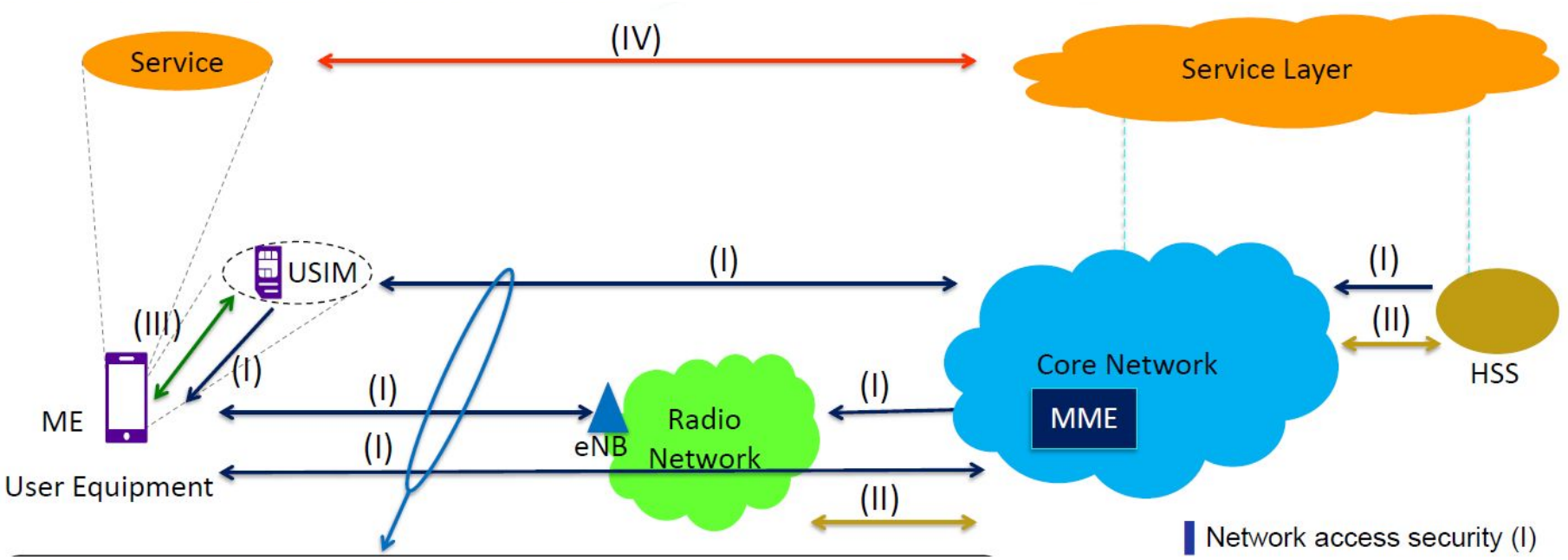
Конструктивно-технологичские особенности средств связи

Безопасность в сетях LTE

Лекция 6

Лектор: Ярлыкова С.М.

Безопасность сети LTE



- I - Безопасность сети доступа
- II - Безопасность сетевого домена
- III – Безопасность пользовательского домена
- IV- Безопасность домена приложений
- V – Управление и конфигурирование безопасности

Принципы безопасности в сетях LTE

- Взаимная аутентификация а сети
- Шифрование сообщений в радиока апе
- Защита целостности передаваем сообщений
- Защита аутентификационных данных а

AKA – процедура аутентификации и соглашения о ключах и выработка ключа K_{asme}

Протокол безопасности ESP инкапсулирующий IPsec

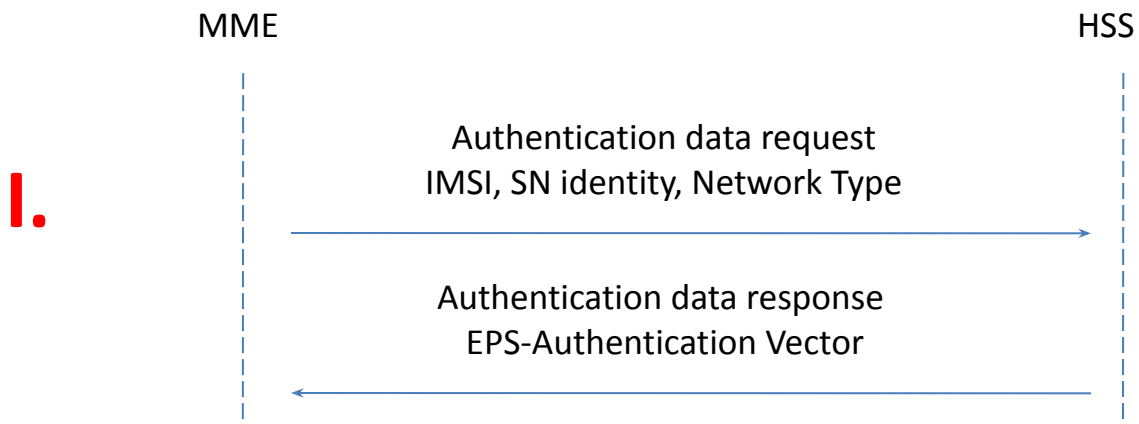
M-TMSI, S-RNTI, C-RNTI

Особенности

- иерархическая ключевая инфраструктура, в рамках которой для решения различных задач используются различные ключи;
- разделение механизмов безопасности для слоя без доступа (NAS), на котором осуществляется поддержка связи между узлом ядра сети и мобильным терминалом (UE), и механизмов безопасности для слоя с доступом (AS), обеспечивающего взаимодействие между оконечным сетевым оборудованием (включая набор базовых станций NodeB(eNB)) и мобильными терминалами;
- концепция превентивной безопасности, которая способна снизить масштабы урона, наносимого при компрометации ключей;
- добавление механизмов безопасности для обмена данными между сетями 3G и LTE.

