Процедуры безопасности в сетях LTE и NR

2. LTE радио протокол

Для передачи трафика в радиоканале в eNB и UE происходит обработка дейтаграмм на протокольном уровне L2, в результате которой формируют блоки, передаваемые по радиоинтерфейсу. Структура уровня L2 в eNB при передаче вниз показана на рисунке 2.1; структура уровня L2 в UE при передаче вверх – на рисунке 2 .2.

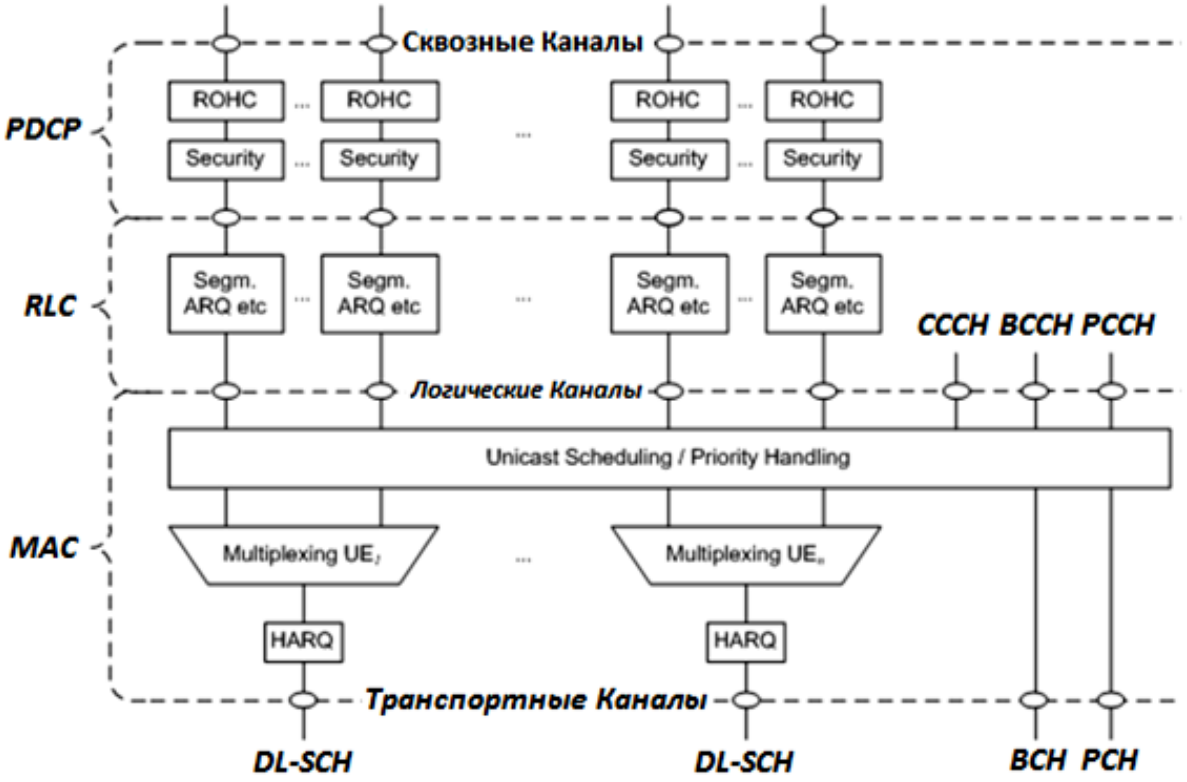


Рисунок 2.1 – Структура уровня L2 при передаче вниз

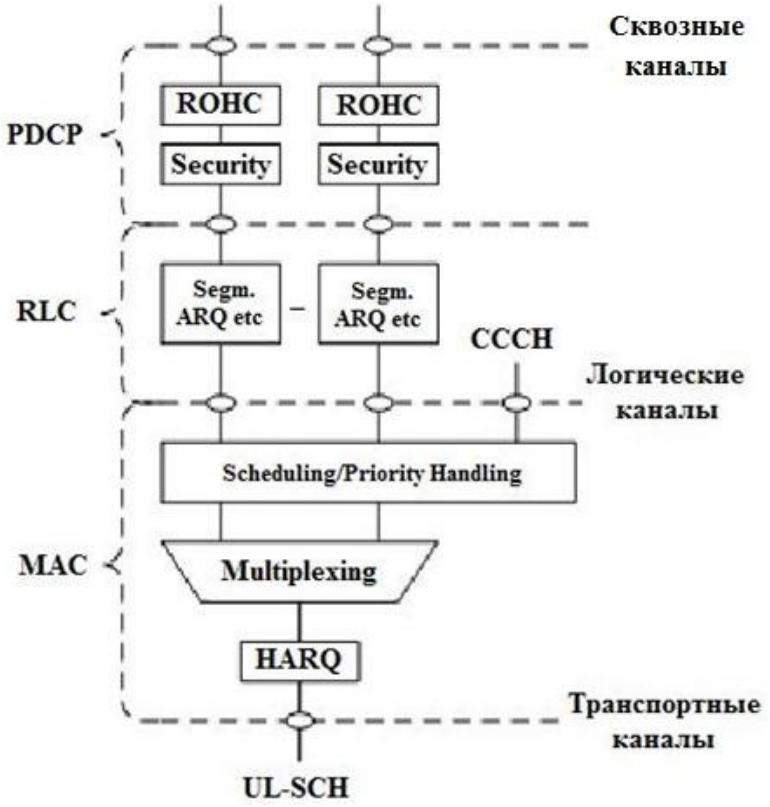


Рисунок 2.2 – Структура уровня L2 при передаче вверх

LTE радио протокол включает в себя 3 уровня (рисунок 2.3).

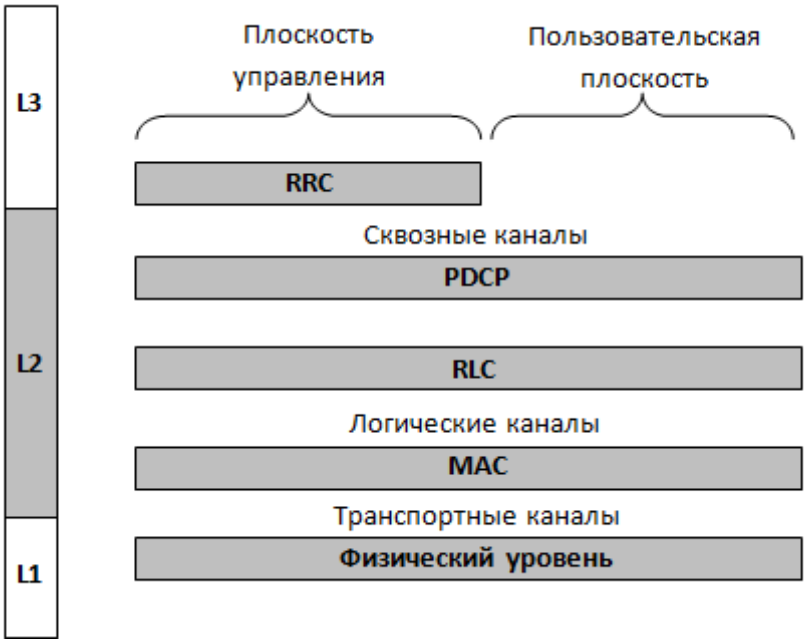


Рисунок 2.3 – Структура радио протоколов LTE

В плоскости управления на уровне L3 находится RRC (Radio Resource Control) протокол. Уровень L2 расщеплен на 3 подуровня:

