

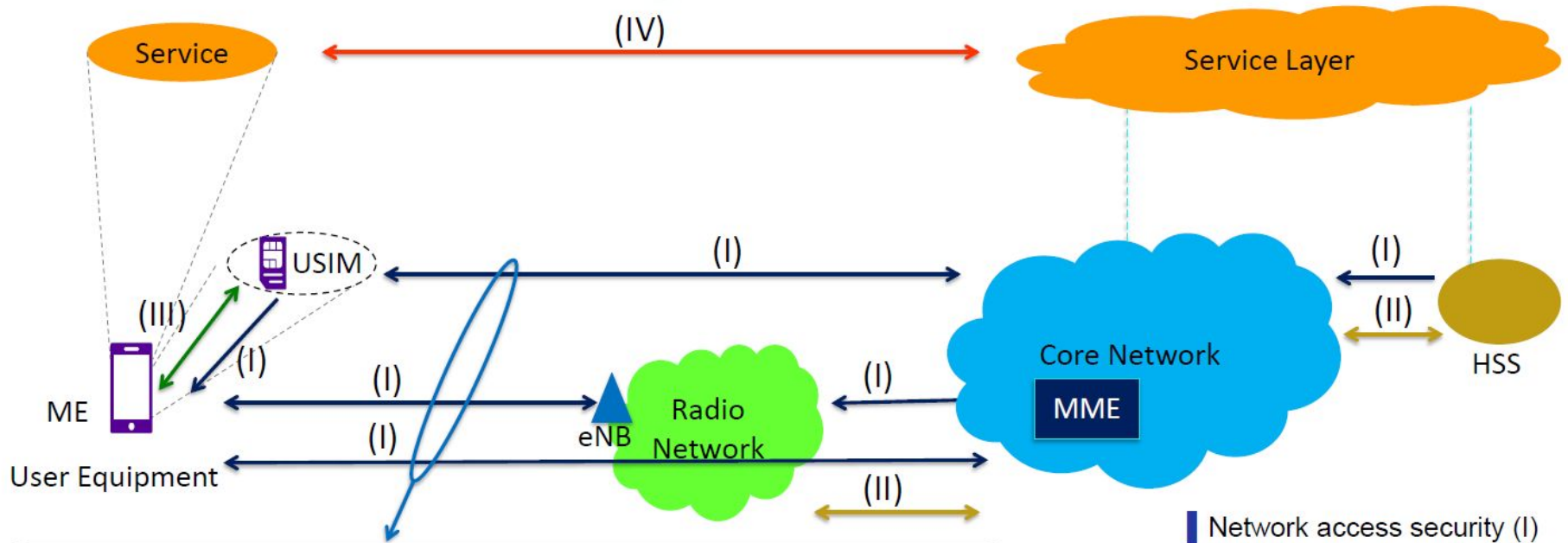
Конструктивно- технологические особенности средств связи

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

АКА – процедура аутентификации и соглашения о ключах и выработка ключа

K_{asme}

- Шифрование сообщений в радиоканале

- Защита целостности передаваемых сообщений

Протокол безопасности ESP инкапсулирующий IPsec

- Защита аутентификационных данных

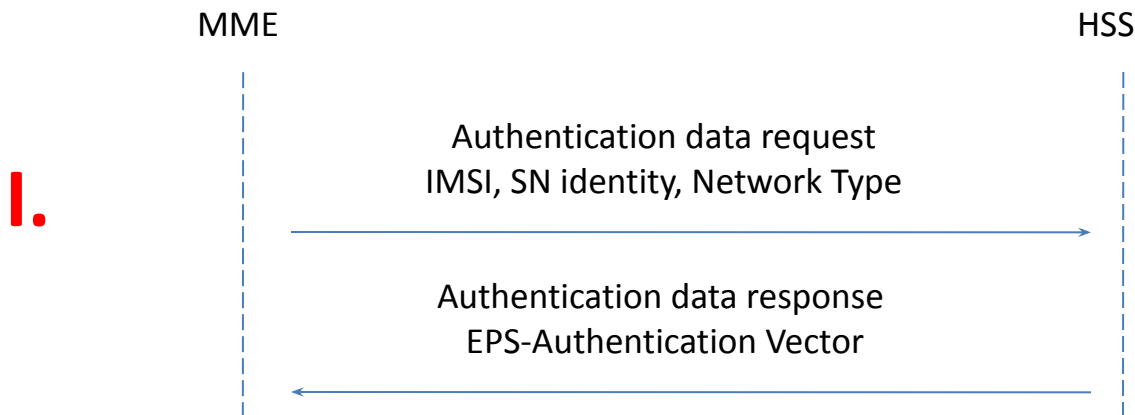
M-TMSI, S-RNTI, C-RNTI

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.

