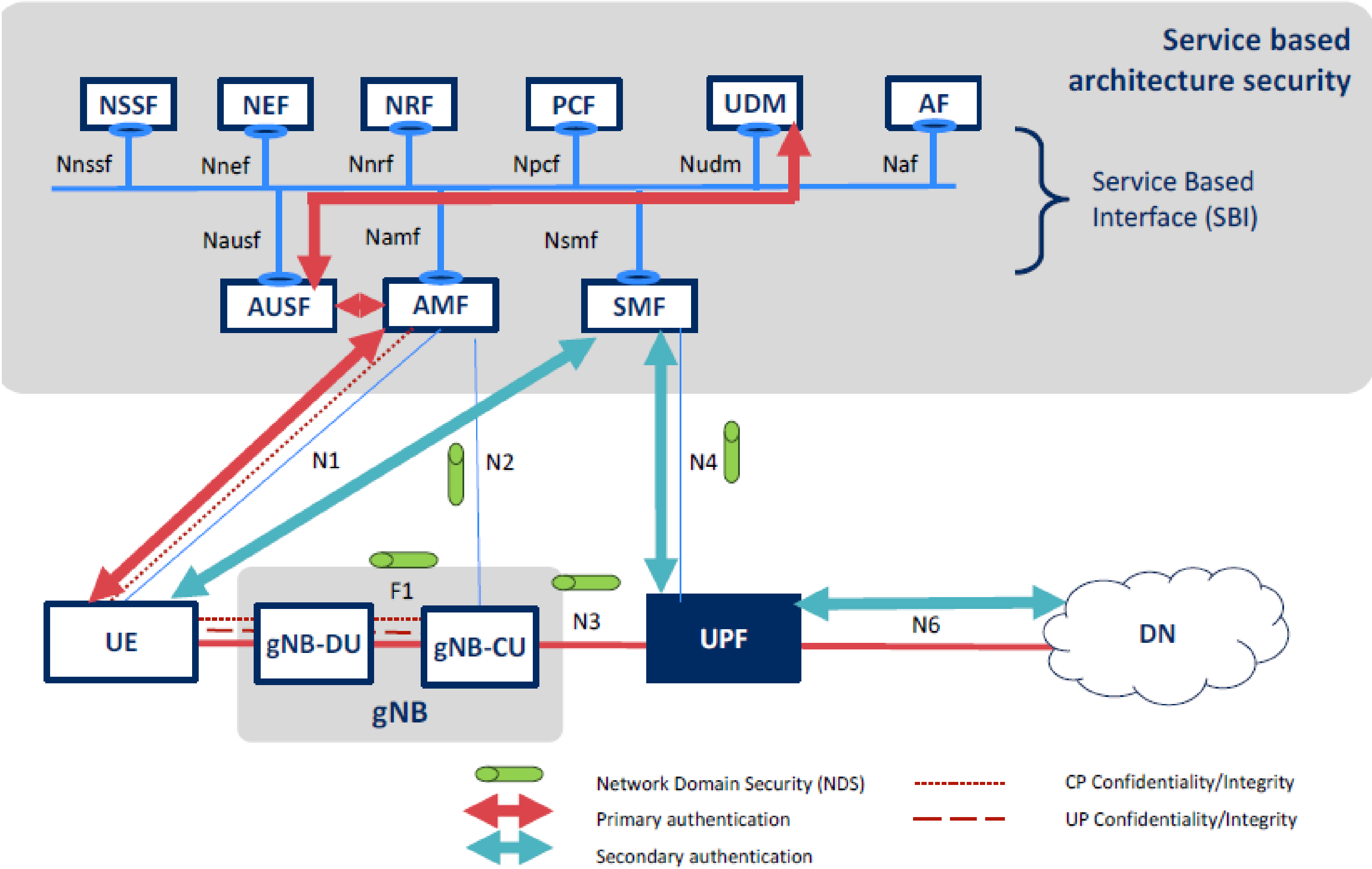
Elements in a 5G security architecture



SECURITY CHALLENGES IN 5G NETWORK SEGMENTS

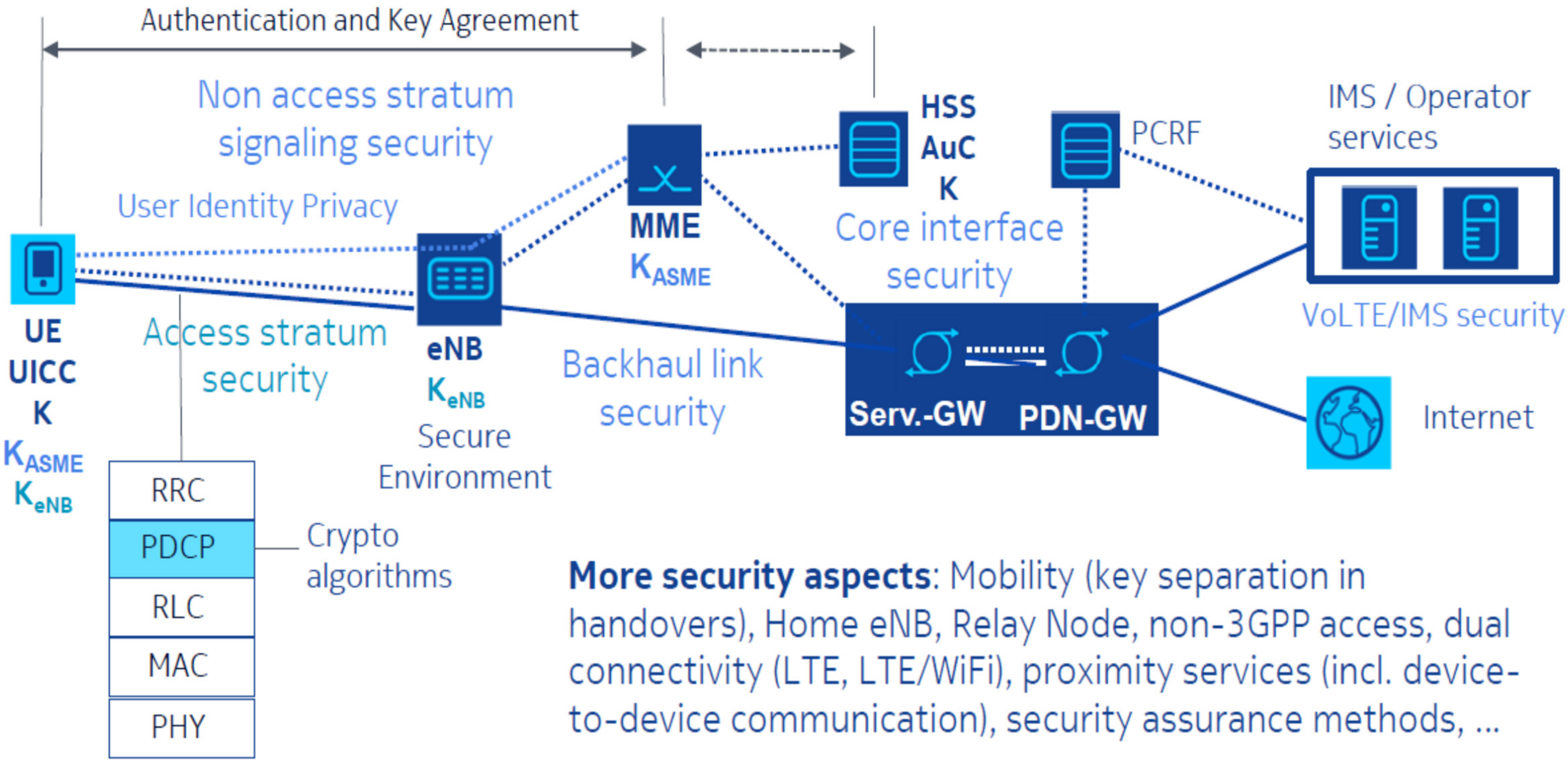
Security threats	Potential targets	Affected network segments		
		HetNet Access	Backhaul	Core Network
DoS attack on signaling plane	Centralized control elements			✓
Hijacking attacks	SDN controller, hypervisor	✓	✓	
Signaling storms	5G core network elements			✓
Un-authorized access	Low-power access points	✓		
Configuration attacks	Low-power access points	✓		
Saturation attacks	Ping-pong behavior in access points, and MME	✓		✓
Penetration attacks	Subscriber information			✓
User identity theft	User information data bases			✓
Man-in-the middle attack	Un-encrypted channels, e.g. in IoT	✓		
TCP level attacks	Gateways, router and switches		✓	
Key exposure	Radio interfaces	✓		
Session replay attacks	Session keys in non-3GPP access	✓		
Reset and IP spoofing	Control channels	✓		
Scanning attacks	Radio interfaces interfaces	✓		
IMSI catching attacks	Roaming and UE	✓		
Jamming attacks	Wireless channels	✓		
Channel prediction attacks	Radio interfaces	✓		
Active eavesdropping	Control channels	✓		✓
Passive eavesdropping	Control channels	✓		✓
NAS signaling storms	Bearer activation in core network elements			✓
Traffic bursts by IoT	Saturation of GTP end-points		✓	✓

5G security overview



Synthesis

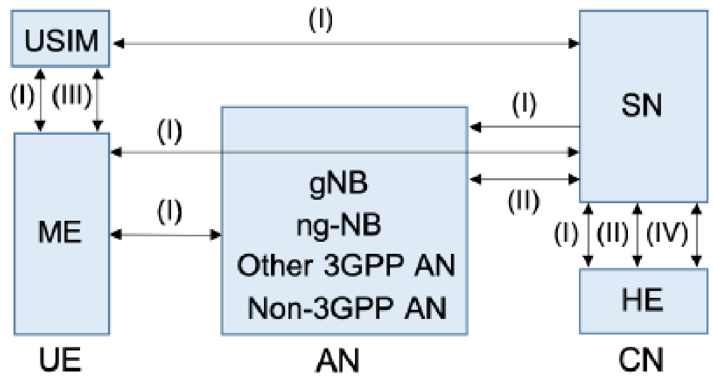
LTE Security Algorithms



More security aspects: Mobility (key separation in handovers), Home eNB, Relay Node, non-3GPP access, dual connectivity (LTE, LTE/WiFi), proximity services (incl. device-to-device communication), security assurance methods, ...