- PDCP – Packet Data Convergence Protocol, протокол конвергенции пакетов данных;

- RLC – Radio Link Control Protocol, протокол управления радиосоединением;

- MAC – Medium Access Control Protocol, протокол управления доступом к среде.

Протокол RRC представляет собой систему алгоритмов и команд, используемых для обслуживания UE на радиоинтерфейсе.

Рассмотрим функции, выполняемые различными подуровнями L2 радиоинтерфейса. На ***протокольном уровне PDCP*** обрабатывают данные более высоких уровней: SDU (Service Data Units) – дейтаграммы трафика и сигнальные сообщения. При этом осуществляют:

- сжатие (и, соответственно, восстановление) IP-заголовков, используя протокол ROHC (Robust Header Compression),

- шифрацию и дешифрацию SDU трафика и сигнализации (в UMTS это делают на уровнях RLC или MAC),

- защиту (проверку) целостности сигнальных сообщений (в UMTS это осуществляют на уровне RLC).

Последовательность производимых операций показана на рисунке 2.4.

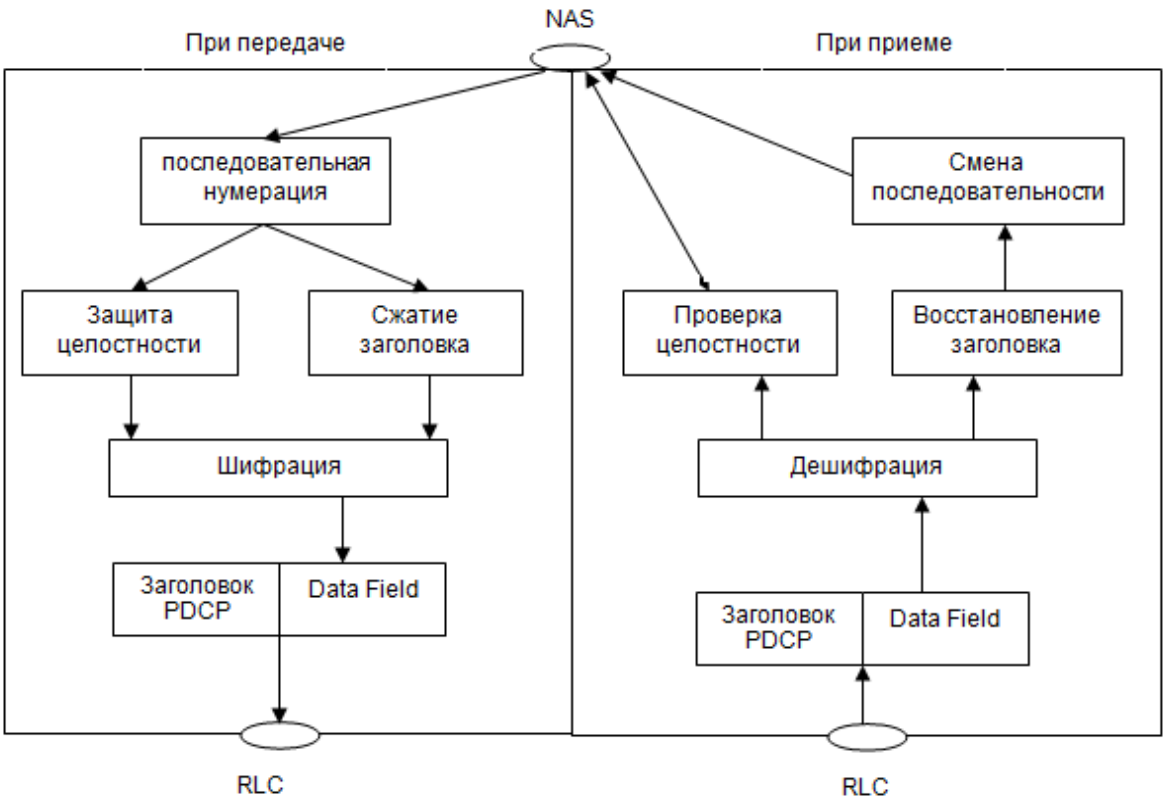


Рисунок 2.4 – Операции, выполняемые на уровне PDCP

Кроме указанных функций, уровень PDCP обеспечивает передачу данных без потерь при хэндоверах и обрывах связи.

На ***уровне RLC*** осуществляют:

- сегментацию SDU на PDU (Protocol Data Unit) для передачи и объединение пакетов при приеме в требуемой последовательности,

- коррекцию ошибок при передаче, используя повторную передачу (ARQ),

- устранение ошибок в передаче пакетов, вызванных ошибками сигнализации.

Возможны 3 режима обработки пакетов на уровне RLC в зависимости от характера передаваемой информации:

- прозрачный (transparent mode) пакеты не обрабатывают на уровне RLC,

- передача без подтверждения (unacknowledged mode),

- передача с подтверждением (acknowledged mode).

На ***уровне MAC*** происходит размещение и мультиплексирование пакетов логических каналов в транспортных с последующей передачей их по физическим каналам. Уровень MAC осуществляют:

- управление выделением канального ресурса с учетом приоритетов трафика, т.е. выполняют задачи планирования передач,