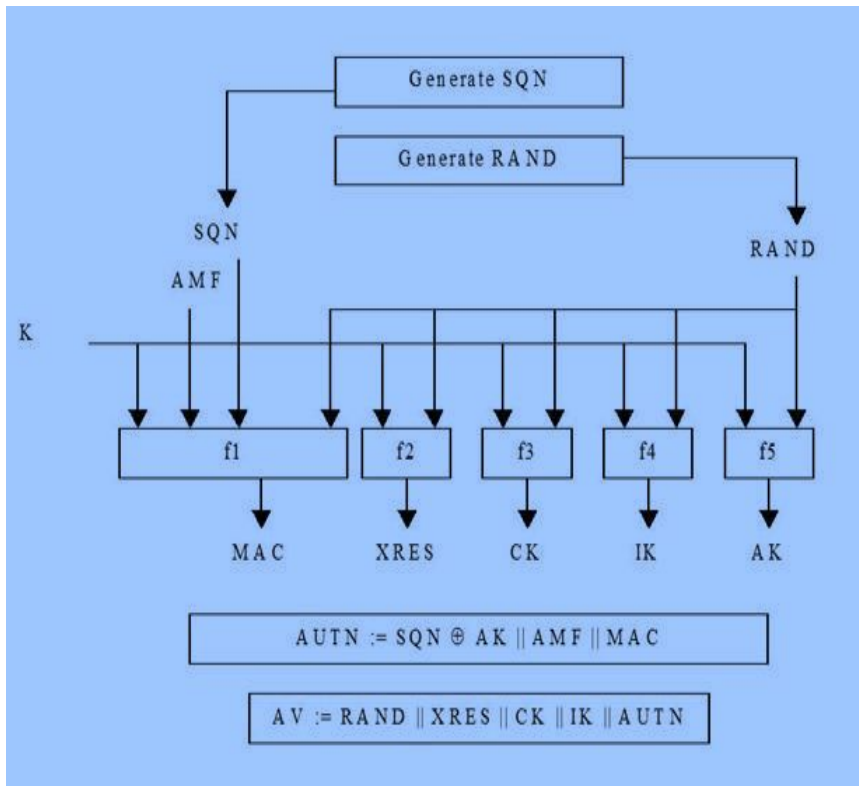
Алгоритм АКА

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

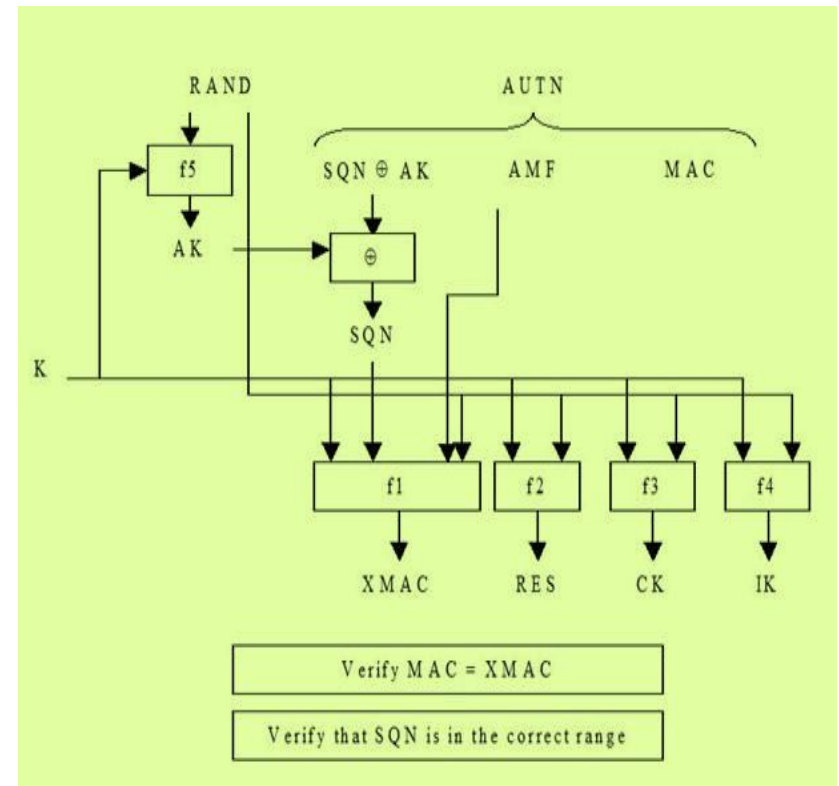


II. а) Алгоритм создания вектора аутентификации

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 АК (anonymity key) – 48 бит;
- поле управления аутентификацией AMF (authentication management field) – 16 бит;
- код сообщения аутентификации MAC (message authentication code) – 64 бит;
- ключ шифрования СК (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. 6) Второй этап генерации вектора аутентификации