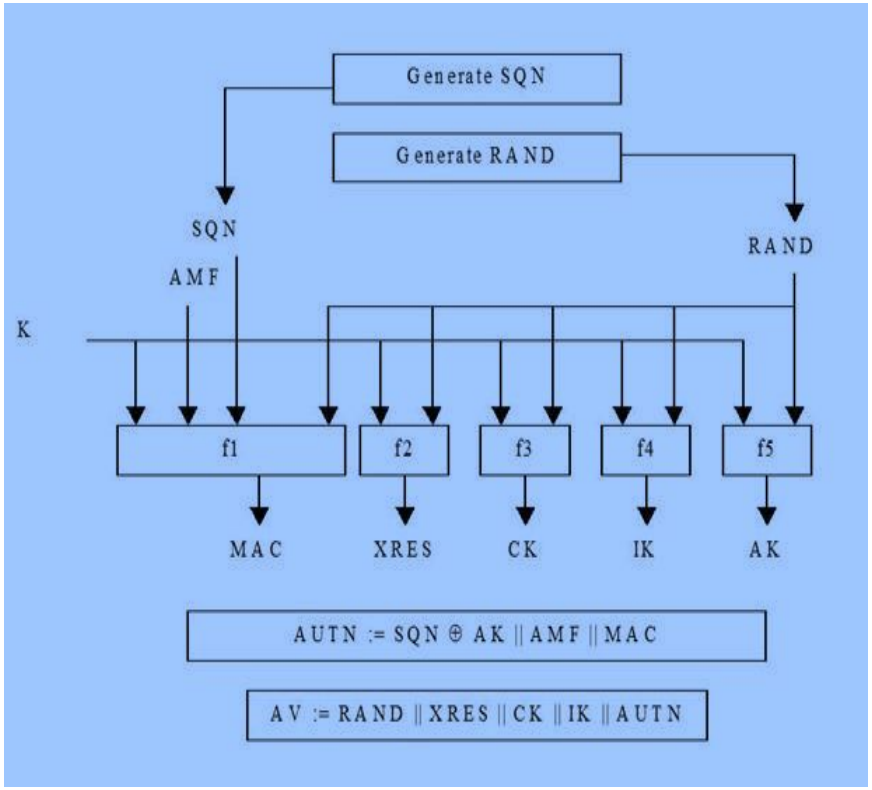
Алгоритм АКА

- I. Запрос на аутентификацию.
- II. а) генерация вектора аутентификации; б)генерация ключа K_{ASME} .
- III. Завершение процедуры аутентификации.

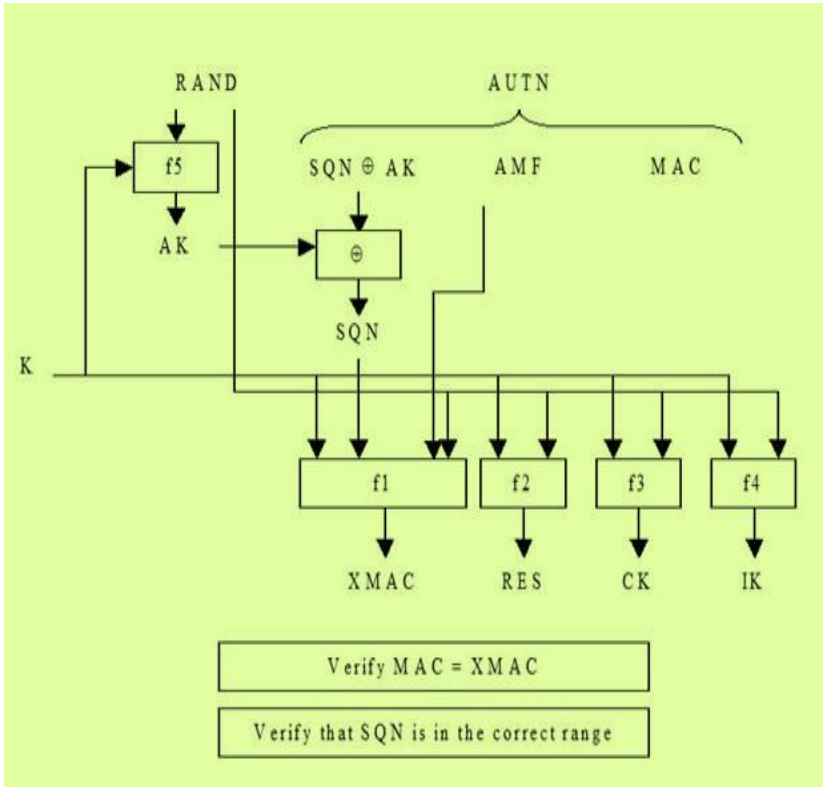


II. a) Алгоритм создания вектора аутентификации

На стороне сети (HSS)



На абонентском устройстве (USIM)



Параметры различных элементов

- ключ K – 128 бит;
- случайное число RAND – 128 бит;
- номер последовательности SQN – 48 бит;
- анонимный ключ AK (anonymity key) – 48 бит;
- поле управления аутентификацией AMF (authentication management field) – 16 бит;
- код сообщения аутентификации MAC (message authentication code) – 64 бит;
- ключ шифрования CK (cipher key) – 128 бит;
- ключ контроля целостности IK (integrity key) – 128 бит;
- маркер аутентификации AUTN (authentication token – 128 бит;
- ключ управления защитой доступа KASME (access security management entity) – 256 бит;
- отклик аутентификации RES (authentication response) – 416 октетов.