- выбор транспортных форматов передач,

- управление повторными передачами непринятых пакетов,

- организацию процедур доступа UE к сети и периодической синхронизации UE,

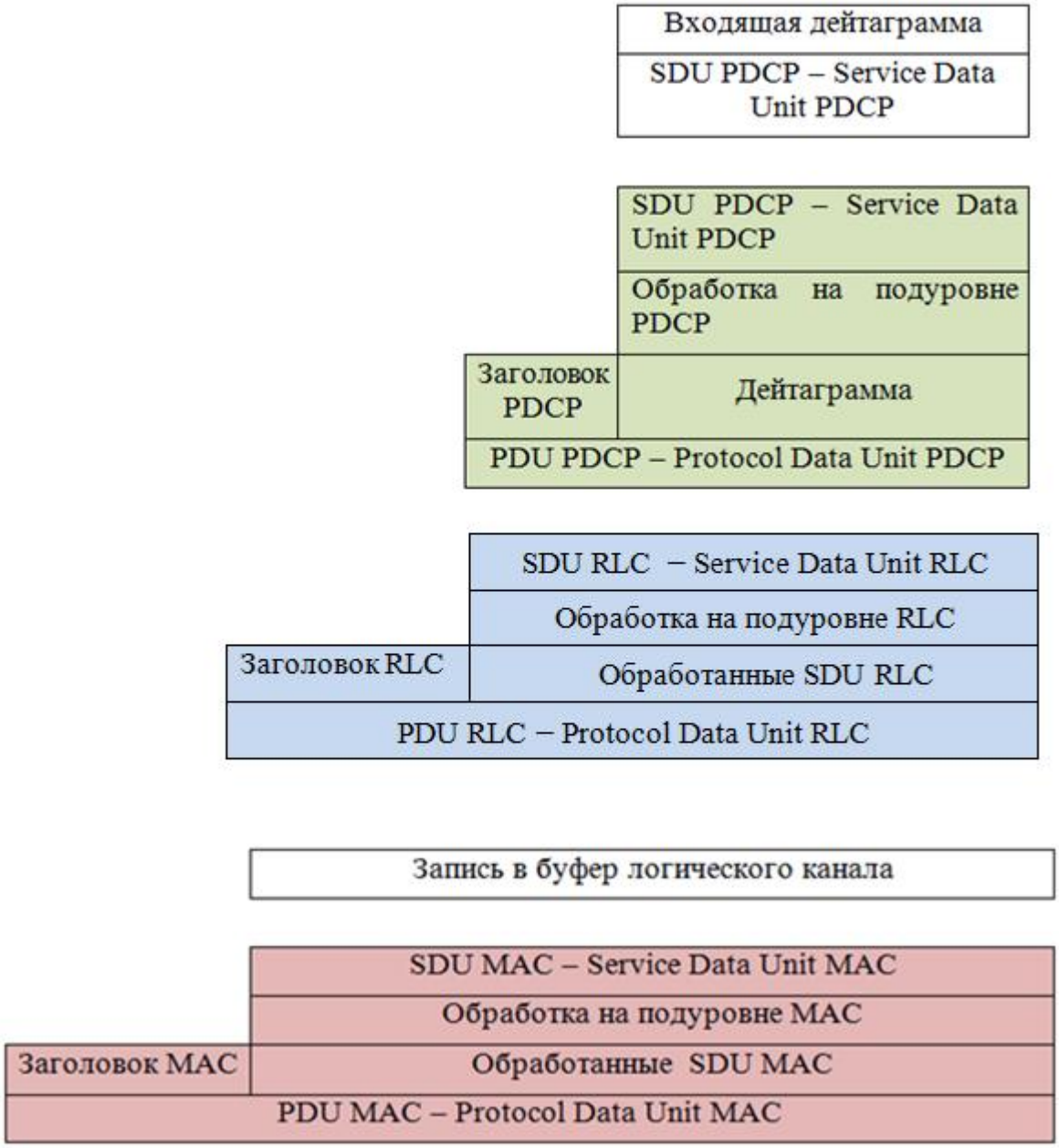
- измерения: объема передаваемого трафика, загрузки канала, состояния буферов передачи UE, относительной мощности передачи UE и ряд других,

- организацию режима сна/прерывистого приема (DRX) абонентских станций.

Протокольные уровни MAC и RLC тесно связаны между собой. В зависимости от характеристик канала связи и загрузки сети MAC выбирает оптимальный формат передачи (модуляцию, скорость избыточного кодирования, объем передачи), на основе которого RLC устанавливает размер PDU. MAC уведомляет RLC о начале передачи по конкретному соединению и о числе PDU, которые RLC должен выставить в данный момент. При неприеме PDU MAC сообщает RLC о необходимости повторной передачи.

Работой уровня MAC непосредственно руководит планировщик (scheduler), алгоритмы работы которого и ПО являются know-how производителя аппаратуры.

Последовательность обработки дейтаграмм



Рассмотренная структура уровня L2 на радиоинтерфейсе с незначительными добавками сохраняется и в стандарте NR. Принципиальным является ввод ещё одного верхнего подуровня SDAP – Service Data Adaptation Protocol, расположенного над подуровнем PDCP. Задачей подуровня является выделение потоков трафика с определёнными QoS и обеспечение QoS на радиоинтерфейсе. Однако подуровень SDAP является опциональным.

Сигнальный протокол RRC обеспечивает следующие функции и процедуры:

- передачу системной информации по радиоинтерфейсу,
- пейджинг,
- установление, поддержку и разрыв соединения по протоколу RRC между UE и e-UTRAN,
- выполнение задач безопасности, в том числе управление ключами,
- организацию части сквозного канала на радиоинтерфейсе,
- хэндоверы,
- селекцию сот при перемещении UE,
- передачу сигнализации NAS между UE и ядром сети,
- исправление системных ошибок между UE и ядром сети,
- поддержку самоконфигурации и самооптимизации сети.

3. Процедуры безопасности в сетях LTE

В стандарте LTE технологии безопасности фактически были заимствованы у стандартов прошлых поколений, в частности из UMTS, но с рядом изменений. Изменения коснулись защиты целостности сигнальных сообщений. Все сигнальные сообщения, которыми обмениваются мобильный терминал с сетью, делятся на два класса:

1. сообщения меду UE и BS, которые реализованы по протоколу RRC.
2. сигнальные сообщения, которыми обмениваются непосредственно UE и MME в ядре сети. Эти сообщения относятся к классу NES, их дополнительно шифруют и защищают их целостность в узлах UE и MS.

Безопасность в сетях E-UTRA (LTE) включает в себя:

- взаимная аутентификация абонента и сети;
- шифрование сообщений в радиоканале;
- обеспечение защиты целостности передаваемых сообщений;
- защита абонентов.

Защита абонента достигается закрытием его временными идентификаторами M-TMSI, S-RNTI и C-RNTI. Отметим, что в сетях четвертого поколения были приняты меры для обеспечения безопасности внутрисетевых соединений (туннели). На интерфейсах S1 и X2 передаваемые пакеты можно шифровать, используя IPsec ESP. Подвергаются шифрацию и сообщения в сигнальных плоскостях этих интерфейсов.

При каждом подключении или активизации UE в сети, сеть начинает процедуру аутентификации и соглашения о ключах AKA (Authentication and Key Agreement). Это делается для взаимной аутентификации абонента с сетью и выработке промежуточного ключа K_{ASME}.