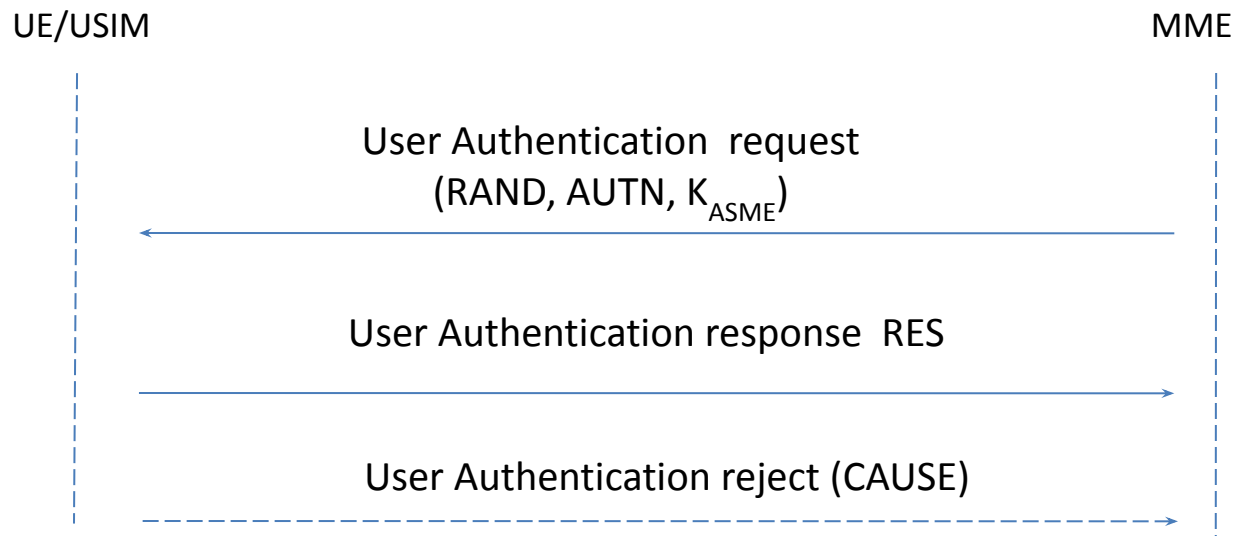
AMF = 0, то это сеть GERAN/UMTS

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

AMF = 0, то это сеть E-UTRAN

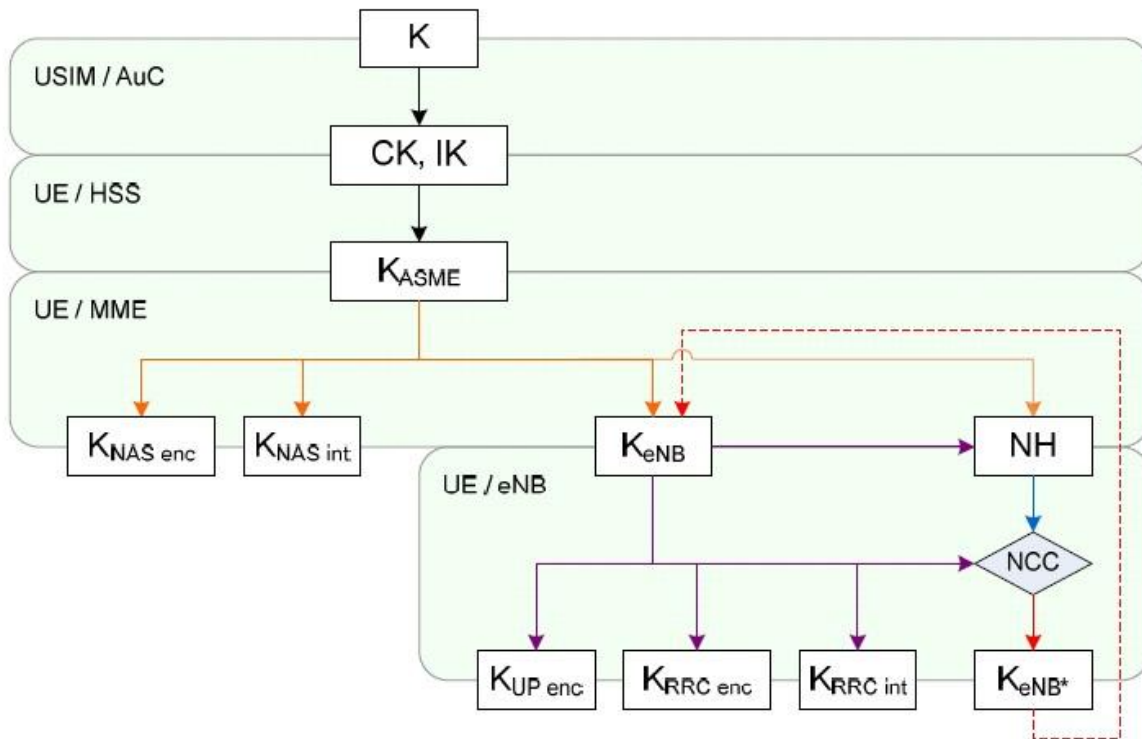
- Ключи СК и IK в открытом виде в ядро сети не передают.
- HSS генерирует K_{ASME} с помощью алгоритма KDF (Key Derivation Function), для которого исходными параметрами являются СК и IK, а также идентификатор обслуживающей сети и SQN Å AK.
- Вектор аутентификации содержит RAND, XRES, AUTN и K_{ASME}' 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:

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

- $K_{NAS\ enc}$ – ключ, используемый для шифрования NAS сигнального трафика; вычисляется абонентским терминалом (UE) и MME из K_{ASME} .