II. б) Второй этап генерации вектора аутентификации

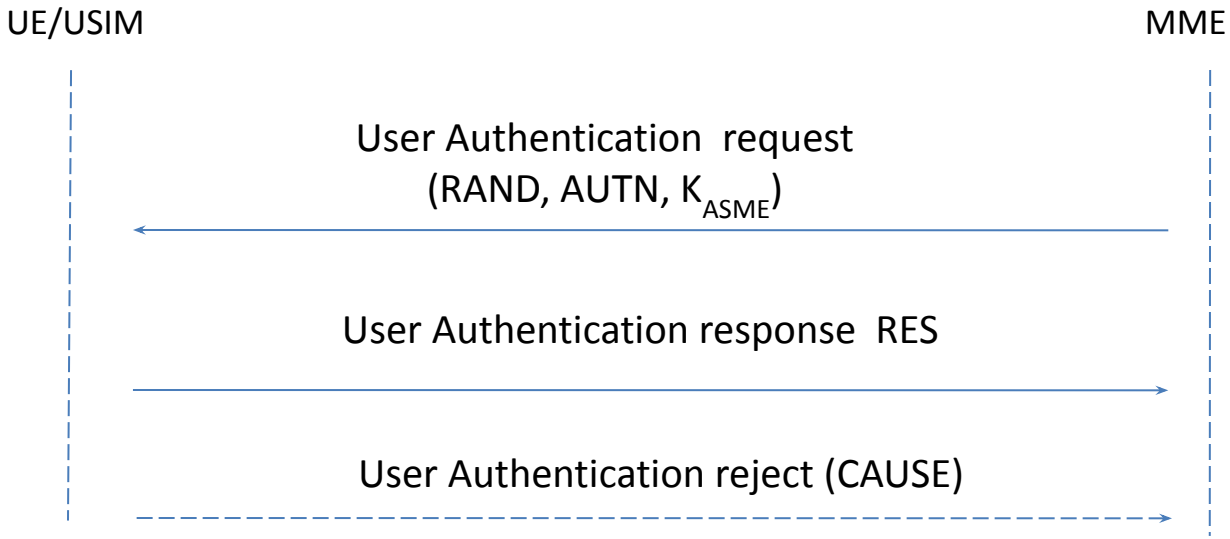
AMF = 0, то это сеть GERAN/UMTS

- Вектор аутентификации состоит из чисел RAND, XRES, ключей CK, IK и числа AUTN представляющего собой запись в строку трех параметров: SQN Å AK, AMF и MAC.

AMF = 0, то это сеть E-UTRAN

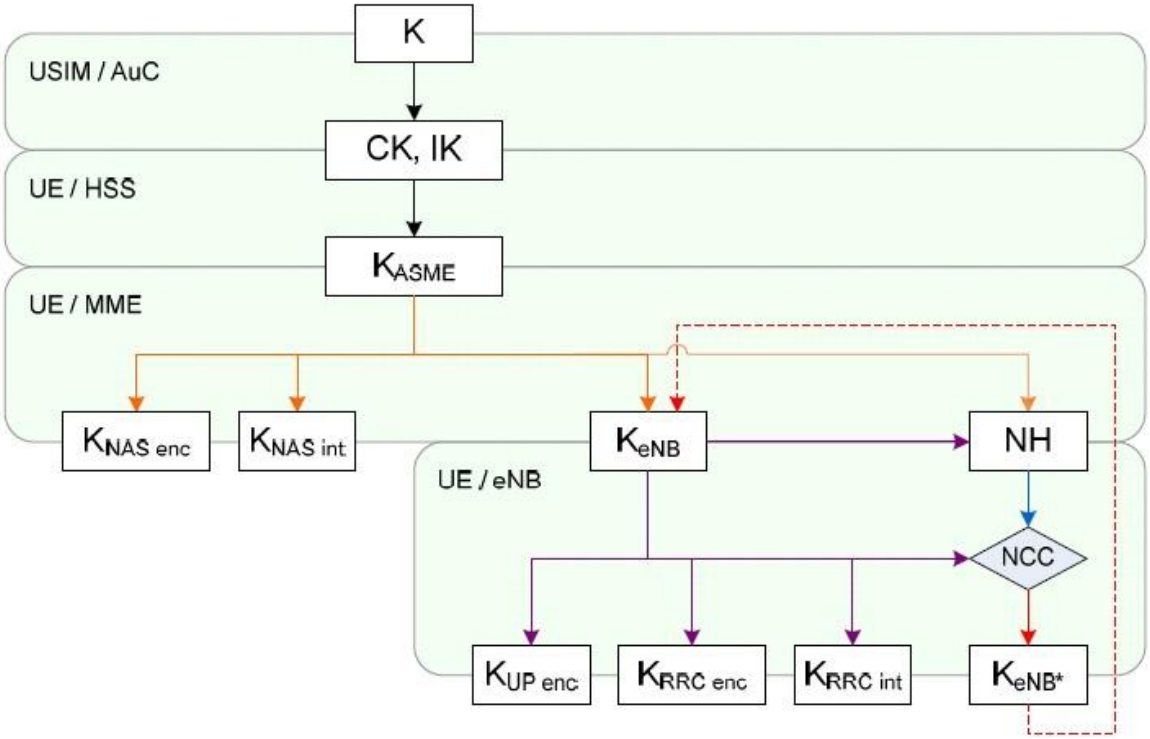
- Ключи CK и IK в открытом виде в ядро сети не передают.
- HSS генерирует K_{ASME} с помощью алгоритма KDF (Key Derivation Function), для которого исходными параметрами являются CK и IK, а также идентификатор обслуживающей сети и SQN ÅAK.
- Вектор аутентификации содержит RAND, XRES, AUTN и K_{ASME}, на основе которого происходит генерация ключей шифрации и целостности.

III. Завершение процедуры аутентификации



K_{ASME} - Key Access Security Management Entries

Генерация ключа K_{ASME}



Ключи для защиты NAS сигнального трафика:

- K_{NASint} – ключ, используемый для контроля целостности NAS сигнального трафика; вычисляется абонентским терминалом (UE) и MME из K_{ASME}.
- K_{NASenc} – ключ, используемый для шифрования NAS сигнального трафика; вычисляется абонентским терминалом (UE) и MME из K_{ASME}.

Ключи для защиты RRC сигнального трафика:

- K_{RRCint} – ключ, используемый для контроля целостности RRC сигнального трафика; вычисляется абонентским терминалом (UE) и базовой станцией (eNodeB) из K_{eNB}.
- K_{RRCenc} – ключ, используемый для шифрования RRC сигнального трафика; вычисляется абонентским терминалом (UE) и базовой станцией (eNodeB) из K_{eNB}.

Ключи для защиты пользовательского трафика

- K_{UPint} – ключ, используемый для контроля целостности пользовательского трафика; вычисляется абонентским терминалом (UE) и базовой станцией (eNodeB) из K_{eNB}.
- K_{UPenc} – ключ, используемый для шифрования пользовательского трафика; вычисляется абонентским терминалом (UE) и базовой станцией (eNodeB) из K_{eNB}.