Процедуру аутентификации инициирует MME, посылая в HSS соответствующий запрос. В ответ HSS направляет в MME вектор аутентификации:

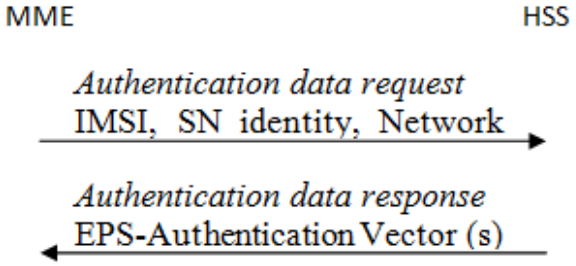


Рисунок 3.2 – Запуск процедуры аутентификации

На рисунке 3.2 SN (Serving Network) identity – идентификатор обслуживающей сети (24 бита), который состоит из MCC и MNC (кода страны и кода оператора). Тип сети (Network Type) – E-UTRA. Из HSS обслуживающая сеть (MME) получает вектор аутентификации EPS (Evolved Packet System). Вектор аутентификации в HSS генерируется в два этапа. На первом этапе используют алгоритм, принятый в UMTS (рисунок 3.3) [12].

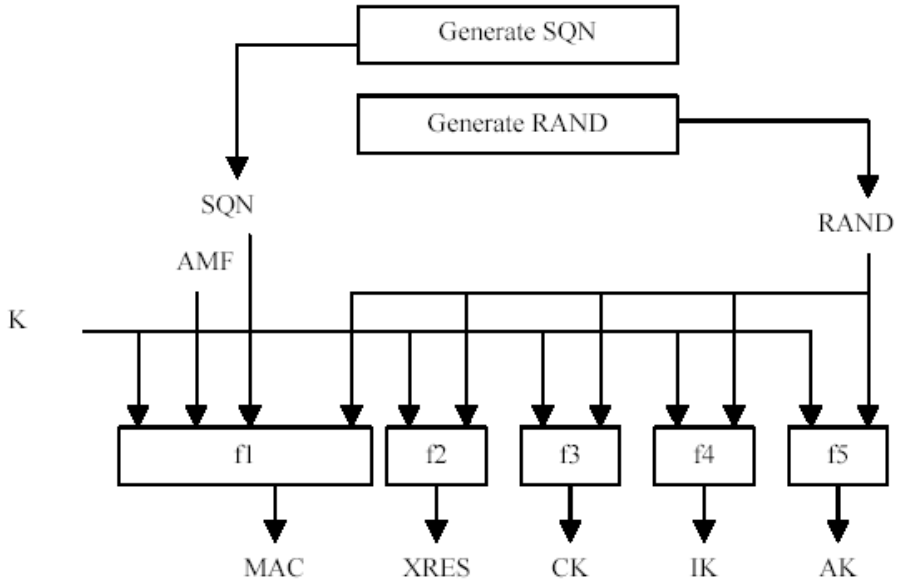


Рисунок 3.3 – Исходный алгоритм генерации вектора аутентификации

Криптографический алгоритм (рисунок 3.3) реализован с помощью однонаправленных функций. Это означает, что прямой результат получают путем простых вычислений, но, к сожалению, не существует эффективного алгоритма для получения обратного результата. В самом алгоритме используются 5 однонаправленных функций: *f*1, *f*2, *f*3, *f*4 и *f*5. Исходными параметрами являются случайное число RAND <128бит>, Master Key K абонента <128бит> и порядковый номер процедуры Sequence Number SQN. Счетчик SQN меняет свое значение при каждой генерации вектора аутентификации. Аналогичный счетчик SQN работает в USIM. Это позволяет каждый раз получать новый вектор аутентификации и делает повторение уже использованного вектора невозможным.

Кроме трех исходных величин SQN, RAND и K в алгоритме *f*1 участвует поле управления аутентификацией Authentication Management Field AMF, в алгоритмах *f*2–*f*5 исходные параметры – RAND и K. На выходах соответствующих функций получают Message Authentication Code (MAC) 64 бита, XRES – eXpected Response, результат работы алгоритма аутентификации 32–128 бит, ключ шифрации CK, ключ целостности IK и промежуточный ключ Anonymity Key AK 64 бита.

Второй этап генерации вектора аутентификации зависит от типа сети обслуживания. Поле AMF содержит специальный бит (separation bit), определяющий тип сети: если он равен 0, то это сеть GERAN/UMTS. В этом случае вектор аутентификации состоит из чисел RAND, XRES, ключей CK, IK и числа AUTN, который представляет собой запись в строку трех параметров: SQN⊕AK, AMF и MAC.

При обслуживании абонента сетью E-UTRA ключи CK и IK не передают в открытом виде в ядро сети. 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⊕AK. Вектор аутентификации содержит RAND, XRES, AUTN и K_{ASME}, на основе которого происходит генерация ключей шифрации и целостности, используемых в соответствующих алгоритмах.

Мобильная станция получает из ядра сети три параметра: RAND, AUTN и KSI_{ASME} (рисунок 3.4). KSI – Key Set Identifier, индикатор установленного ключа, однозначно связанный с K_{ASME} в мобильной станции.

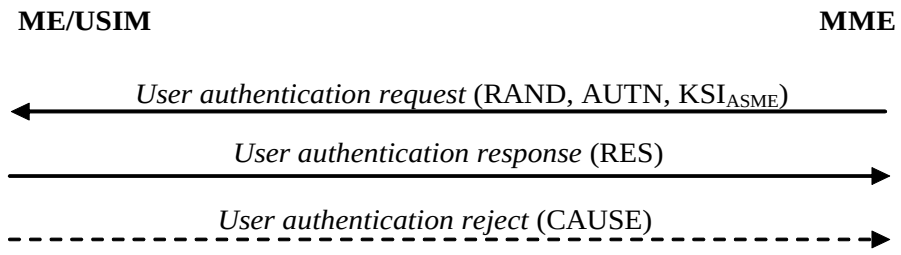


Рисунок 3.4 – Завершение процедуры аутентификации

Используя RAND и AUTN, USIM на основе алгоритмов безопасности, тождественных хранящимся в HSS, производит вычисление MAC, XRES, CK и IK (показано на рисунке 3.5).