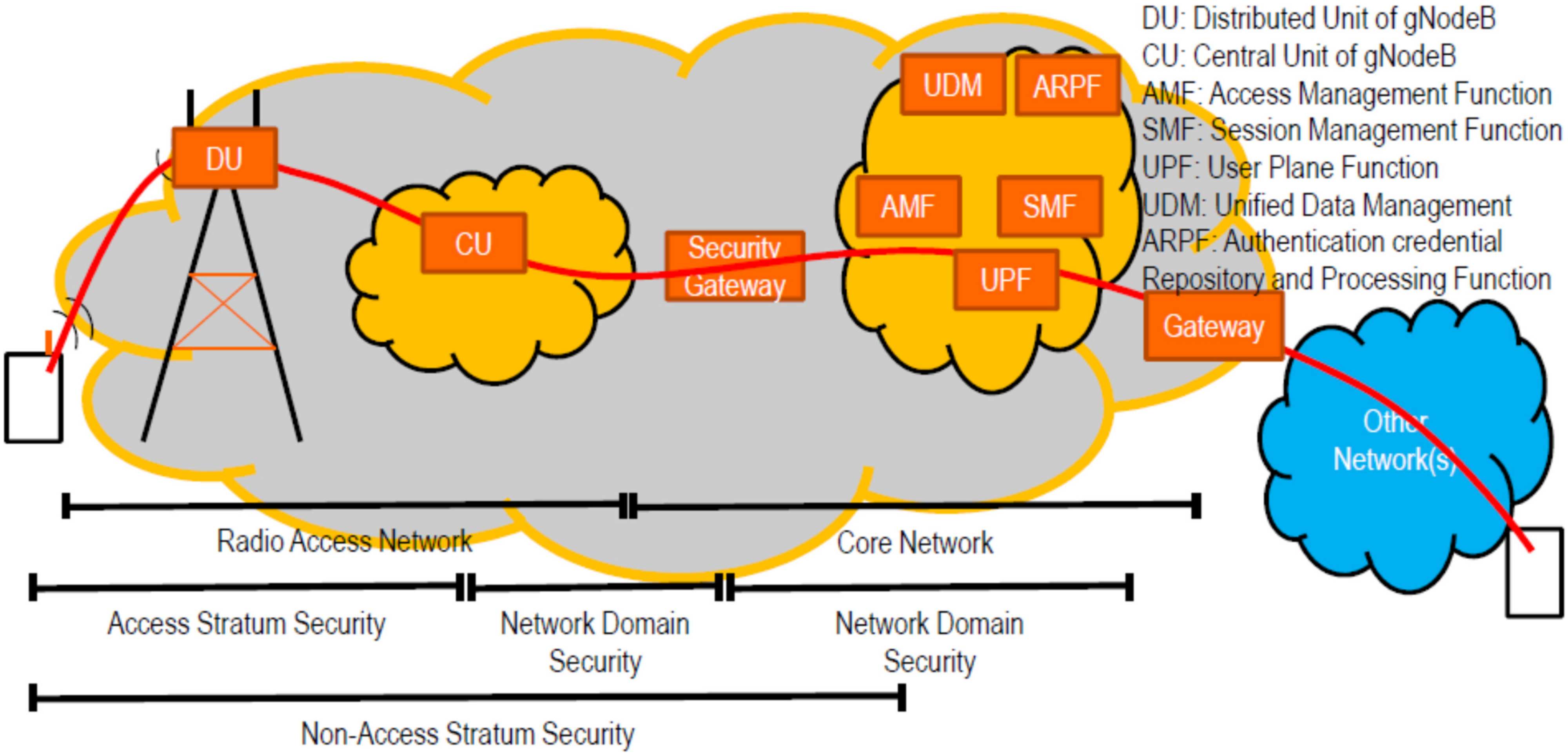
5G Security Architecture and Entities

5G security architecture (AN–Access Network, HE–Home Environment, ME–Mobile Equipment, SN–Serving Network)



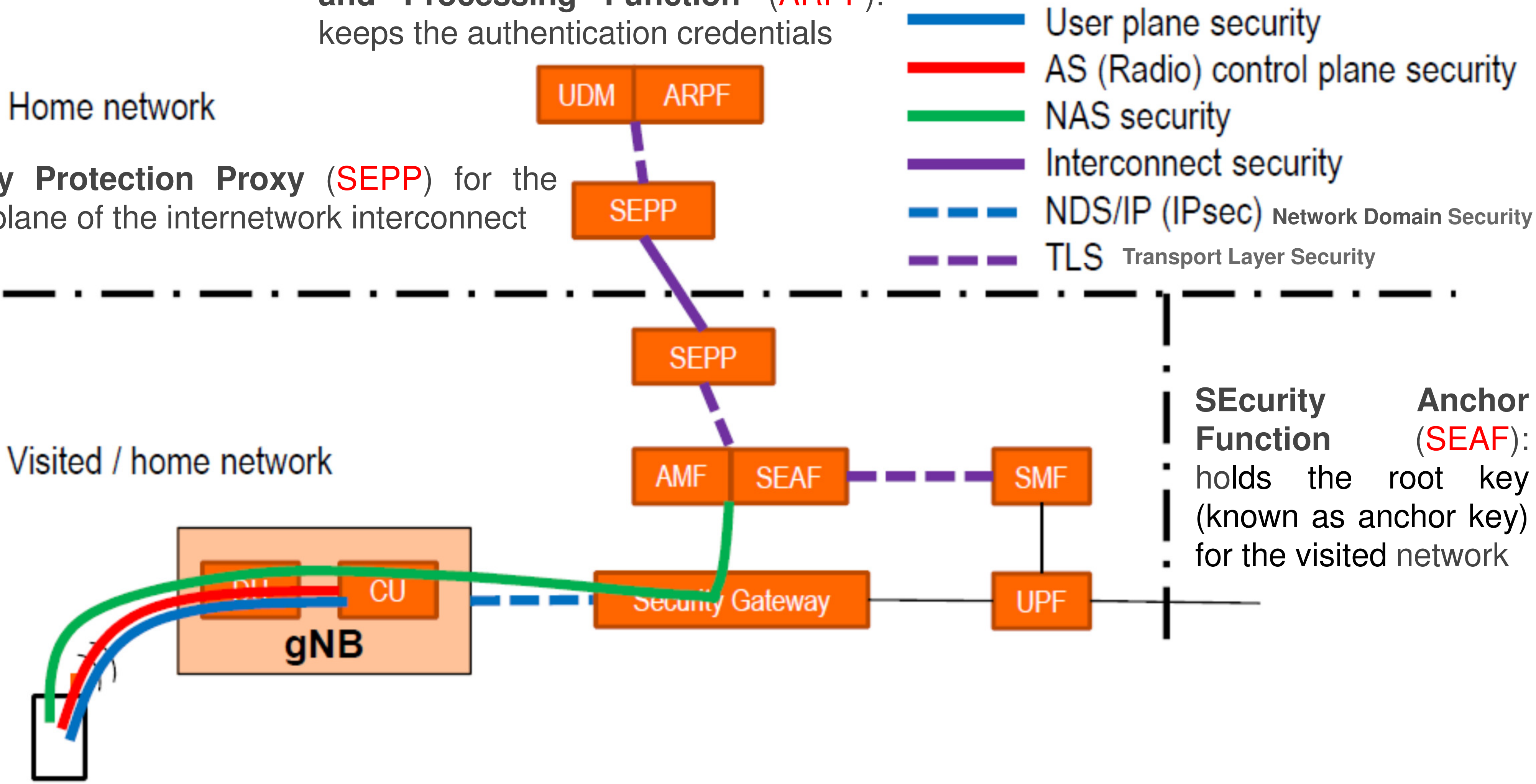
- **Network access security** (I): features and mechanisms to enable a UE to authenticate and securely access network services. UEs exchange protocol messages through the access network with the serving network (SN) and leverage the PKI, where keys are stored in the USIM and the home environment (HE).
- **Network domain security** (II): features and mechanisms to enable network nodes to securely exchange.
- **User domain security** (III): features and mechanisms at the UE that secure the access to UE and mobile services. It establishes hardware security mechanisms to prevent the UEs and USIMs from being altered.
- **Service-Based Architecture** (SBA) **domain security** (IV): network features and mechanisms for network element registration, discovery and authorization, for protecting the service-based interfaces. It allows new 5GC functions, which may be implemented as virtual network functions, to be securely integrated. Enables secure roaming, which involves the SN as well as the home network (HN)/HE.
- **Visibility and configurability of security**: features and mechanisms to allow informing users whether a security feature is in operation. Can be used to configure security features. As the 3GPP 5G security specifications establish optional security features and degrees of freedom for implementation and operation, 5G users may encounter different security context.