Распределение ключей и параметров по разным узлам LTE

	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		

Процедура аутентифкации

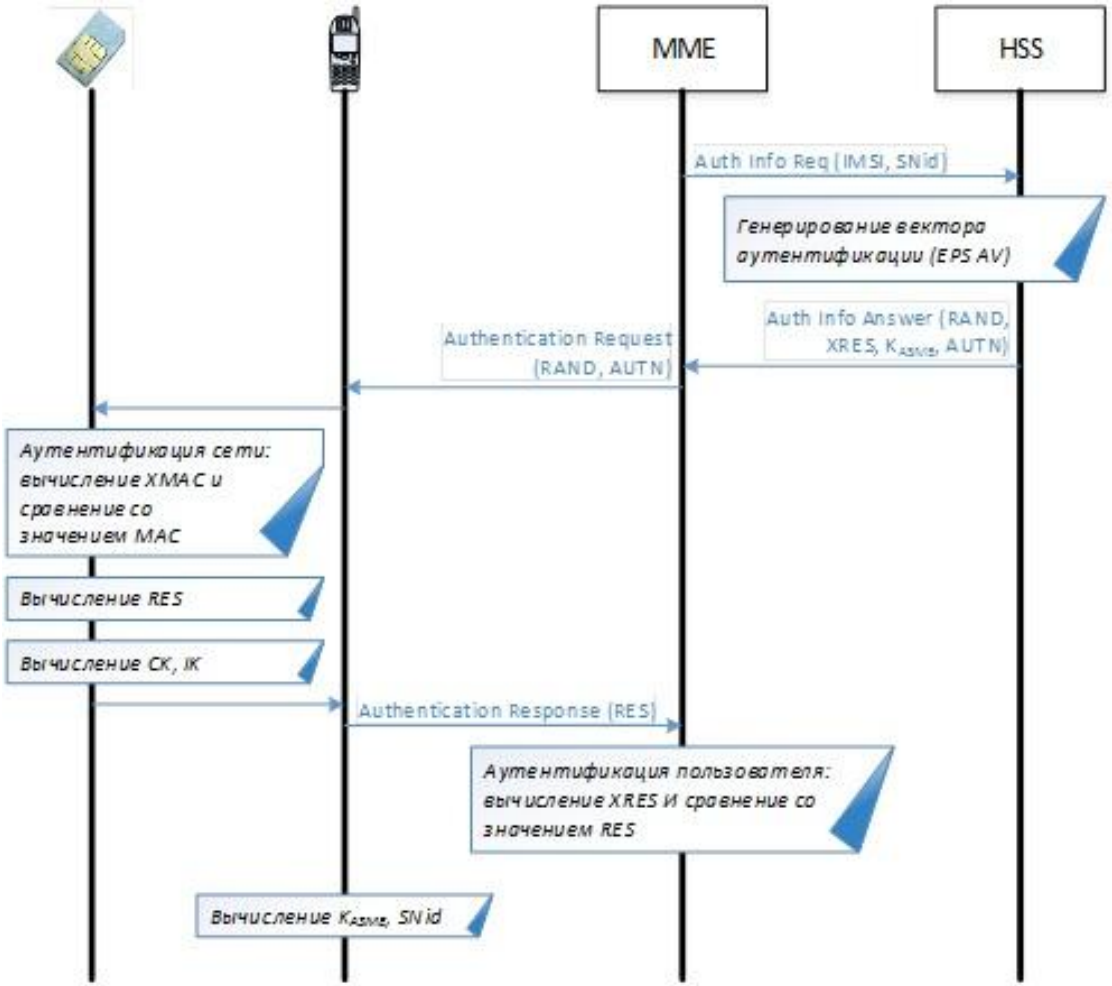
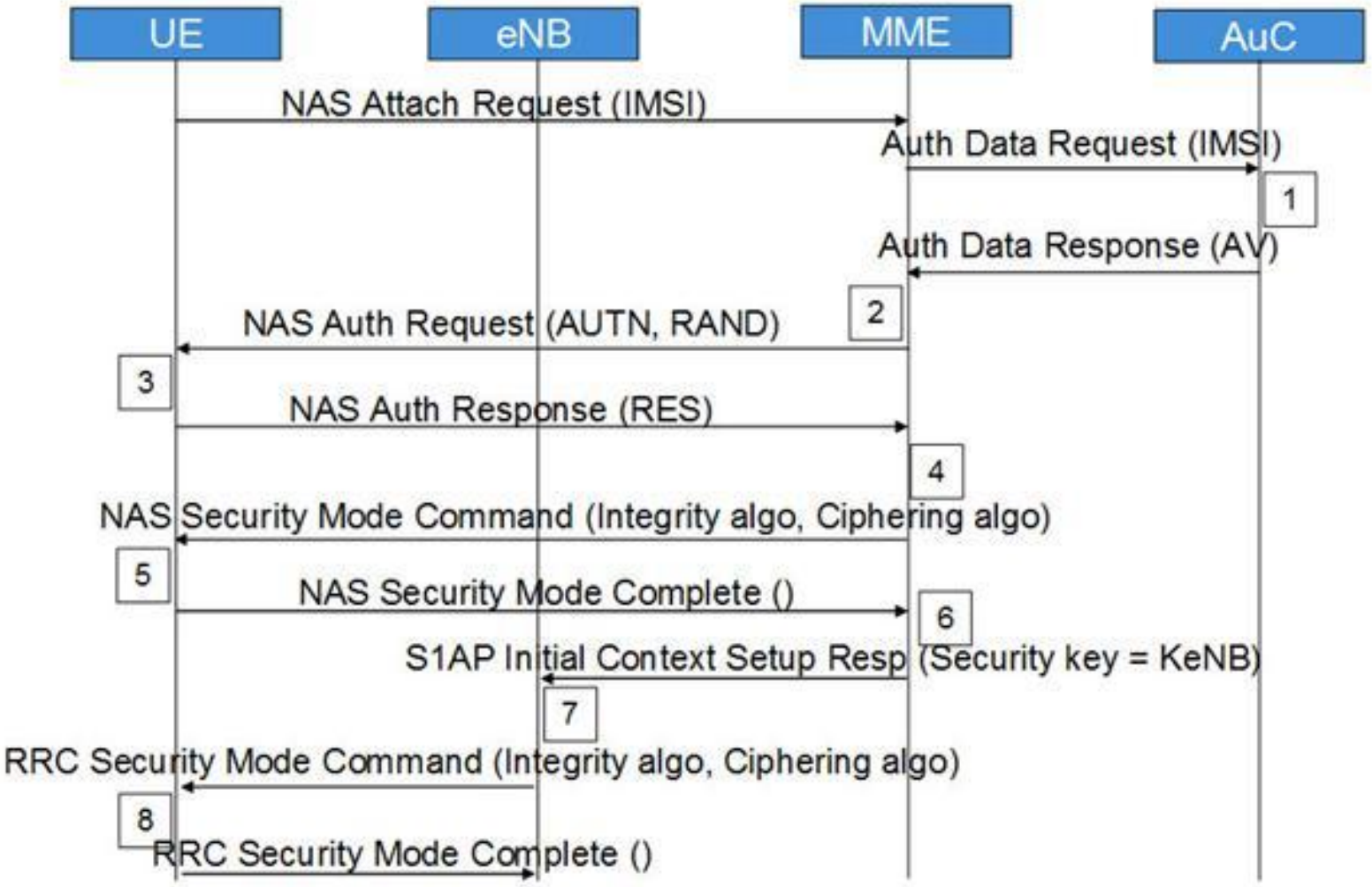
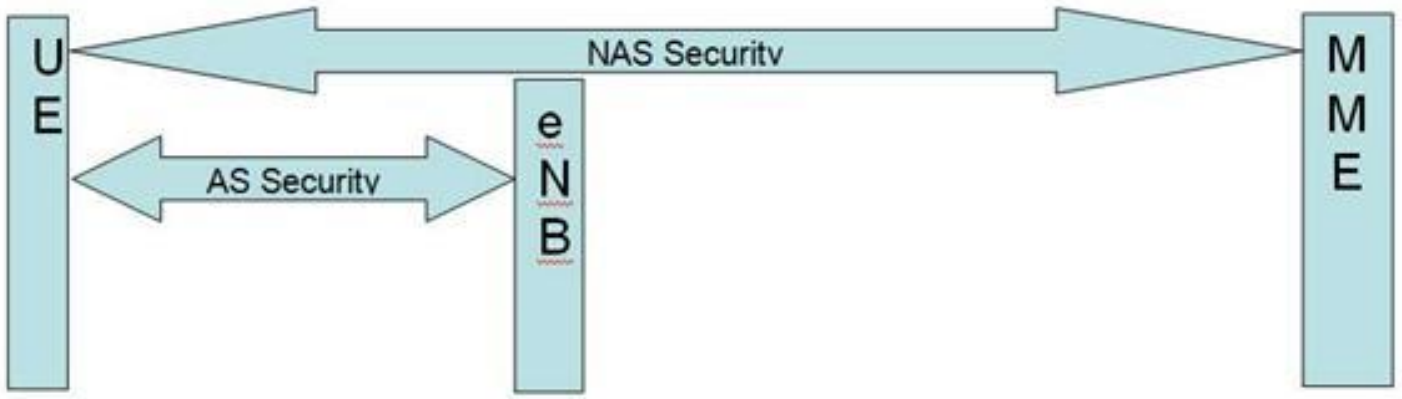