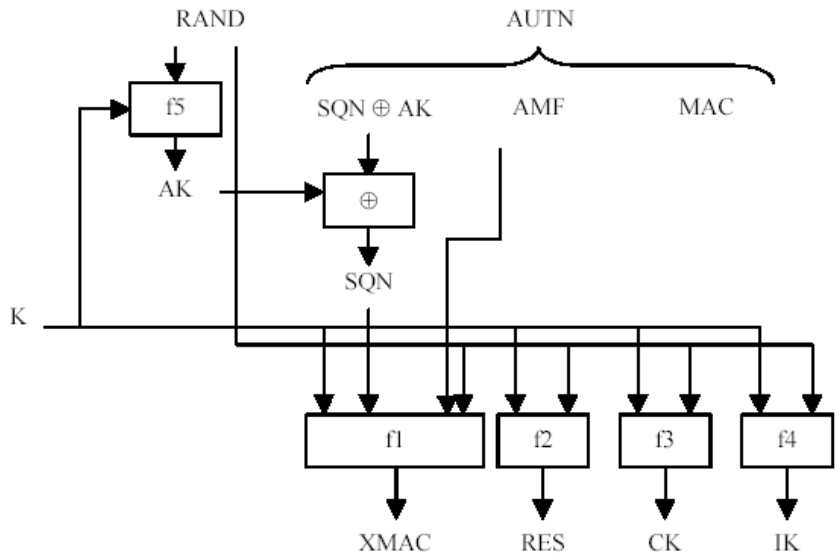


Рисунок 3.5 – Процедура аутентификации в USIM

В ответе *Res* UE передает в MME вычисленное RES, которое должно совпасть с XRES, полученным из HSS. Так сеть аутентифицирует абонента. Вычислив XMAC, UE сравнивает его с MAC, полученным ею в AUTN. При успешной аутентификации абонентом сети (MAC = XMAC) UE сообщает об этом в ответе *RES*. Если аутентификация сети не удалась (MAC ≠ XMAC), то UE направляет в MME ответ *CAUSE*, где указывает причину неудачи аутентификации.

Далее MME, eNB и UE производят генерацию ключей, используемых для шифрации и проверки целостности получаемых сообщений. Иерархия ключей в E-UTRA приведена на рисунке 3.6.

Исходным ключом для всей цепи является K_{ASME} 256 бит. Обеспечивается зашита для сигнального трафика (Control Plane) и для пользовательских пакетов (User Plane) при передаче в радиоканале. Все сообщения сигнализации делят на сквозные сигнальные сообщения между UE и MME протоколов MM и SM (NAS – Non Access Stratum) и сигнальные сообщения между eNB протокола RRC (AS – Access Stratum). Для шифрования и защиты целостности используются разные базовые алгоритмы:

- UEA2 (UMTS Encryption Algorithm 2) и UIA2 (UMTS Integrity Algorithm 2), разработанные для стандартов 3G;
- AES (Advanced Encryption Standard).

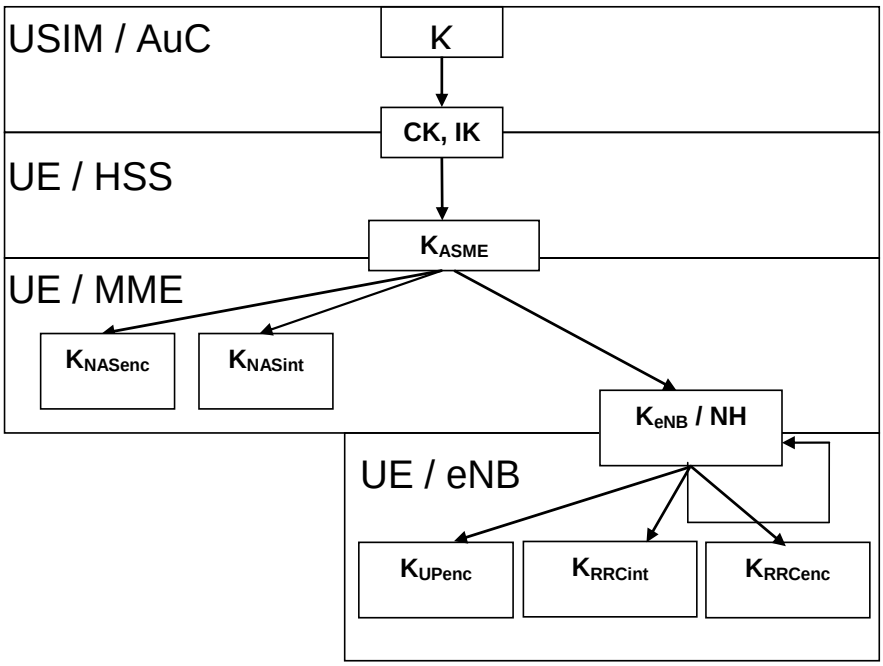


Рисунок 3.6 – Иерархия ключей в E-UTRA

Для сигнальных сообщений NAS ключи шифрации K_{NASenc} и целостности K_{NASint} получают по схеме (рисунок 3.7). Входными параметрами являются K_{ASME}, тип алгоритма (в данном случае *NAS-enc-alg* или *NAS-int-alg*) и идентификаторы базовых алгоритмов (UEA2, UIA2) или AES. На выходах генераторов ключей KDF (Key Derivation Function) соответствующие ключи имеют длину 256 бит. У каждого ключа усекают 128 старших бит (Trunc); в результате получают рабочие ключи длиной 128 бит. Эти процедуры выполняют параллельно в UE и MME.

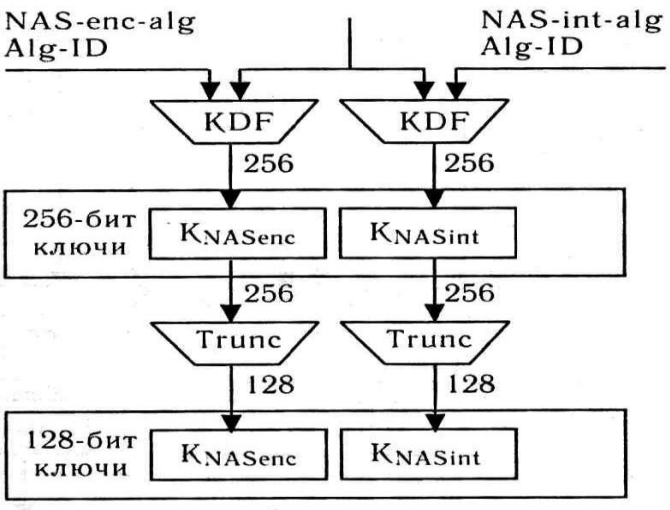


Рисунок 3.7 – Генерирование ключей шифрации и целостности для NAS сигнализации

Сигнальные сообщения протокола RRC (AS) тоже шифруют, обеспечивая их целостность, а трафик только шифруют. Эти операции производят в обслуживающей eNB и UE. Схема получения ключей шифрации и целостности (рисунок 3.8) для AS- и UP-трафика отличается от схемы на рисунке 3.7 тем, что исходным параметром здесь служит вторичный промежуточный ключ K_{eNB} 256 бит. Этот ключ генерируют, также используя KDF, где входными параметрами являются: K_{ASME}, счетчик сигнальных сообщений NAS вверх, прежнее значение K_{eNB}, идентификатор соты и номер частотного канала в направлении вверх. Таким образом, при каждой периодической локализации UE происходит изменение K_{eNB}.