Ключи для защиты RRC сигнального трафика:

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

- $K_{RRC\ enc}$ – ключ, используемый для шифрования RRC сигнального трафика; вычисляется абонентским терминалом (UE) и базовой станцией (eNodeB) из K_{eNB} .

Ключи для защиты пользовательского трафика

- $K_{UP\ int}$ – ключ, используемый для контроля целостности пользовательского трафика; вычисляется абонентским терминалом (UE) и базовой станцией (eNodeB) из K_{eNB} .

- $K_{UP\ enc}$ – 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	
	<u>Knas-int</u>		<u>Knas-int</u>	
	<u>Knas-enc</u>		<u>Knas-enc</u>	
	<u>KeNB</u>	<u>KeNB</u>		
	<u>Krrc-int</u>	<u>Krrc-int</u>		
	<u>Krrc-enc</u>	<u>Krrc-enc</u>		
	<u>Kup-enc</u>	<u>Kup-enc</u>		

Процедура аутентификации

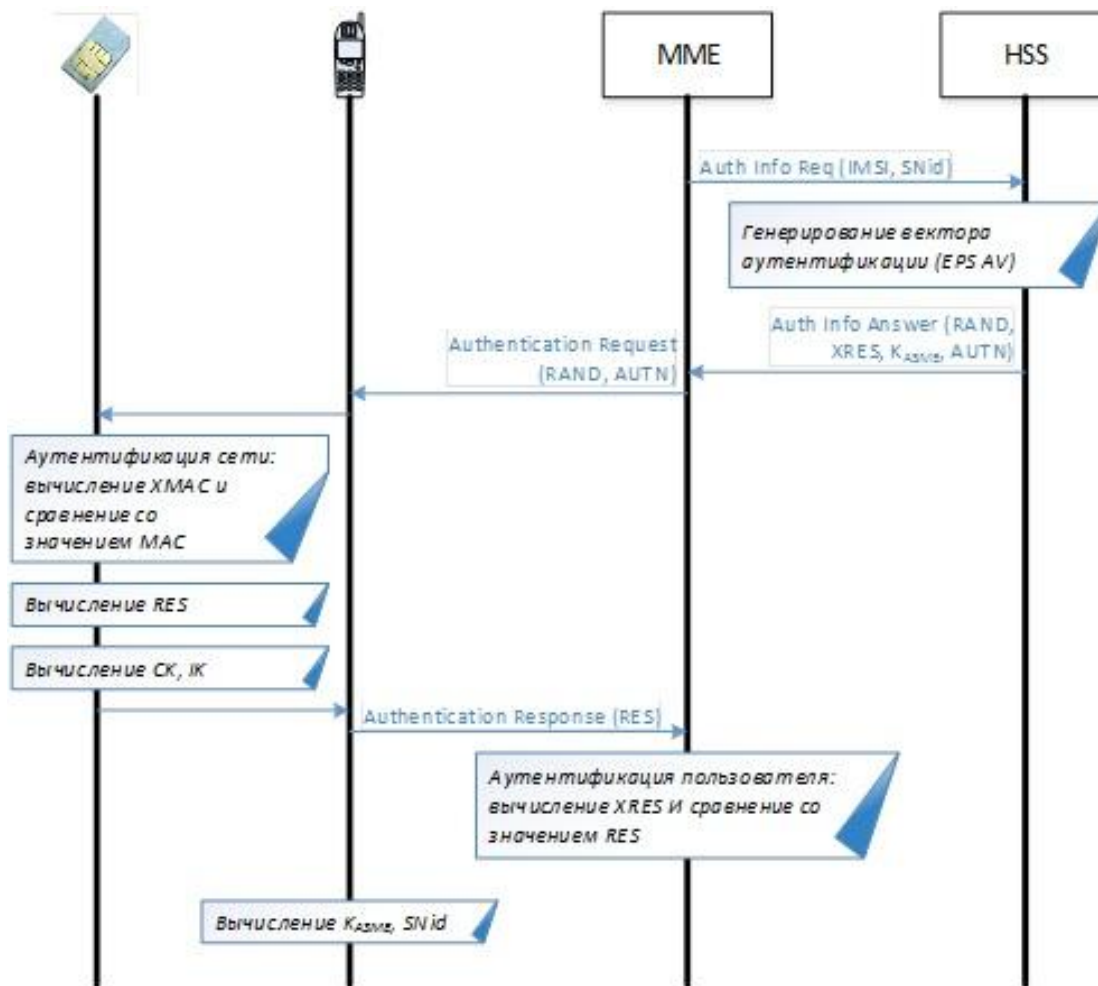
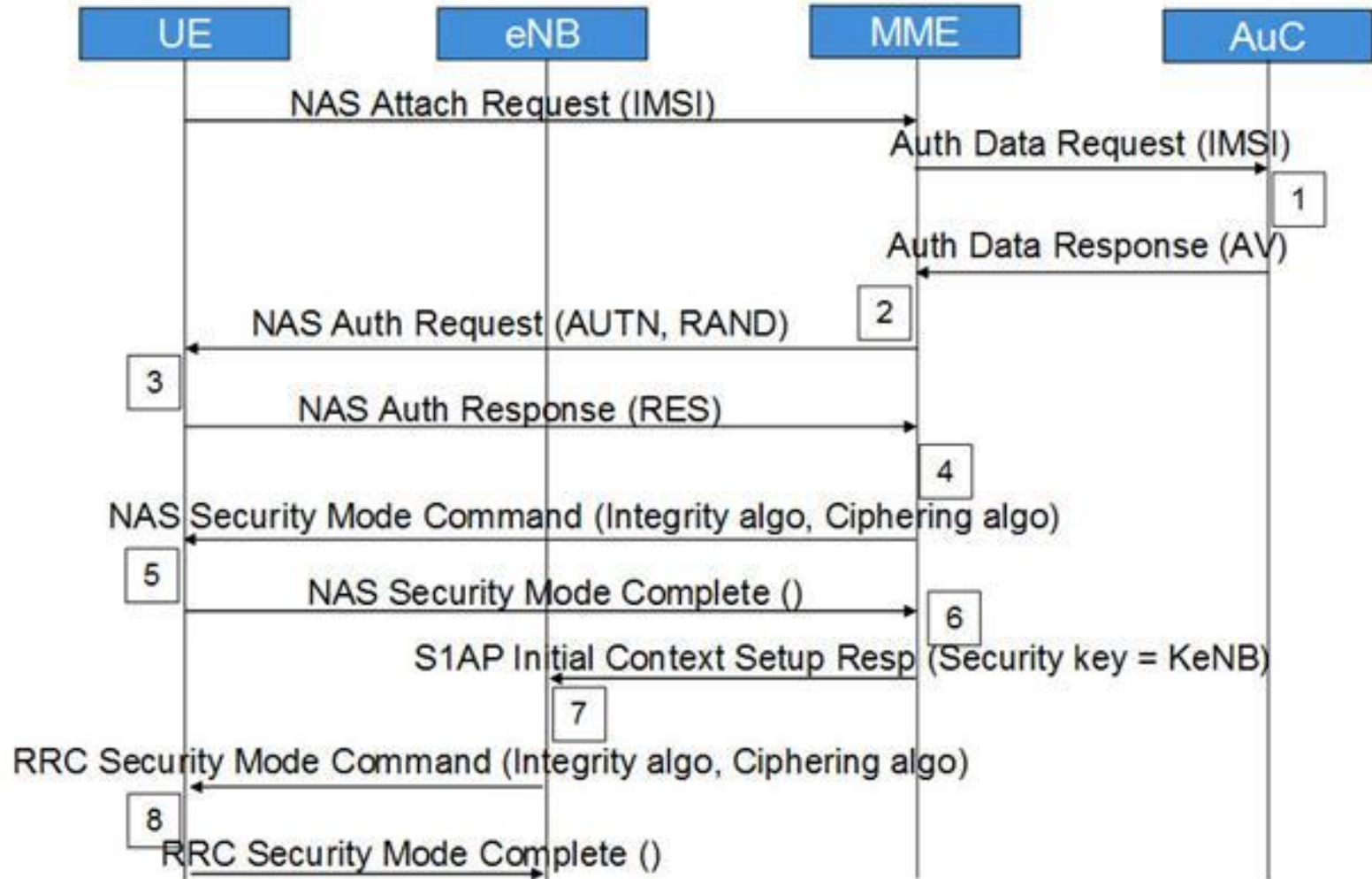
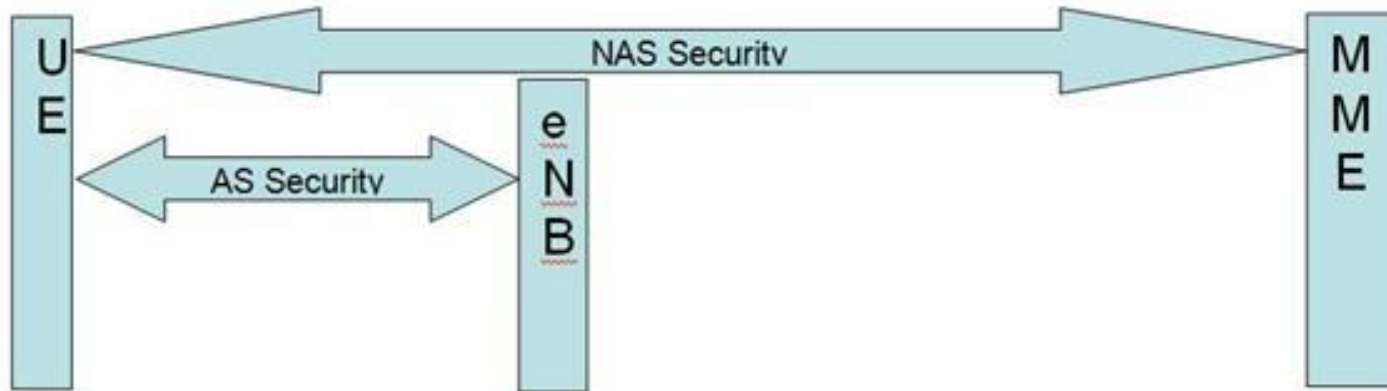