Диаграмма аутентификации и генерации ключа

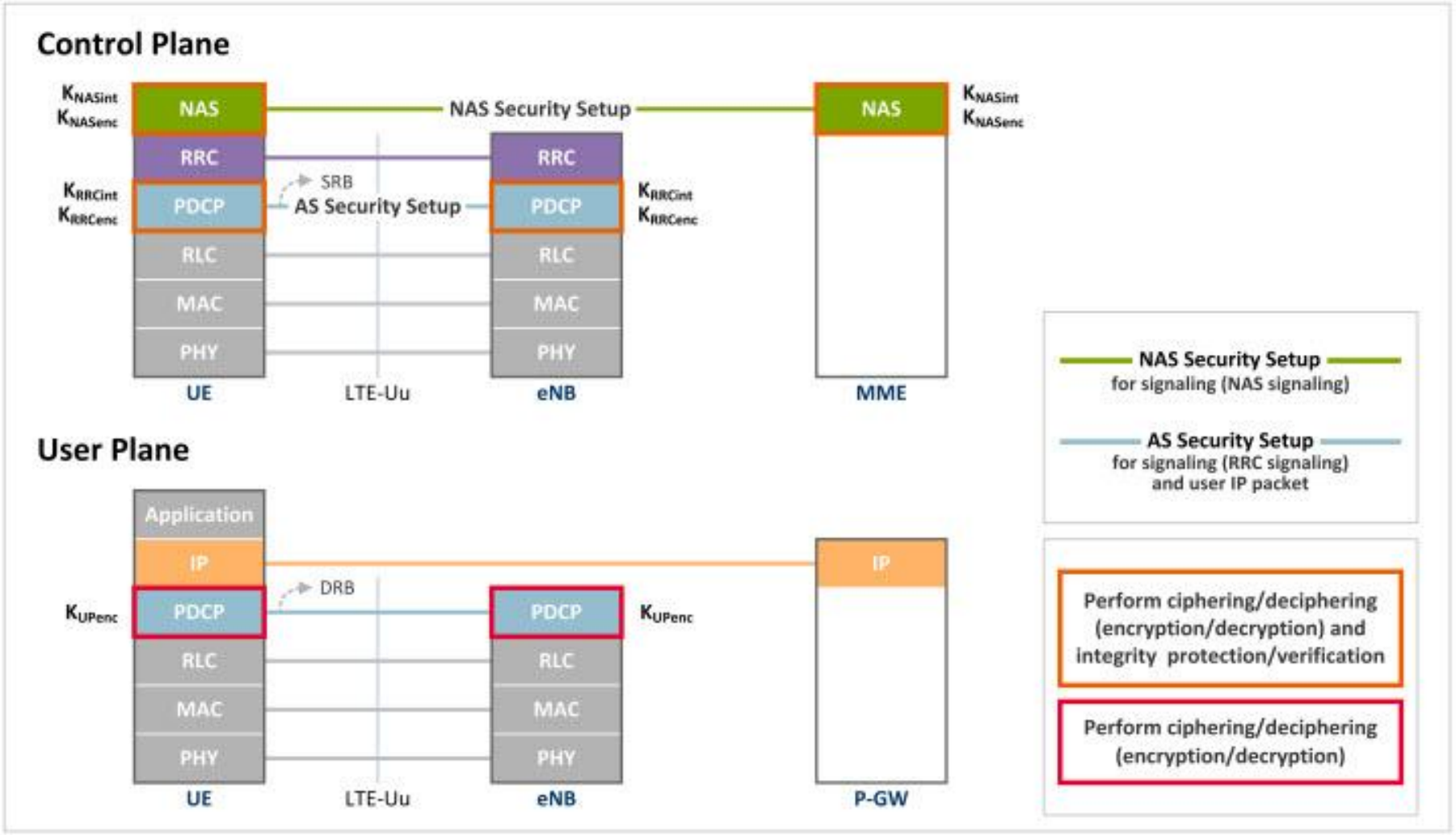


Слои безопасности

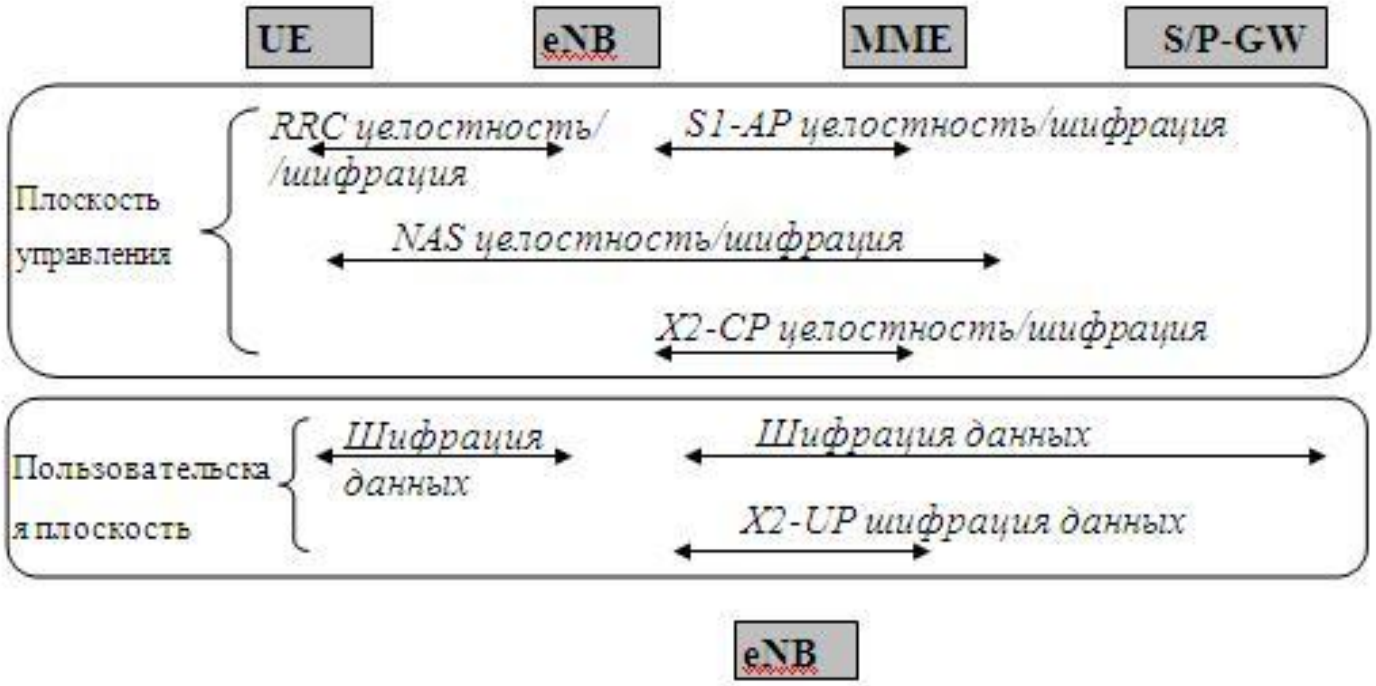


- **Безопасность NAS (Non-Access Stratum - слоя без доступа)**:
- Выполнена для NAS сообщений и принадлежит области UE и MME.
- (Non Access Stratum включает в себя протоколы обеспечивающие управление вызовом, управление мобильностью и прочие.)

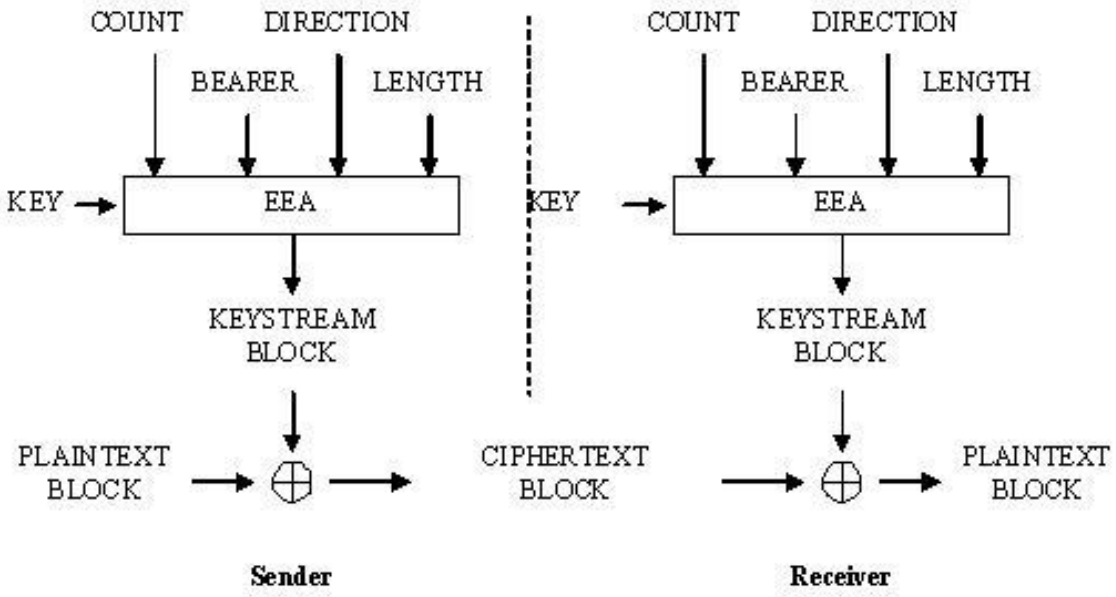
- **Безопасность AS (Access Stratum - слоя с доступом):**
- Выполнена для RRC и плоскости пользовательских данных, принадлежащих области UE и eNB.
- (Access Stratum объединяет в себе протоколы радио доступа. Включает в себя протоколы обеспечивающие совместное использование радио ресурсов оборудования пользователя UE и сети доступа. AS обеспечивает взаимодействие между UE и CN, так называемых Radio Access Bearer (RAB) соединений.)