5G architecture and security domains



Authentication credential Repository and Processing Function (ARPF): keeps the authentication credentials

SEcurity Protection Proxy (SEPP) for the control plane of the internetwork interconnect



SEcurity Anchor Function (SEAF): holds the root key (known as anchor key) for the visited network

Trust model in the UE

2 trust domains:

1. The tamper proof universal integrated circuit card (**UICC**) on which the Universal Subscriber Identity Module (**USIM**) resides as trust anchor
2. The Mobile Equipment (**ME**)

The USIM and the ME form the **UE**.

DU and CU in the RAN

- RAN is separated into:
  - **Distributed Units** (DU): does not have any access to customer communications. May be deployed in unsupervised sites
  - **Central Units** (CU): terminates the AS security. Deployed in sites with restricted access to maintenance personnel
- DU and CU form the **gNB**

Core network security

- **Access and Mobility Management Function** (AMF) serves as termination point for NAS security.
- AMF is collocated with the **SEcurity Anchor Function** (SEAF) that holds the **root key** (known as **anchor key**) for the visited network
- The security architecture allows separation of the **security anchor** from the **mobility function** in a future evolution of the system architecture
- The **ARPF** (*Authentication Credential Repository and Processing Function*) is collocated with the UDM and stores the long-term security credentials like the key **K** (EPS AKA) or **EAP-AKA** for authentication

Identity protection

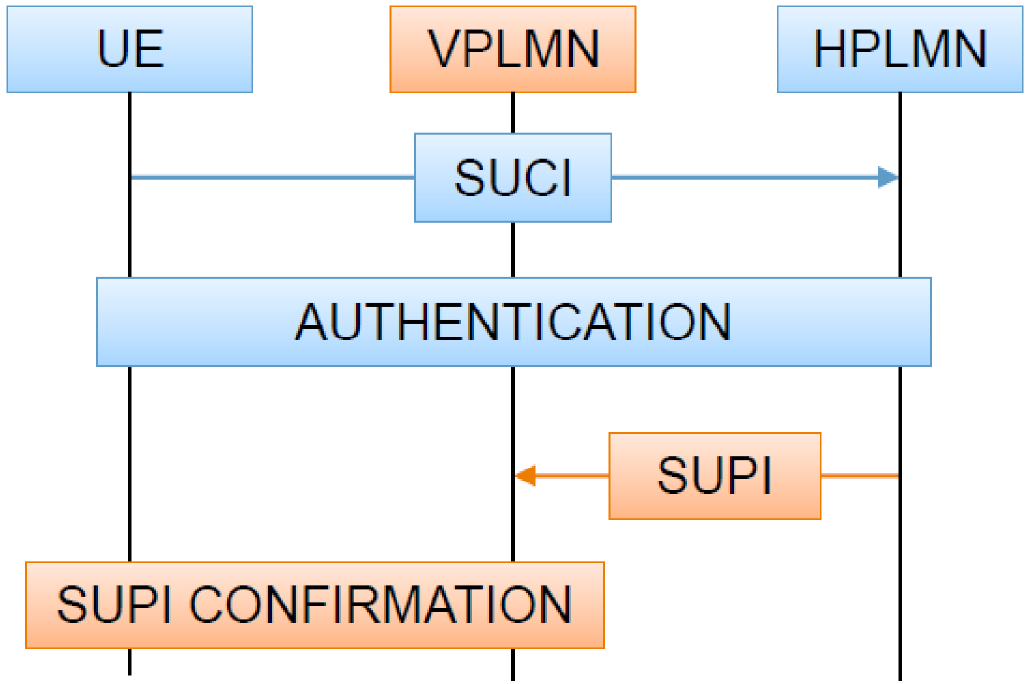
MAJOR CHANGES IN 5G –SUBSCRIBER PRIVACY

Solution:

- SUPI encrypted with home network public key on initial attach (SUCI)
- Complete authentication
- Then, send SUPI from HPLMN to VPLMN
- Finally, confirm SUPI by binding into a key

Further details:

- Encryption can done on UE or USIM
- Two algorithms standardized on UE side
- Algorithms on the USIM can be controlled by operators



Note: in order to fight against IMSI catchers, 5G introduces the **Subscriber Permanent Identifier** (SUPI), as replacement of the IMSI, and a PKI for the encryption of the SUPI into the **Subscriber Concealed Identifier** (SUCI)

4G

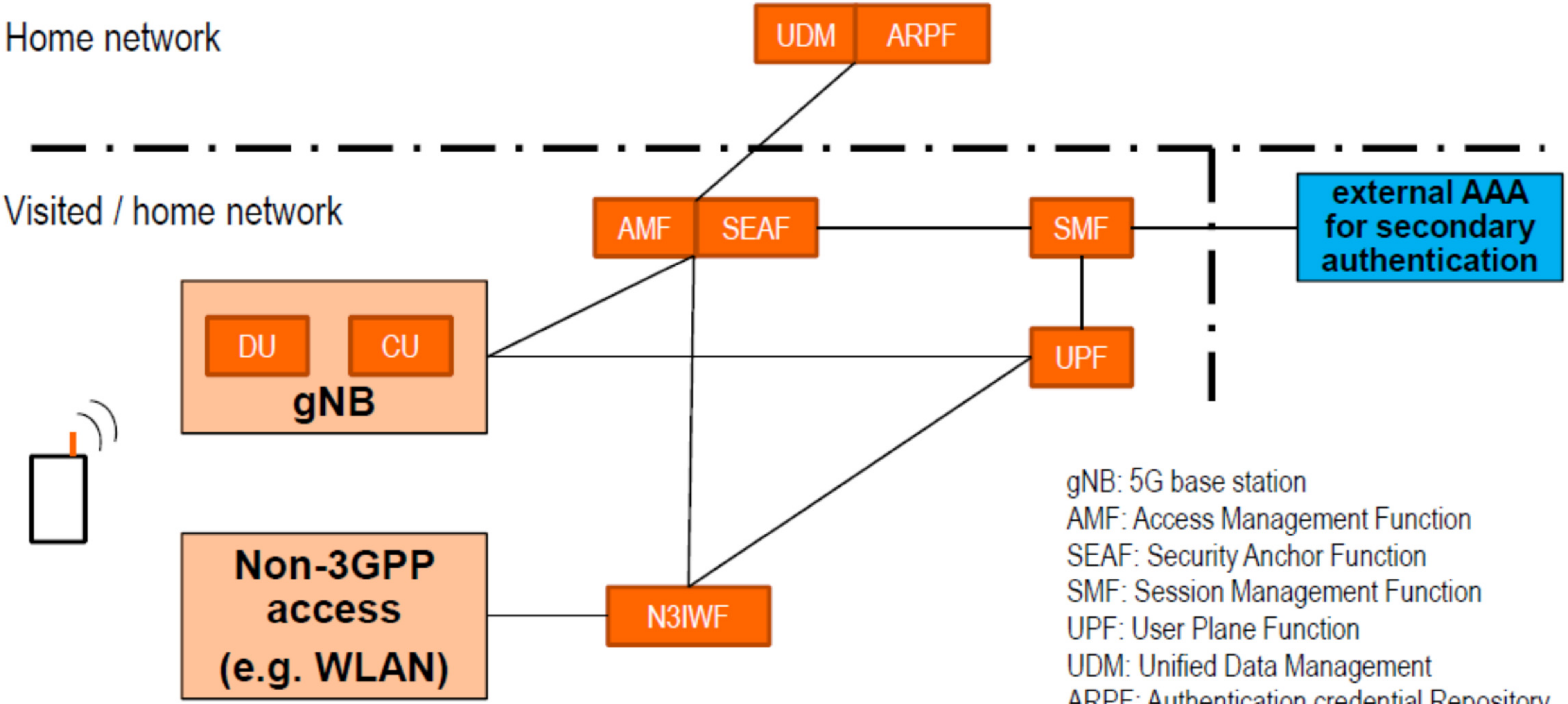
- Initial attach with permanent identity
- Response to identity request in clear