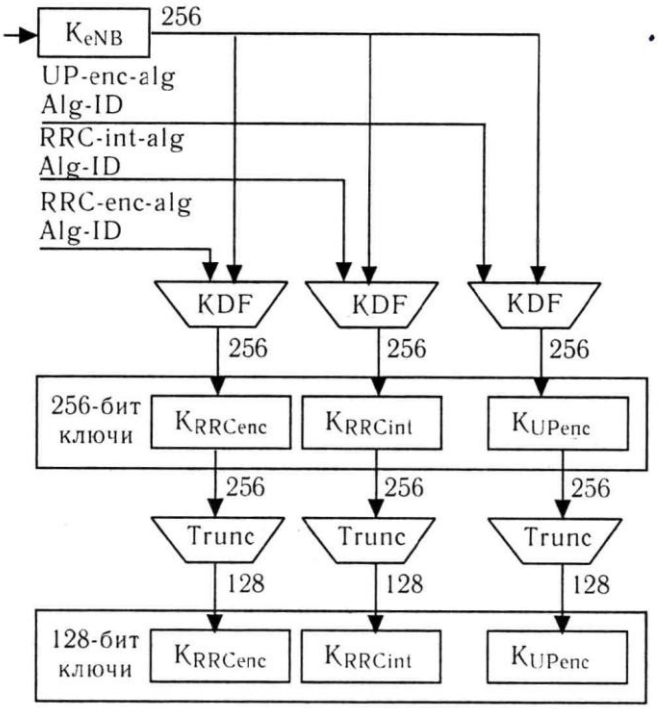


Рисунок 3.8 – Генерирование ключей для сигнализации AS и пакетов трафика UP

K_{eNB} меняется и при хэндовере. При этом в алгоритме генерации нового K_{eNB} можно использовать дополнительный параметр NH (Next Hop), фактически счетчик числа базовых станций, по цепочке обслуживающих абонента. Все реализуемые процедуры безопасности в сети E-UTRAN проиллюстрированы на рисунке 3.9.

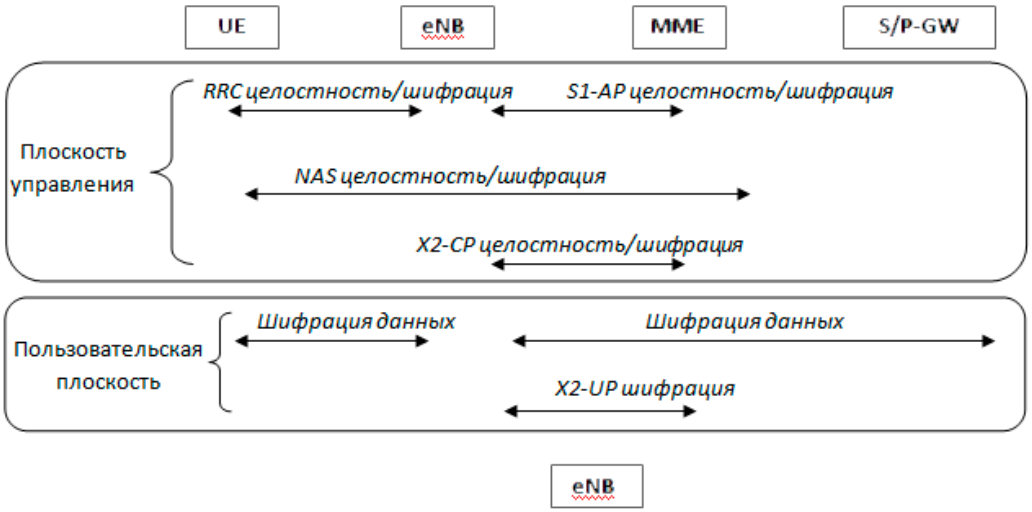


Рисунок 3.9 – Реализуемые процедуры безопасности в сети E-UTRAN

Алгоритм шифрации и дешифрации сообщений представлен на рисунке 3.10. Исходные параметры: шифрующий ключ *KEY* 128 бит, счетчик пакетов (блоков) *COUNT* 32 бита, идентификатор сквозного канала *BEARER* 5 бит, указатель направления передачи *DIRECTION* 1 бит и 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 ту же операцию.

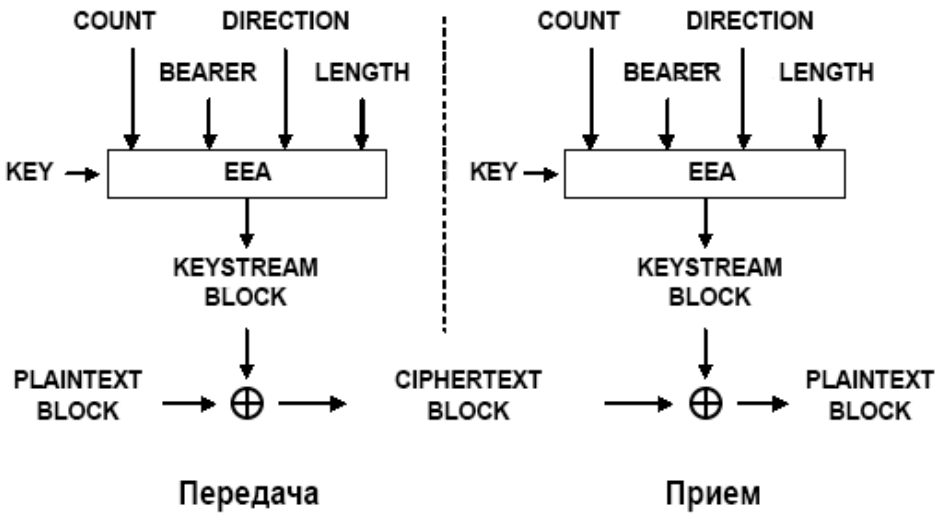


Рисунок 3.10 – Алгоритмы шифрации и дешифрации в E-UTRA

Защита целостности сообщений заключается в генерации «хвоста» MAC (Message Authentication Code) 32 бита, который присоединяется к передаваемому пакету. Алгоритм генерации MAC и проверки целостности полученного пакета путем сравнения XMAC с MAC (они должны совпасть) показаны на рисунке 3.11.