Диаграмма аутентификации и генерации ключа

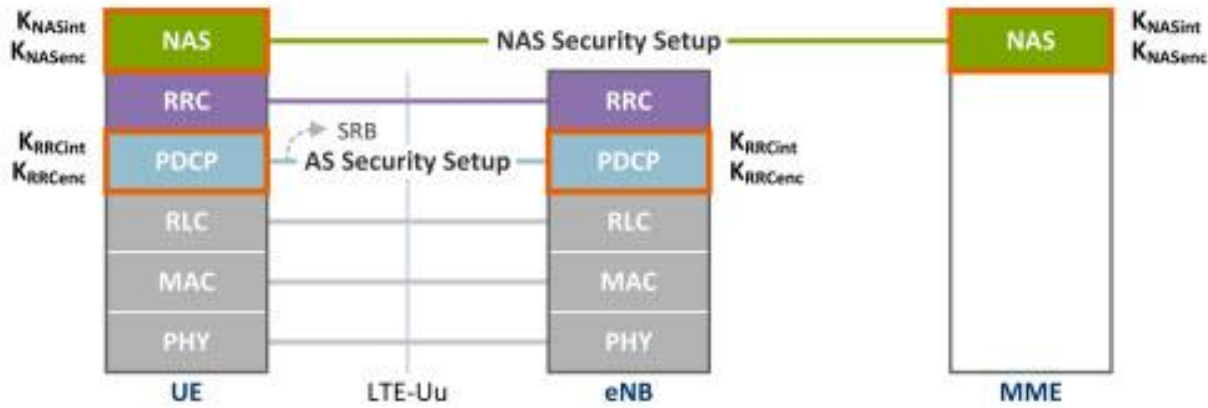


Слои безопасности

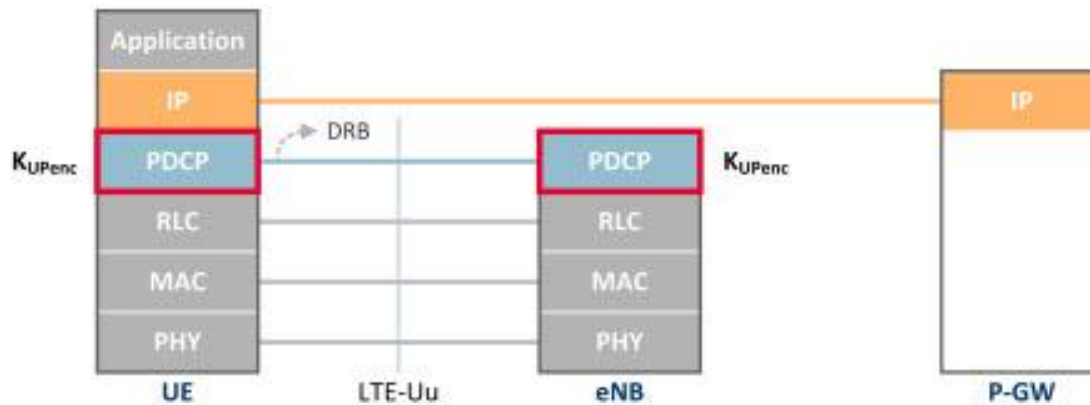


- **Безопасность NAS (Non-Access Stratum - слоя без доступа):**
- Выполнена для NAS сообщений и принадлежит области UE и MME.
- (Non Access Stratum включает в себя протоколы обеспечивающие управление вызовом, управление мобильностью и прочие.)
- **Безопасность AS (Access Stratum - слоя с доступом):**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



User Plane



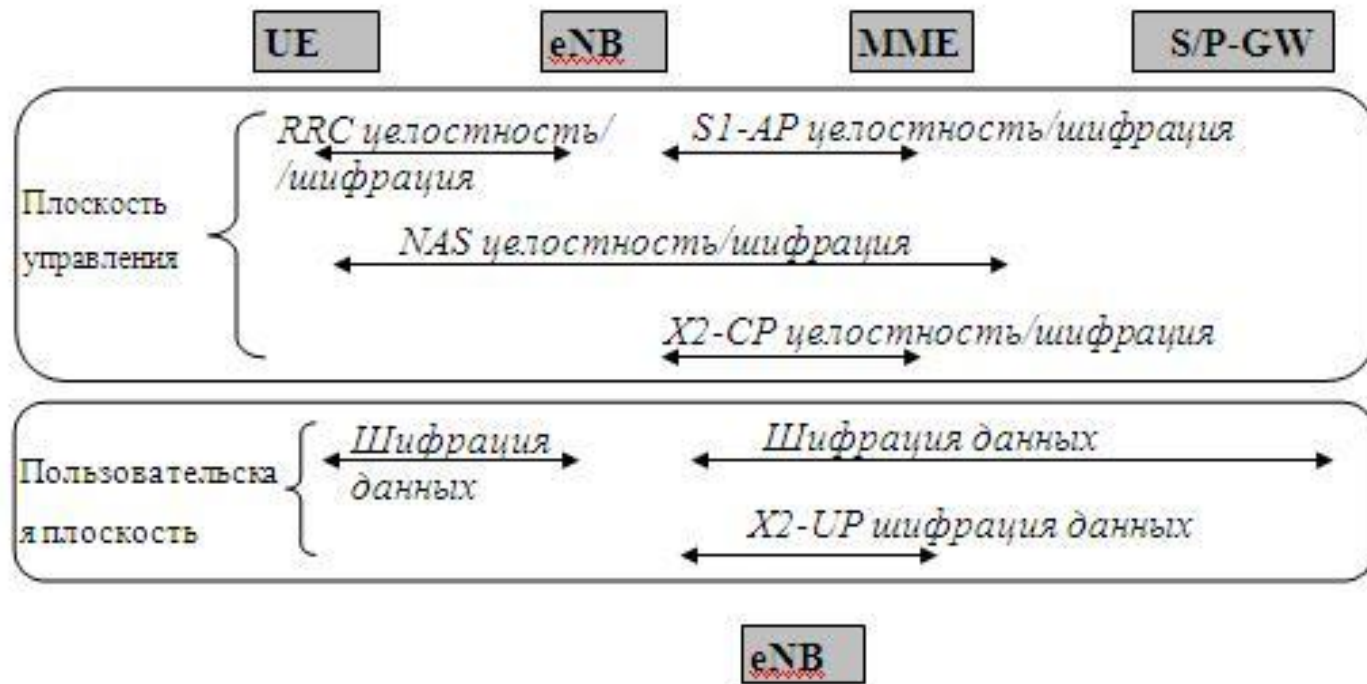
NAS Security Setup
for signaling (NAS signaling)