5G improvements

- Encryption of ***SUPI*** with public key of home operator (***SUCI***)
- Routing information (home network ID) in clear
- SUPI revealed to VPLMN only after authentication
- Binding of SUPI into key
- UE and HPLMN have to use the same SUPI: requested for lawful intercept purposes
- Respond to identifier request with SUCI
- No SUPI based paging

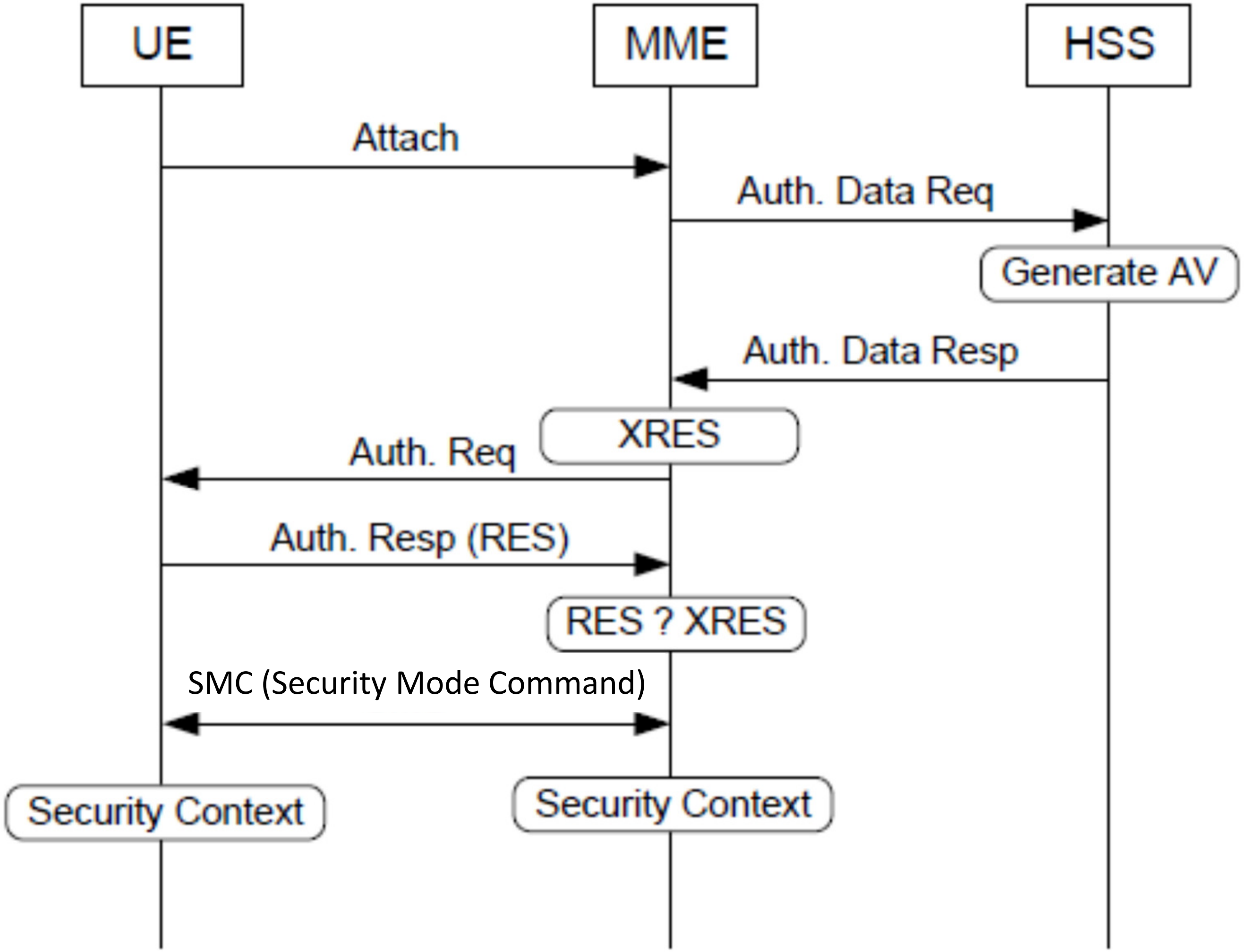
Access Security

Authentication in a non-3GPP network

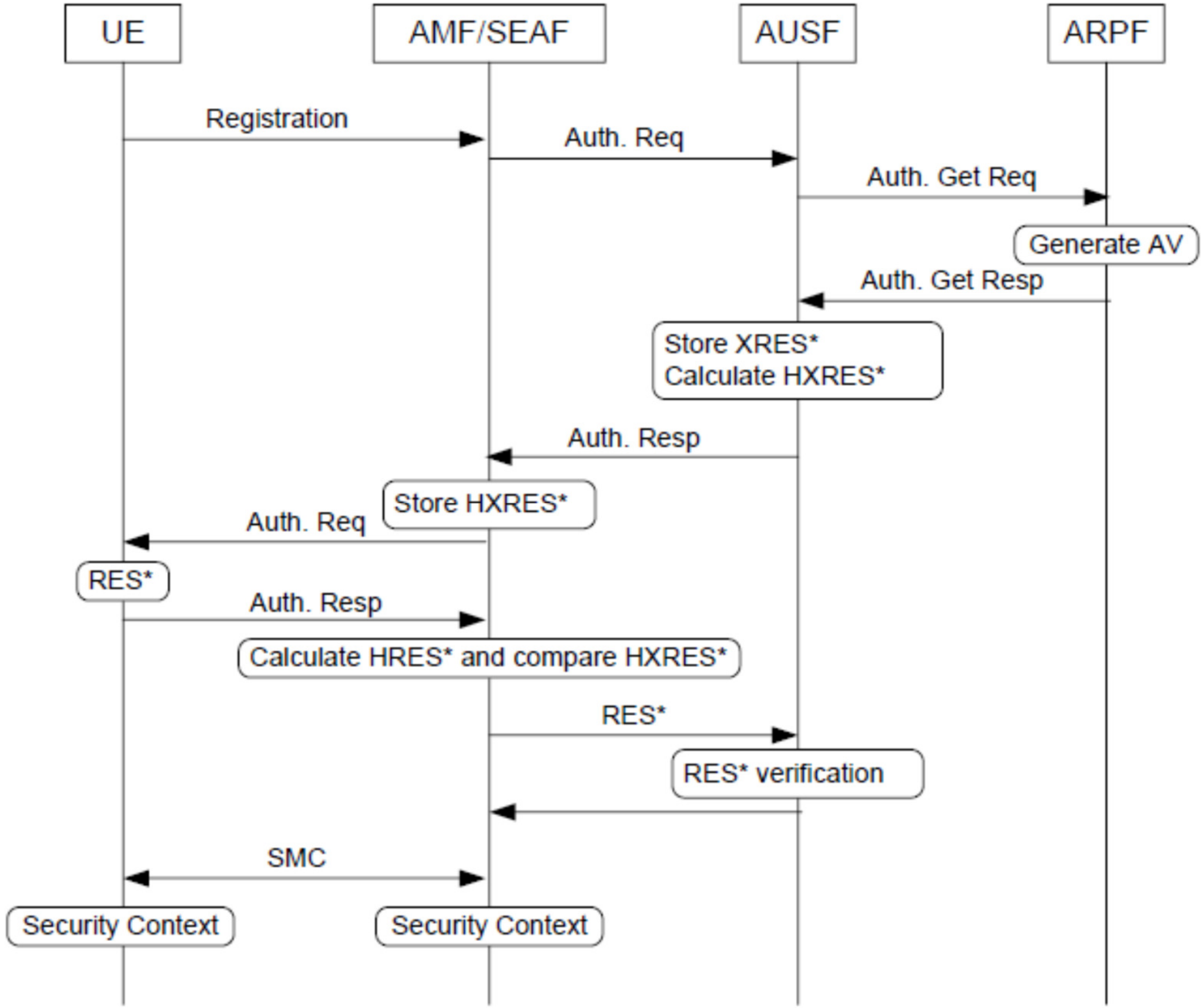


gNB: 5G base station
AMF: Access Management Function
SEAF: Security Anchor Function
SMF: Session Management Function
UPF: User Plane Function
UDM: Unified Data Management
ARPF: Authentication credential Repository and Processing Function
N3IWF: Non-3GPP InterWorking Function