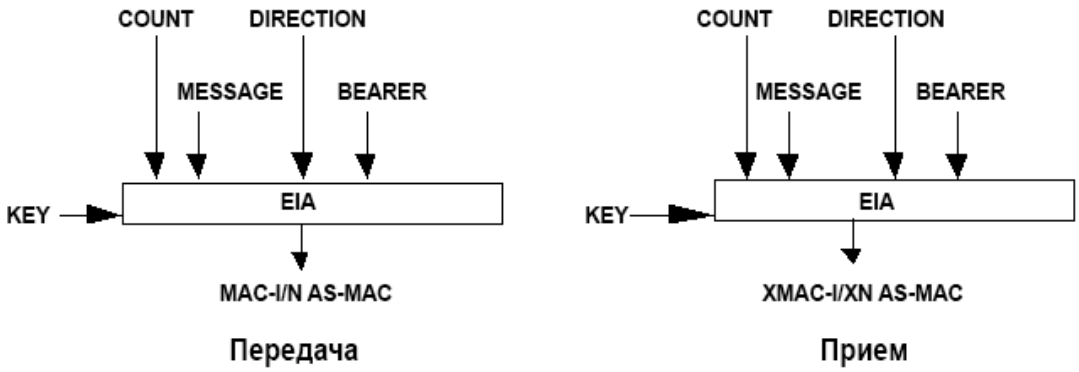


Рисунок 3.11 – Алгоритм проверки целостности в E-UTRA

В алгоритме *EIA (EPS Integrity Algorithm)* использован ключ целостности *KEY* 128 бит, счетчик сообщений *COUNT* 32 бита, идентификатор сквозного канала *BEARER* 5 бит, указатель направления передачи *DIRECTION* 1 бит и само сообщение *MESSAGE*.

В сетях LTE особенно много внимания уделено защите абонентов, а, например, в GSM и UMTS при подключении к сети абонентская станция передает системный номер абонента IMS, который никак не шифруется.

В сетях четвертого поколения продумана возможность использования последнего временного идентификатора абонента при включенной мобильной станции. База данных абонентов в MME после отключения абонентов сети не удаляется, а просто блокируется. Время хранения такой базы данных определяет сам оператор. При новом подключении абонента к сети, где он раньше уже был зафиксирован, абонентская станция вместо посылки IMS посылает GUTI.

4 Безопасность в сетях 5G (New Radio)

4.1 Архитектура сети 5G (New Radio)

Архитектура системы 5G построена на принципах виртуализации сетевых функций (NFV) и программно-определяемых сетей (SDN) для предоставления возможностей передачи данных и предоставления различных услуг. Архитектура системы 5G должна обеспечивать взаимодействие плоскости управления и сетевых функций. Отделение плоскости пользователя и плоскости управления позволяет гибкое развертывание и независимую масштабируемость сети. Все сетевые функции могут взаимодействовать между собой с возможностью их повторного использования. Архитектура NR объединяет различные типы сетей доступа благодаря общему интерфейсу между ядром сети и сетью доступа, например, «3GPP-доступ» и не «3GPP-доступ». Поэтому необходимо обеспечить единую систему проверки подлинности.

Если архитектура сетей 3G+ и 4G базируется на формирование сквозных каналов, то в сетях 5G организуют прямые соединения в виде структурно независимых сетей, ориентированных на реализацию конкретных услуг. Поэтому базовая архитектура NR специфицирована в виде соединений функциональных узлов (рисунок 4.1). Она состоит из подсистемы радиодоступа (R)AN и ядра сети (NR Core). В пользовательской плоскости обеспечивается прямое соединение между (абонентским) терминалом UE и сетью данных DN (на рисунке 4.1 показано жирной линией).

Ядро сети составляют функциональные узлы, которые сеть 5G организует в соответствии с запрошенными услугами. Якорные функции в визитной сети выполняет UPF (User Plane Function), а функции доступа, регистрации и мобильности **AMF (Access and Mobility Management Function).**

AMF включает в себя следующие функции:

- поддержка интерфейса с сетью доступа в плоскости управления;

- формирование и шифрование NAS-сообщений;

- управление соединением;

- передача сообщений управления;

- организация канала для передачи SM (Session Management) сообщений между UE и SMF без обработки этих сообщений;

- аутентификация доступа;

- авторизация доступа;

- организация канала для передачи SMS-сообщений между UE и SMSF;

- осуществление процедур безопасности;

- функция определения местоположения;

- присвоение EPS Bearer ID для взаимодействия с EPS (Evolved Packet System);

- функции, необходимые для поддержки не «3GPP-сетей».

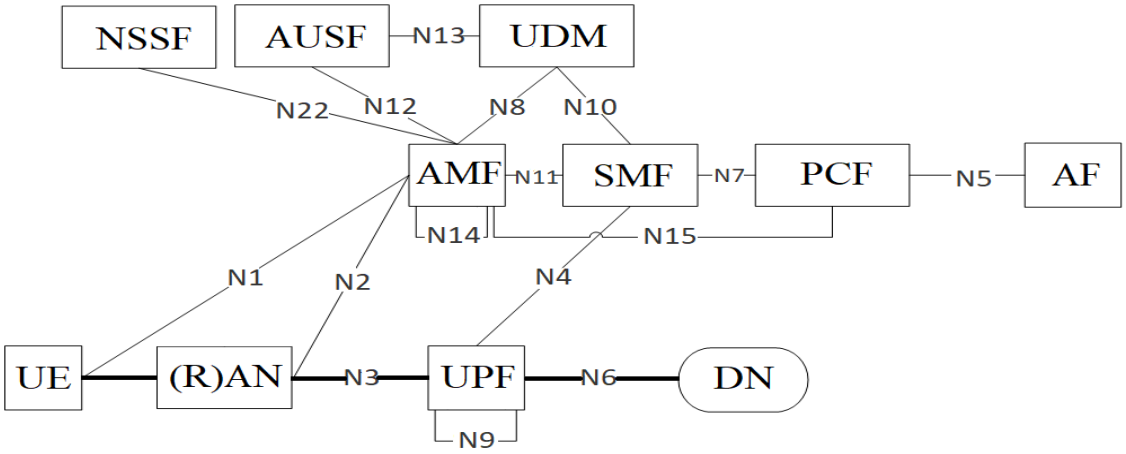


Рисунок 4.1 – Архитектура NR

Функция управления сеансом связи **SMF (Session Management Function)** включает следующие функции:

- управление сеансом, включая туннельное соединение между UPF и узлом сети доступа;
- назначение IP-адреса и дополнительная авторизация;
- поддержка протоколов DHCP (Dynamic Host Configuration Protocol) v4 и v6;
- выбор и управление функцией UPF;
- управление трафиком в UPF для маршрутизации трафика в требуемое место назначения;
- поддержка интерфейса с PCF;
- сбор данных об оплате в UPF;
- формирование SM-сообщений NAS;
- определение режима SSC (Session and Service Continuity) сеанса;
- поддержка взаимодействия с внешними DN для передачи сигналов для PDU. Аутентификация сеанса с помощью внешних сетей данных.