AS Security Setup
for signaling (RRC signaling)
and user IP packet

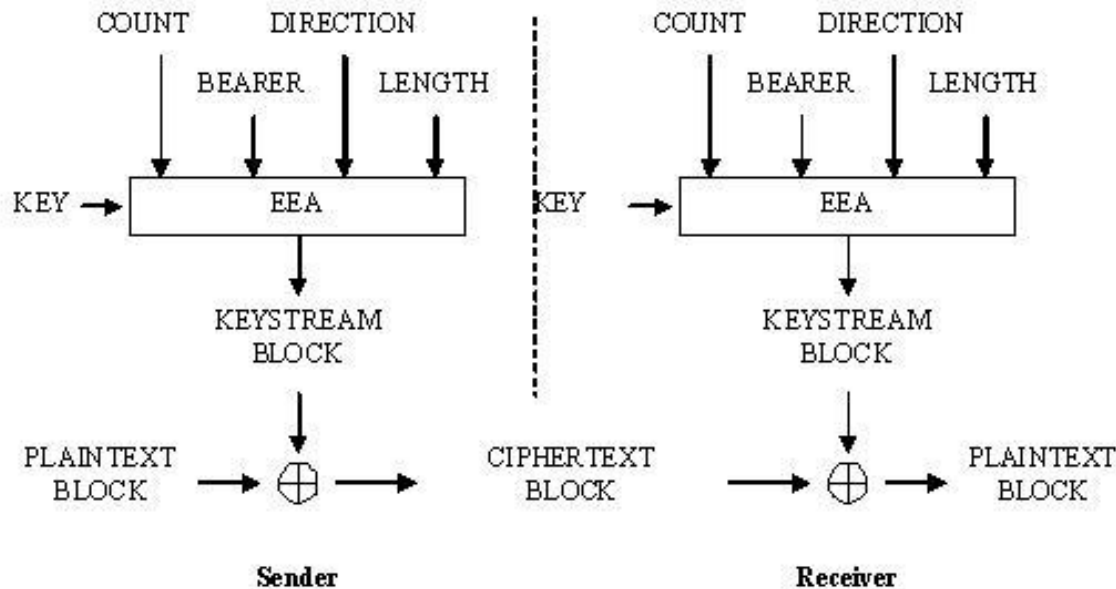
Perform ciphering/deciphering
(encryption/decryption) and
integrity protection/verification

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.