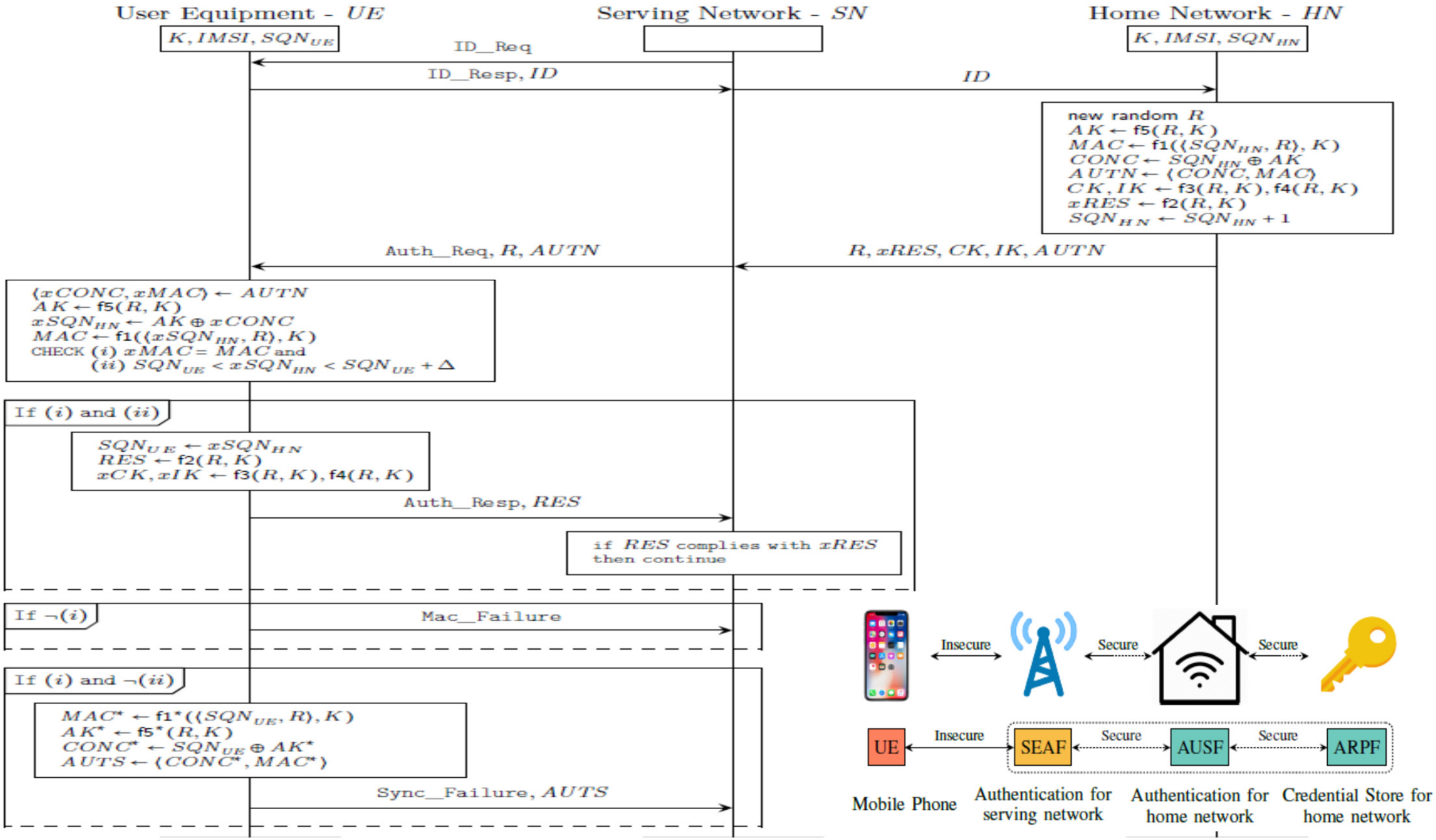
4G AKA protocol



5G AKA protocol



5G AKA protocol

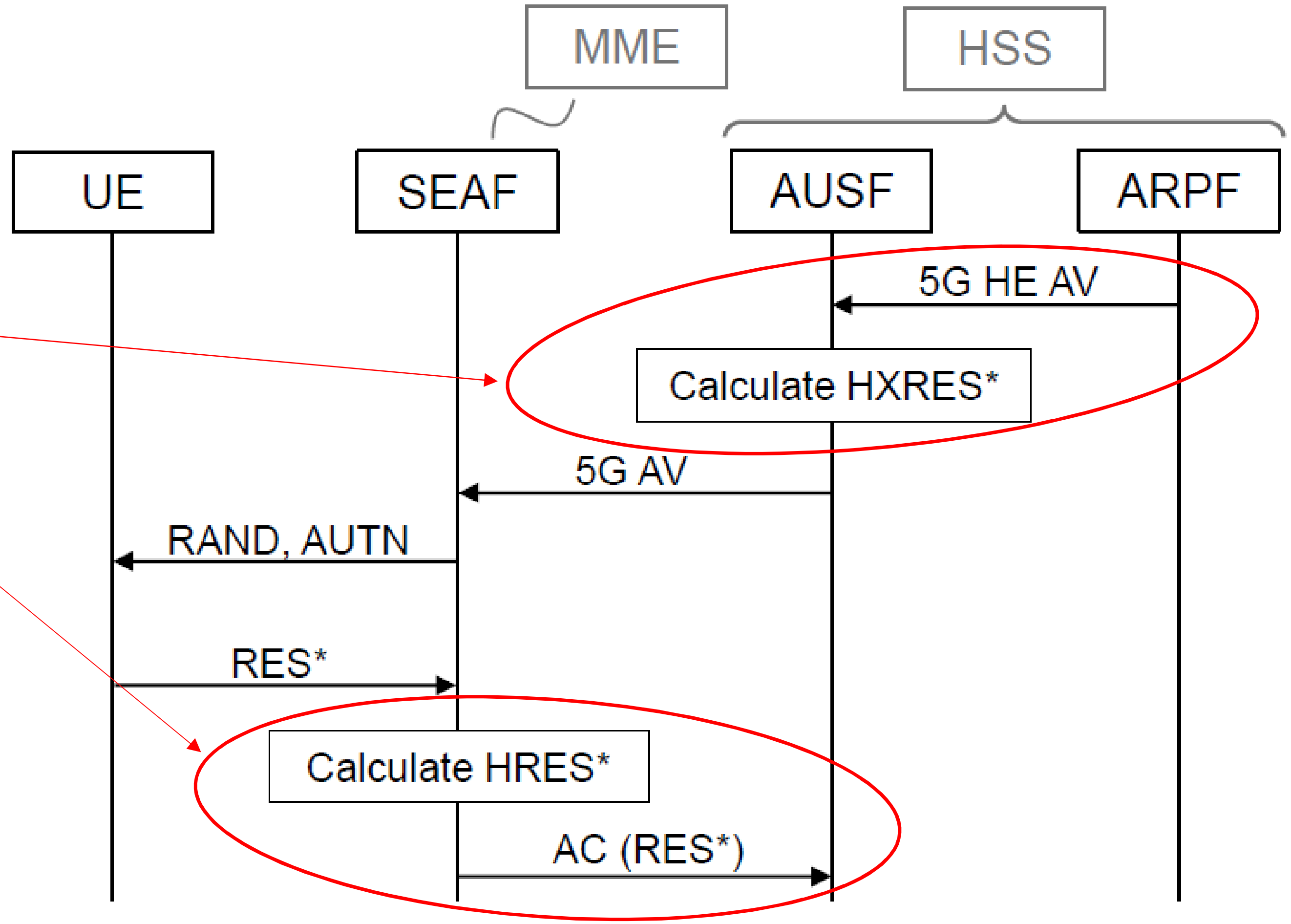


MAJOR CHANGES IN 5G –AUTHENTICATION HOME CONTROL IN 5G AKA

Based on EPS AKA
- New authentication confirmation
- New RES* and H(X)RES*

Calculation of RES*:
- KDF(CK, IK, SN name, RAND, RES)
- Calculated in ARPF and UE