Control Plane
K_{NASint}
K_{NASenc}
NAS
NAS Security Setup
NAS
K_{NASint}
K_{NASenc}
RRC
RRC
K_{RRCint}
K_{RRCenc}
PDCP
SRB
AS Security Setup
PDCP
K_{RRCint}
K_{RRCenc}
RLC
RLC
MAC
MAC
PHY
PHY
UE
LTE-Uu
eNB
MME
User Plane
Application
IP
IP
K_{UPenc}
PDCP
DRB
PDCP
K_{UPenc}
RLC
RLC
MAC
MAC
PHY
PHY
UE
LTE-Uu
eNB
P-GW
NAS Security Setup
for signaling (NAS signaling)
AS Security Setup
for signaling (RRC signaling)
and user IP packet
Perform ciphering/deciphering (encryption/decryption) and integrity protection/verification
Perform ciphering/deciphering (encryption/decryption)

Процедуры безопасности



Алгоритм шифрования сообщений



Исходные параметры в алгоритме :

- шифрующий ключ KEY (128 бит),
- счетчик пакетов (блоков) COUNT (32 бита),
- идентификатор сквозного канала BEARER (5 бит),
- указатель направления передачи DIRECTION (1 бит)
- длина шифрующего ключа LENGTH.

В соответствии с выбранным алгоритмом шифрации EEA (EPS Encryption Algorithm) вырабатывается шифрующее число KEYSTREAM BLOCK, которое при передаче складывают по модулю два с шифруемым исходным текстом блока PLAINTEXT BLOCK. При дешифрации на приемном конце повторно совершают эту же операцию.

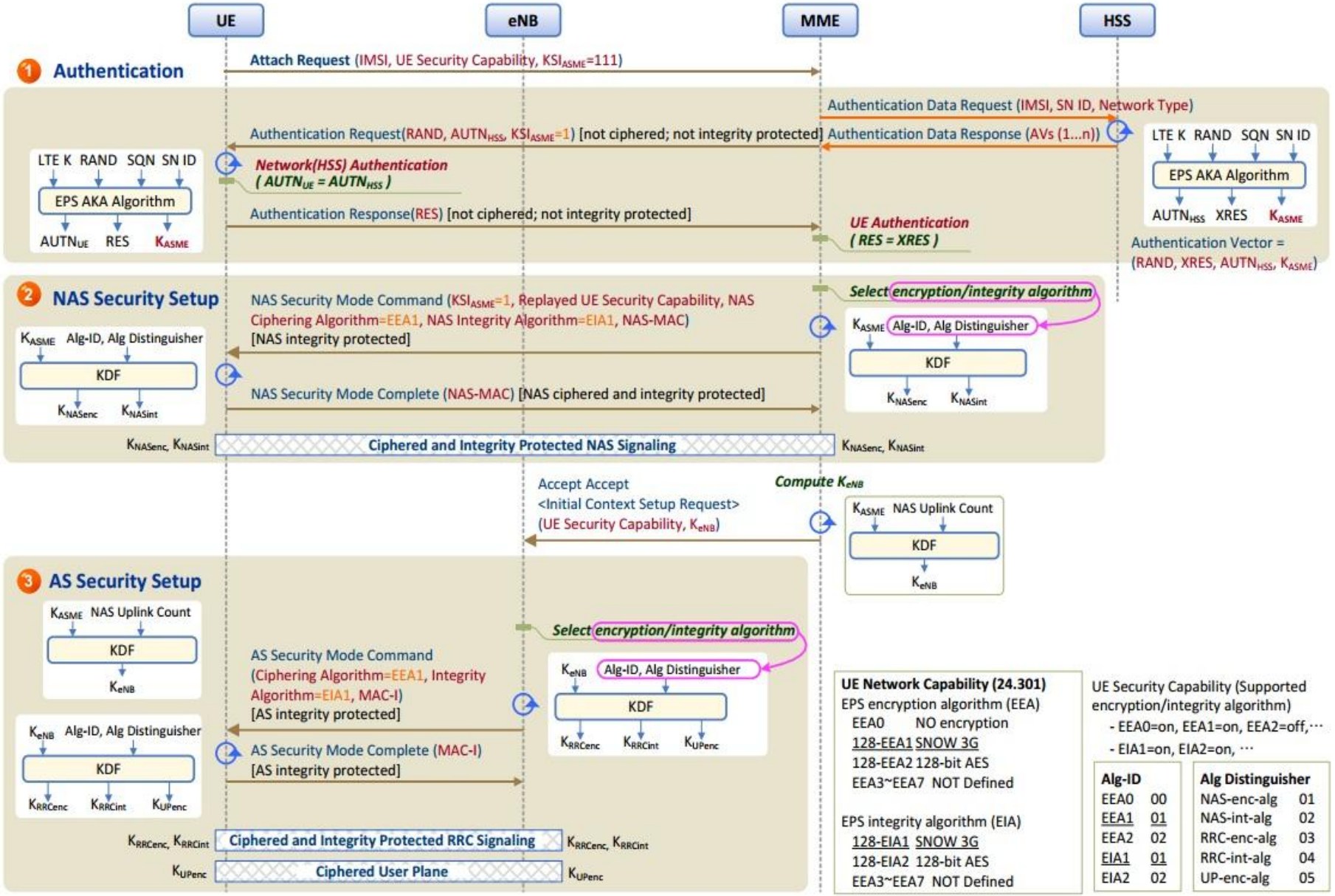
Типы алгоритмов и размеры ключей в сетях LTE