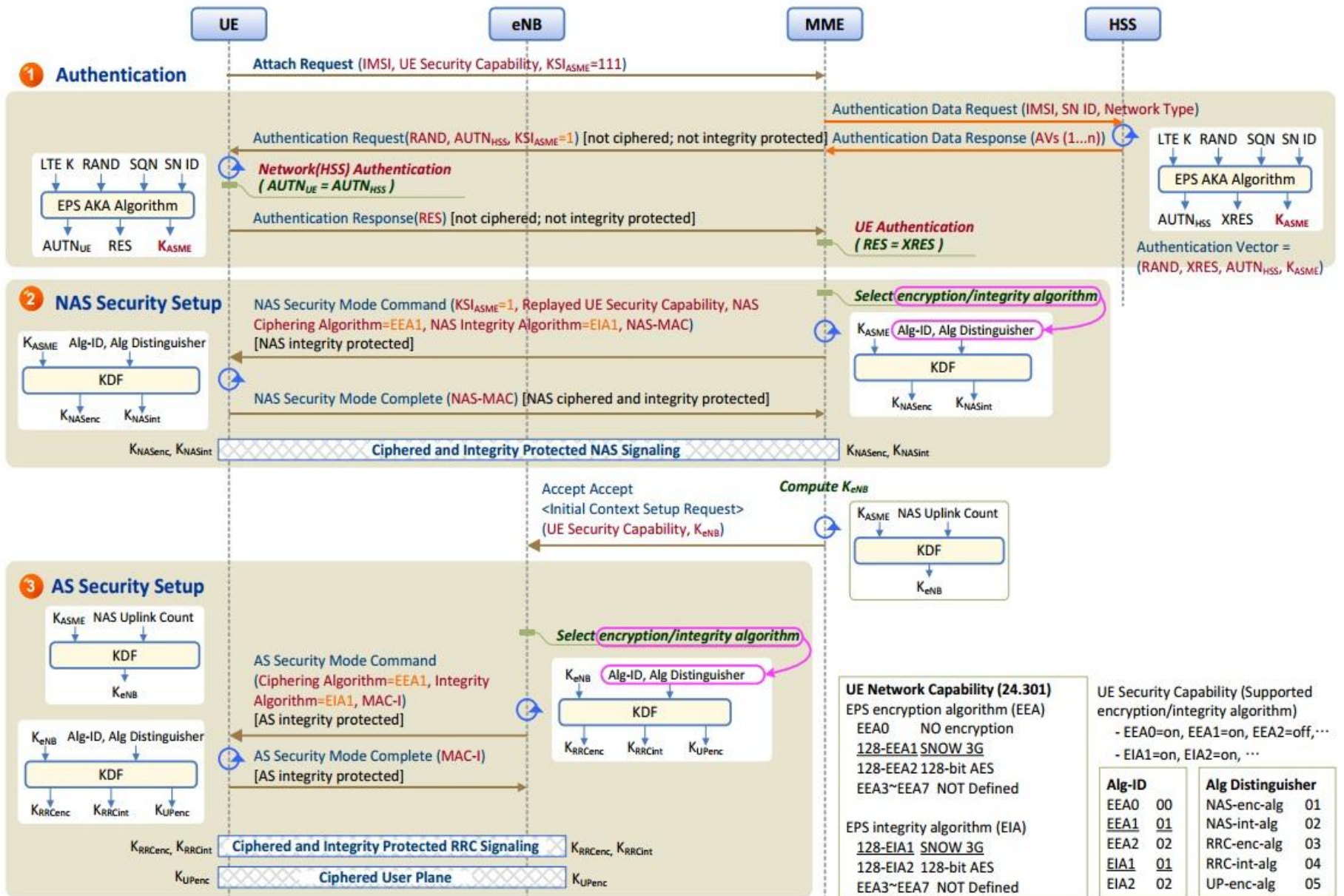
Типы алгоритмов и размеры ключей в сетях LTE

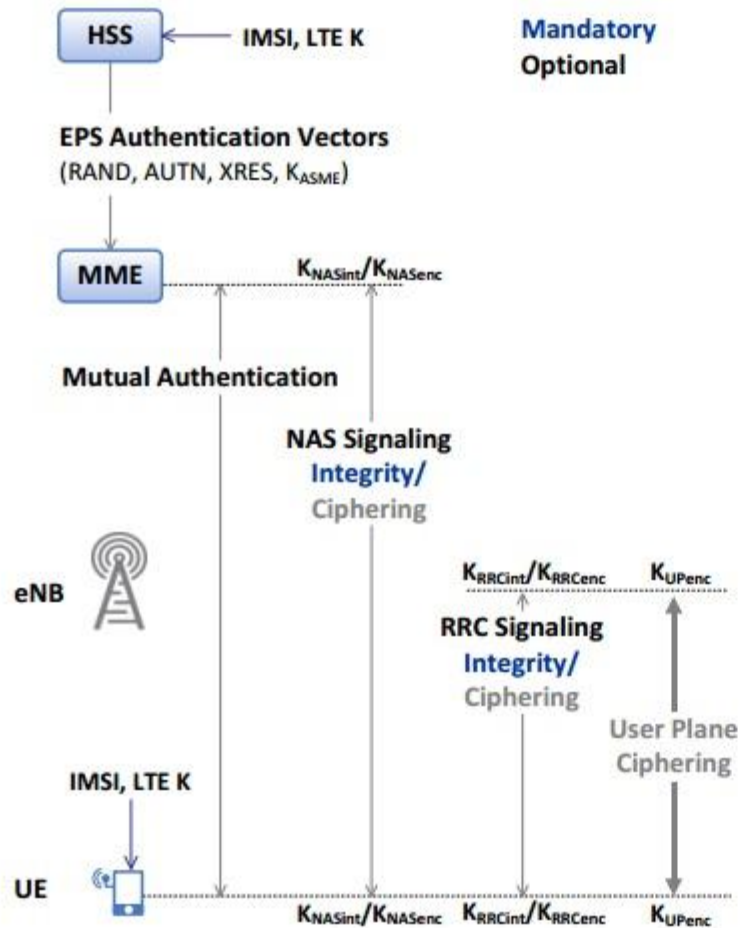
В качестве алгоритмов шифрования используются следующие:

- **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





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)**