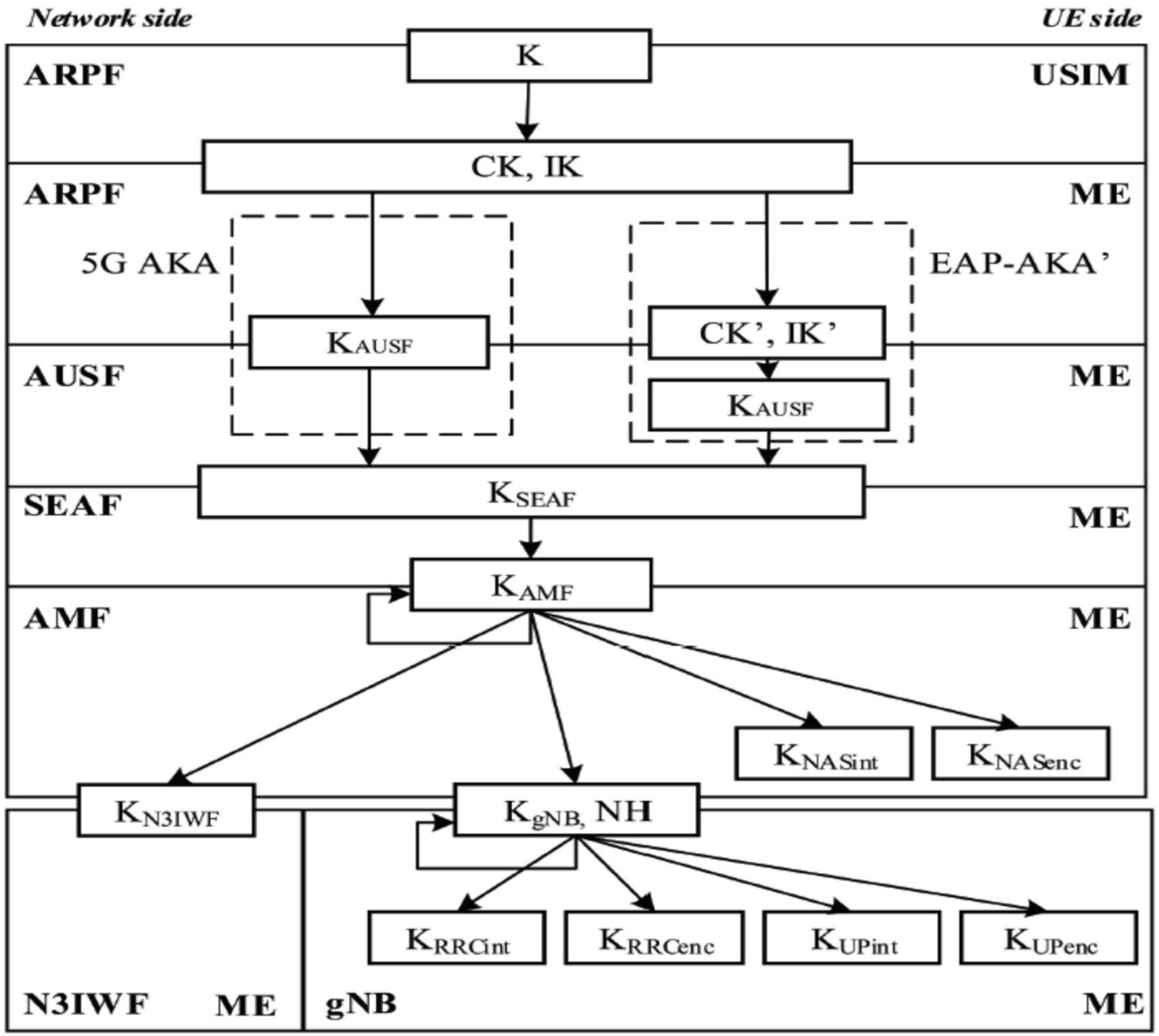
Calculation of HRES*:
- HASH(RAND, RES*)
- Calculated in SEAF and AUSF
- Used for authentication by the SEAF