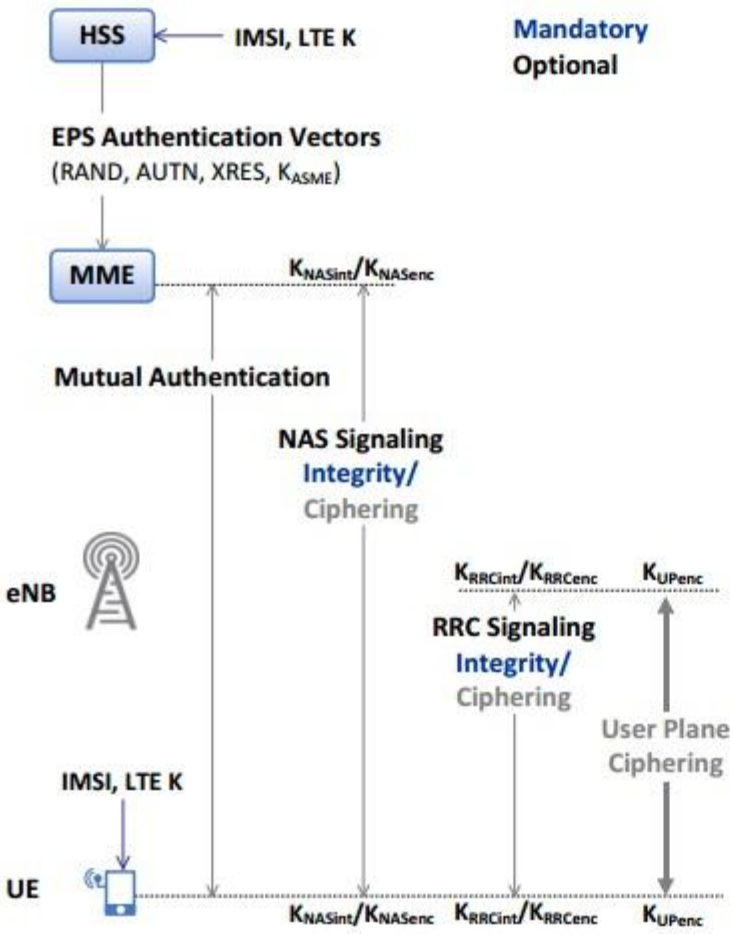
В качестве алгоритмов шифрования используются следующие:

- **128-EEA1** основанный на алгоритме Snow 3G. В точности повторяет алгоритм UEA2, специфицированный для сетей UMTS
- **128-EEA2** основанный на алгоритме AES

Для проверки целостности данных, спецификации предлагают следующие алгоритмы:

- **128-EIA1** основанный на алгоритме Snow 3G. В точности повторяет алгоритм UIA2, специфицированный для сетей UMTS
- **128-EIA2** основанный на алгоритме AES


UE
eNB
MME
HSS
1 Authentication
Attach Request (IMSI, UE Security Capability, KSI$_{ASME}$=111)
Authentication Data Request (IMSI, SN ID, Network Type)
Authentication Request(RAND, AUTN$_{HSS}$, KSI$_{ASME}$=1) [not ciphered; not integrity protected]
Authentication Data Response (AVs (1...n))
LTE K RAND SQN SN ID
EPS AKA Algorithm
AUTN$_{UE}$ RES K$_{ASME}$
Network(HSS) Authentication
(AUTN$_{UE}$ = AUTN$_{HSS}$)
Authentication Response(RES) [not ciphered; not integrity protected]
UE Authentication
(RES = XRES)
AUTN$_{HSS}$ XRES K$_{ASME}$
Authentication Vector =
(RAND, XRES, AUTN$_{HSS}$, K$_{ASME}$)
2 NAS Security Setup
K$_{ASME}$ Alg-ID, Alg Distinguisher
KDF
K$_{NASenc}$ K$_{NASint}$
NAS Security Mode Command (KSI$_{ASME}$=1, Replayed UE Security Capability, NAS Ciphering Algorithm=EEA1, NAS Integrity Algorithm=EIA1, NAS-MAC)
[NAS integrity protected]
Select encryption/integrity algorithm
NAS Security Mode Complete (NAS-MAC) [NAS ciphered and integrity protected]
K$_{NASenc}$, K$_{NASint}$
Ciphered and Integrity Protected NAS Signaling
Accept Accept
<Initial Context Setup Request>
(UE Security Capability, K$_{eNB}$)
Compute K$_{eNB}$
K$_{ASME}$ NAS Uplink Count
3 AS Security Setup
K$_{eNB}$ Alg-ID, Alg Distinguisher
K$_{RRCenc}$ K$_{RRCint}$ K$_{UPenc}$
AS Security Mode Command
(Ciphering Algorithm=EEA1, Integrity Algorithm=EIA1, MAC-I)
[AS integrity protected]
AS Security Mode Complete (MAC-I)
[AS integrity protected]
K$_{RRCenc}$, K$_{RRCint}$
Ciphered and Integrity Protected RRC Signaling
K$_{UPenc}$
Ciphered User Plane
UE Network Capability (24.301)
EPS encryption algorithm (EEA)
EEA0 NO encryption
128-EEA1 SNOW 3G
128-EEA2 128-bit AES
EEA3~EEA7 NOT Defined
EPS integrity algorithm (EIA)
128-EIA1 SNOW 3G
128-EIA2 128-bit AES
EEA3~EEA7 NOT Defined
UE Security Capability (Supported encryption/integrity algorithm)
- EEA0=on, EEA1=on, EEA2=off,…
- EIA1=on, EIA2=on, …
Alg-ID
EEA0 00
EEA1 01
EEA2 02
EIA1 01
EIA2 02
Alg Distinguisher
NAS-enc-alg 01
NAS-int-alg 02
RRC-enc-alg 03
RRC-int-alg 04
UP-enc-alg 05



EPS AKA provides authentication, confidentiality and integrity protection for LTE network

- Authentication method: EPS AKA
- Authentication parameters: IMSI, EPS AV (K_{ASME}, RAND, AUTN, XRES), RES
- NAS integrity protection (AES, Snow 3G)
- NAS ciphering (Null, AES, Snow 3G)
- RRC signaling integrity protection (AES and Snow 3G)
- RRC signaling ciphering (Null, AES, Snow 3G)
- User plane ciphering (Null, AES, Snow 3G)
- Key derivation function: HMAC-SHA-256
- Security master key: K_{ASME}
- Security key for NAS signaling: K_{NASenc}, K_{NASint}
- Security key for RRC signaling: K_{RRCenc}, K_{RRCint}
- Security key for user plane: K_{UPenc}

- References
  TS 24.301
  TS 33.401

- ПРИКАЗ от 25 июня 2018 года N 319. Об утверждении Правил применения оборудования коммутации сетей подвижной радиотелефонной связи.

ETSI TS 133 401 V10.3.0 (2012-07)

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
3GPP System Architecture Evolution (SAE);
Security architecture
(3GPP TS 33.401 version 10.3.0 Release 10)