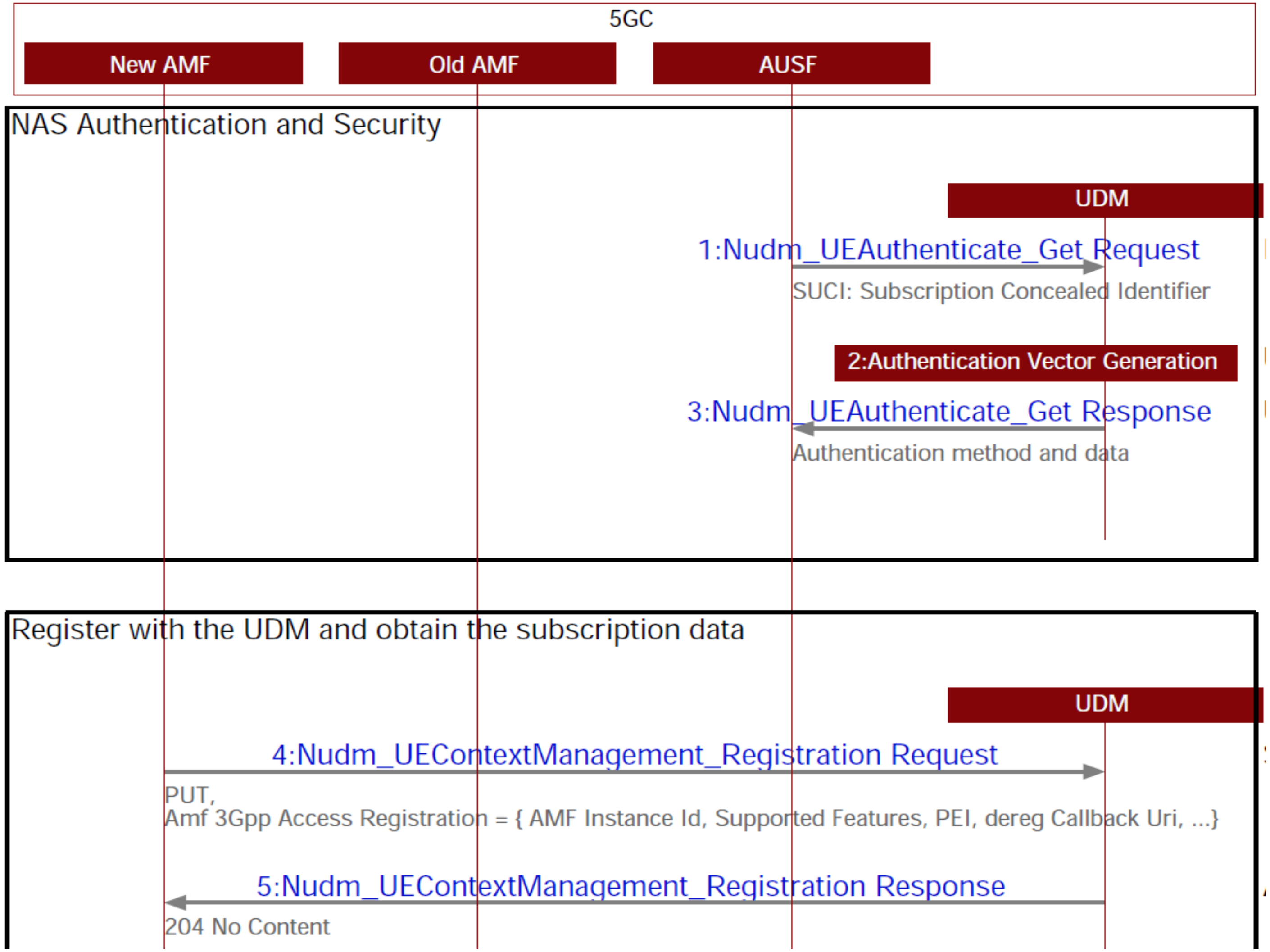
Key Hierarchy

Authentication Credential Repository and Processing Function

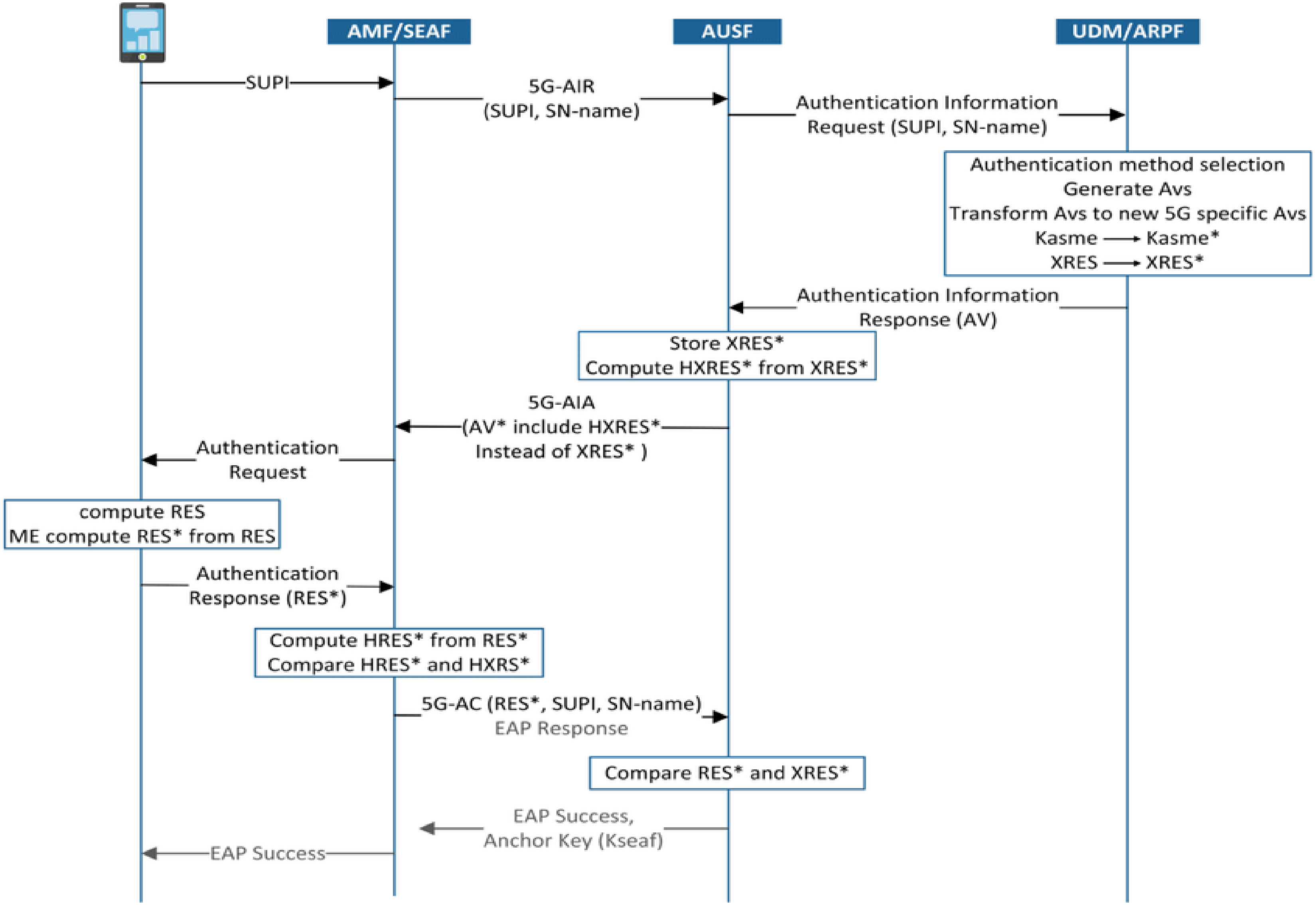
Security Anchor Function



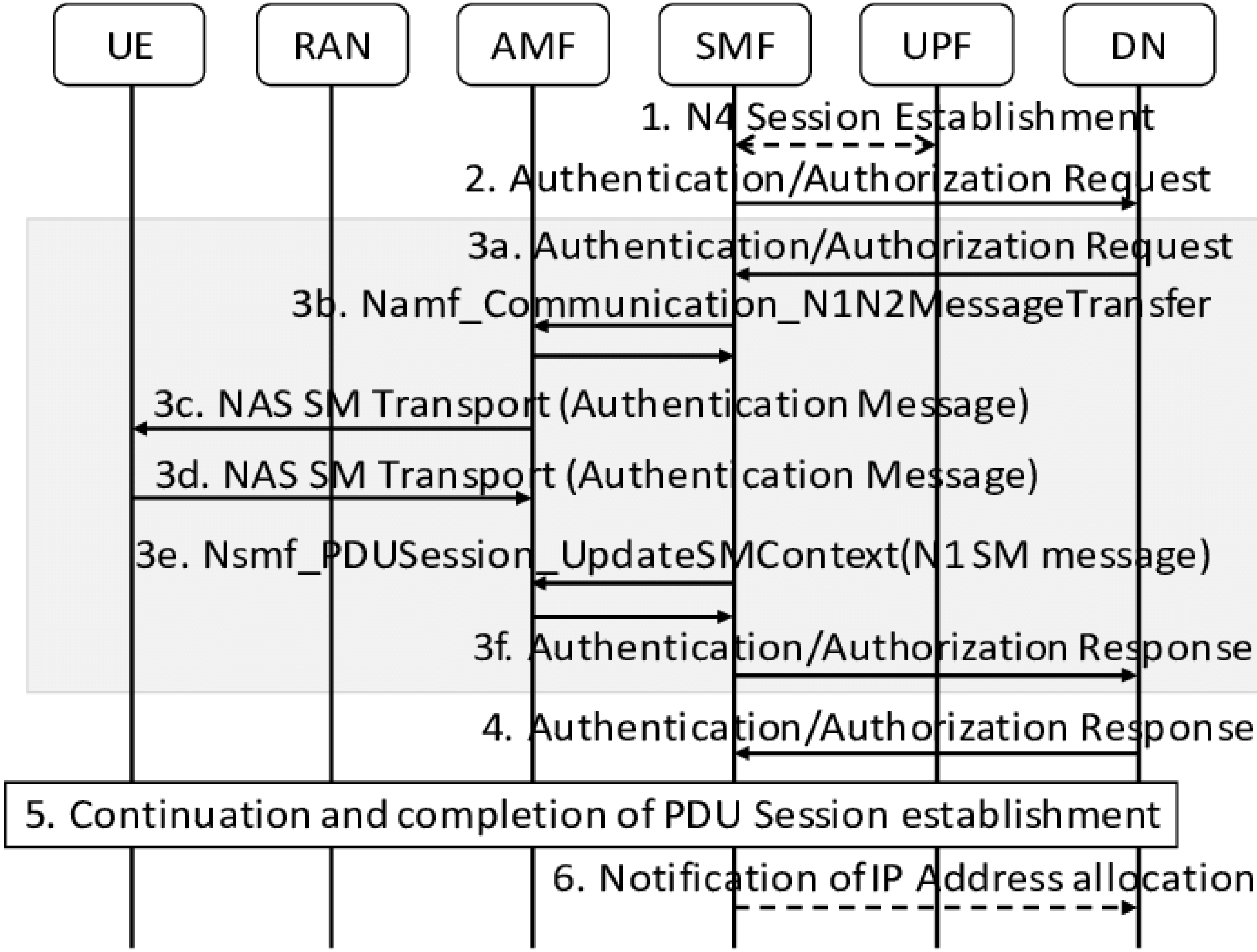
Authentication and registration



Authentication

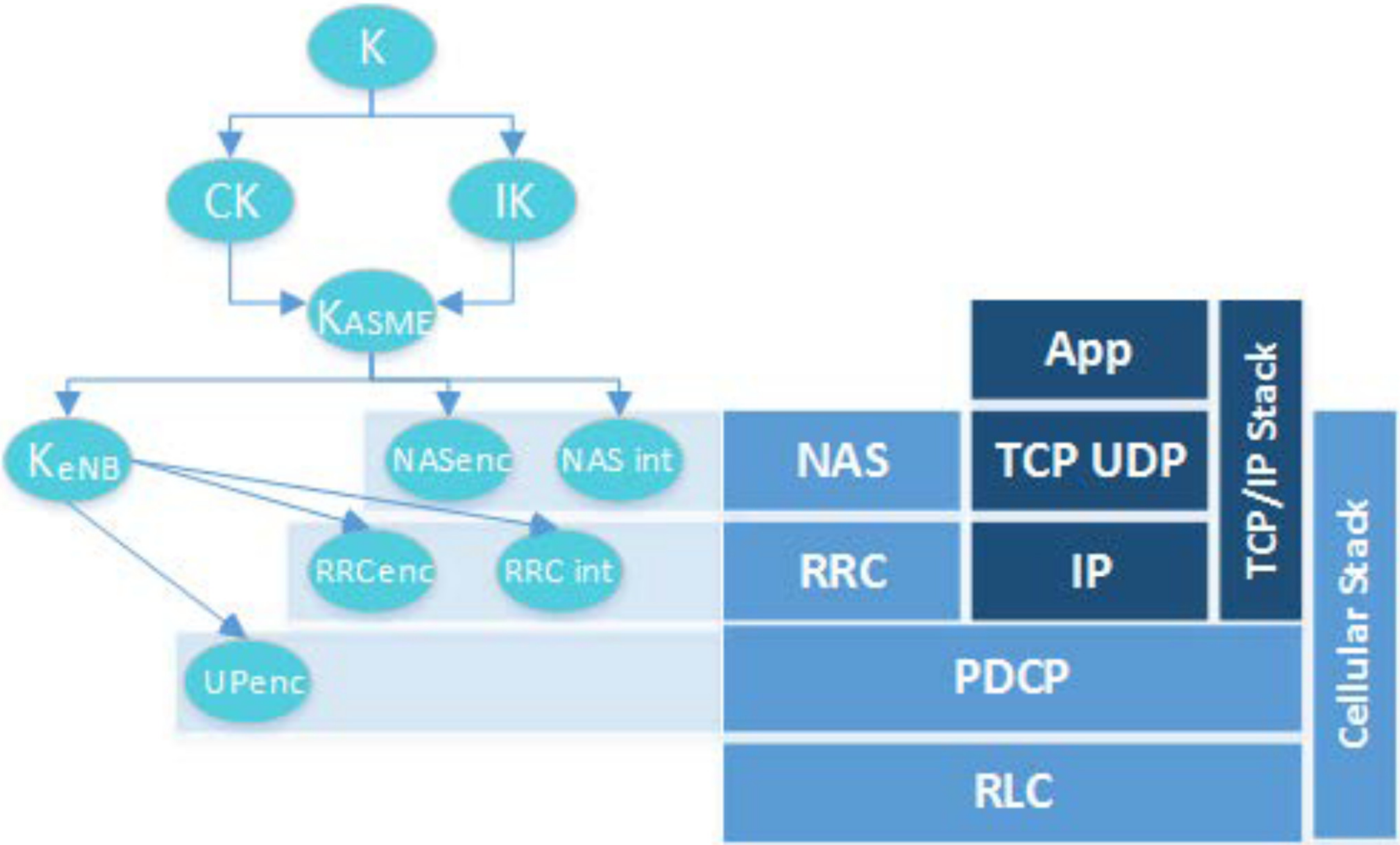


Secondary Authentication Call Flow



Data and Signaling protection

Key distribution



5G key hierarchy

Key hierarchy **extended**:

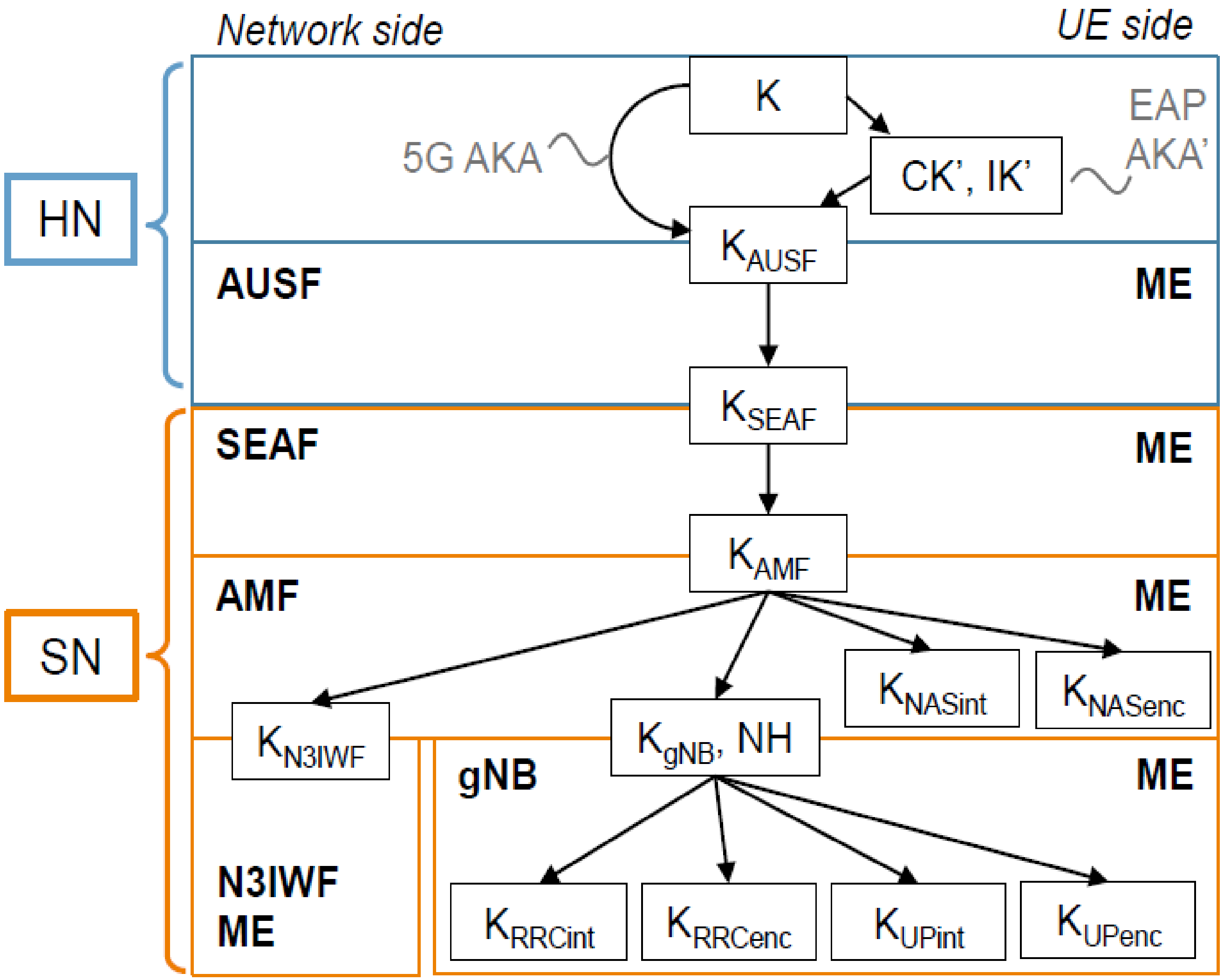
- K_{AUSF} at home network
- K_{SEAF} at visited network

Reasons for $\mathbf{K_{AUSF}}$

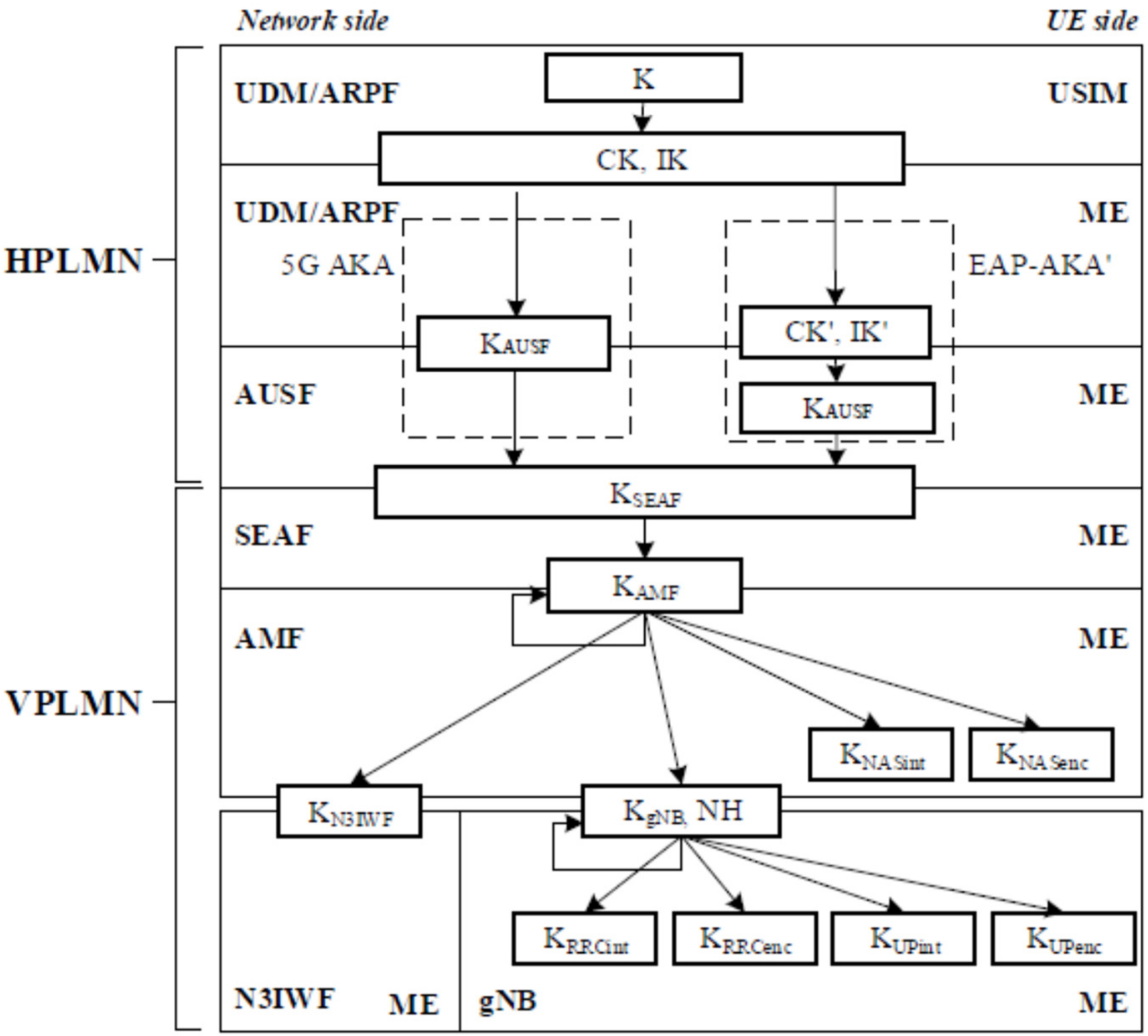
- Quick reauthentication
- Protecting home to UE traffic, e.g. steering of roaming under discussion

Reasons for $\mathbf{K_{SEAF}}$

- Separate security anchor from mobility anchor
- Pre-empts AMF at insecure locations



5G key hierarchy when roaming



Integrity

Integrity protection

Split of gNB into Central and Distributed Unit (CU/DU)

- CU performs security functions (confidentiality/integrity)
- Can be located closer to the core

Visibility

- Requirement to enable applications to check security being applied to the connection

Slice security

Network Slice Isolation

- Virtual machine isolation
- Physical network function isolation
- Virtual network function isolation

Tenant Isolation

- Identification, authentication, authorization and delegation (Tokenization technique)
- Network resources provisioning platform isolation (e.g., multi-factor authentication and tokenization)
- Tenant data isolation (many-to-one synchronization)

Virtual Network Infrastructure Visibility

- Virtual machine introspection to reduce the semantic gap
- Proactive Tenant's Network Slice Service Chain Behaviour Detection

Network Slice Communication Confidentiality and Integrity

- Intra- and Inter-Network Slice Communications Model

Trust Model

- Stakeholder trust model and network entities trust

Conclusions

Main security enhancements with 5G

- Security anchor in the **SEAF** co-located with the AMF. The SEAF creates the ***primary authentication*** a unified anchor key $\mathbf{K_{SEAF}}$ (common for all accesses)
- Access agnostic **primary authentication** with home control
- Protection **SUPI** (*Subscriber Permanent Identifier* 5G IMSI-equivalent) of the air with a public key encryption
- **Security key** establishment and management
- **Security for mobility**
- **Service based** architecture security
- Inter-network security, privacy and security for services provided over 5G with **secondary authentication** (for ex. between an enterprise and the UE to authenticate access to a corporate APN)

Thank You