Функциональное устройство в пользовательской плоскости **UPF (User Plane Function)** включает следующие функции:

- якорные функции в визитной сети;
- маршрутизация пакетов в DN;
- проверка пакетов;
- соблюдение правил политики в пользовательской плоскости;
- передача данных;
- ведение отчетов о проходящем трафике;
- маркировка и обработка трафика в соответствии с QoS в восходящей и нисходящей линиях;
- проверка Uplink трафика;
- буферизация пакетов на линии вниз и инициирование уведомления о наличии данных для доставки на UE;
- отправка и пересылка одного или нескольких «конечных маркеров» на узел NG-RAN источника;
- проксирование ARP (Allocation and Retention Priority);

Функция управления политикой **PCF (Policy Control Function)** включает следующие функции:

- поддержка унифицированной структуры управления политикой сети;
- обеспечение соблюдения правил политики управления функциями;
- обеспечение доступа к информации о подписке в едином репозитории данных UDR (Unified Data Repository).

Функция унифицированного управления данными **UDM (Unified Data Management)** включает поддержку следующих функций:

- генерация учетных данных аутентификации 3GPP AKA;
- управление идентификацией пользователя;
- авторизация доступа на основе данных подписки;
- управление администрированием NF при обслуживании;
- поддержка непрерывного обслуживания (сохранение значений SMF и DNN текущих сеансов);
- поддержка доставки MT (Mobile Terminating) SMS;
- функция законного перехвата;
- управление подпиской;
- управление SMS.

Чтобы обеспечить эту функциональность, UDM использует данные подписки (включая данные аутентификации), которые могут быть сохранены в UDR (Unified Data Repository), и в этом случае UDM реализует логику приложения и не нуждается во внутреннем хранилище данных пользователя; затем несколько разных UDM могут обслуживать одного и того же пользователя в разных транзакциях.

AUSF (Authentication Server Function) поддерживает функции сервера аутентификации.

Прикладная функция **AF (Application Function)** взаимодействует с ядром сети 3GPP для предоставления услуг и поддерживает следующие функции:

- управление маршрутизацией трафика;
- функция доступа к внешним приложениям;
- взаимодействие с PCF для управления политикой.

Прикладные функции, авторизованные оператором, могут иметь разрешение для непосредственного взаимодействия с соответствующими сетевыми функциями NF.

Прикладные функции, не авторизованные оператором для прямого доступа к сетевым функциям, должны иметь связь с NEF (Network Exposure Function) для взаимодействия с соответствующими сетевыми функциями.

Функция выбора сетевого слоя **NSSF (Network Slice Selection Function)** поддерживает следующие функции:

- выбор сетевых слоев, обслуживающих UE;
- определение разрешенного NSSAI и хранение информации о доступных сетевых слоях;
- определение AMF, которые будут использоваться для обслуживания UE или списка кандидатов AMF.

Расположение функциональных узлов в визитной и домашней сетях при роуминге абонентов и при обслуживании через точку доступа в домашней сети показано на рисунке 4.2.

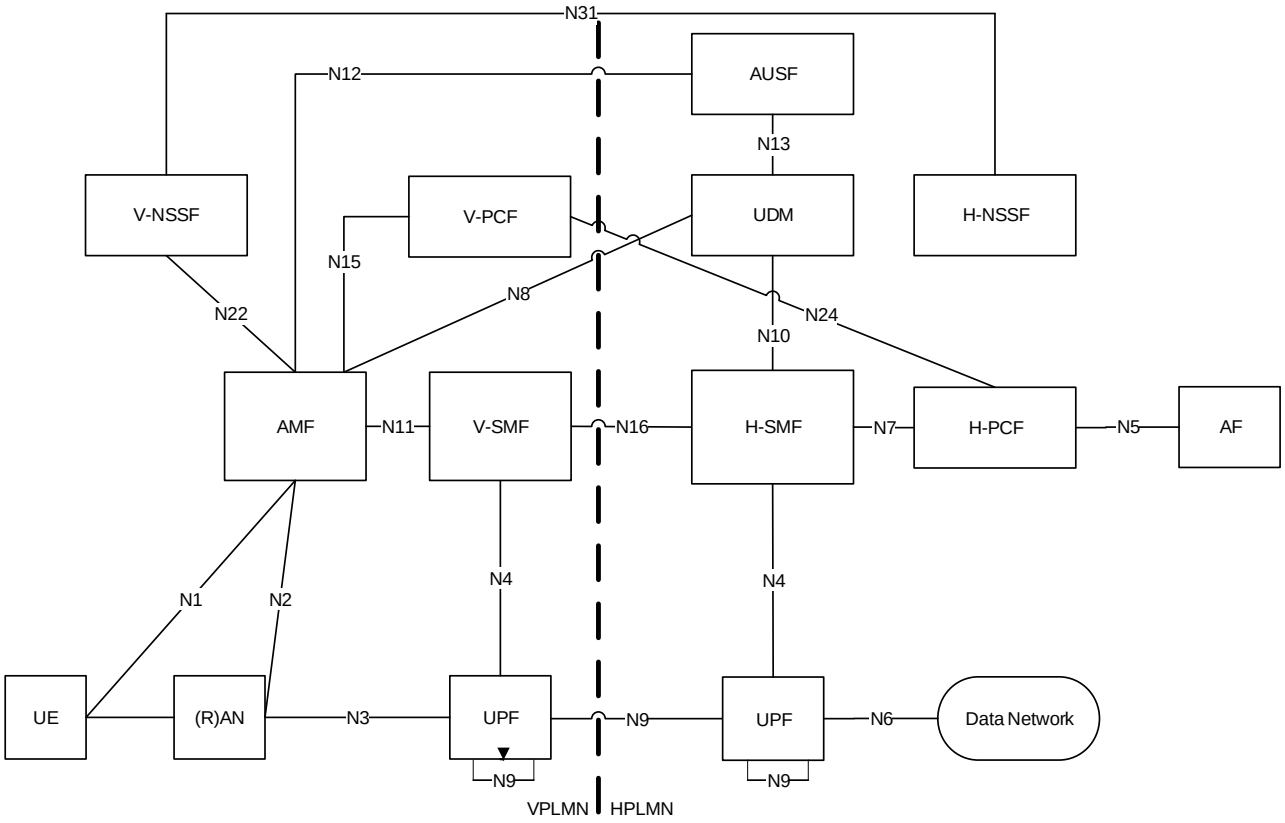


Рисунок 4.2 – Архитектура NR при роуминге при доставке трафика через домашнюю сеть

4.2 Базовая архитектура безопасности в сетях 5G

Структура безопасности в сетях 5G специфицирована в [3GPP TS 33.501; Security architecture and procedures for 5G system]. В сетях NR процедура безопасности выполняется на разных логических уровнях (рисунок 4.3).

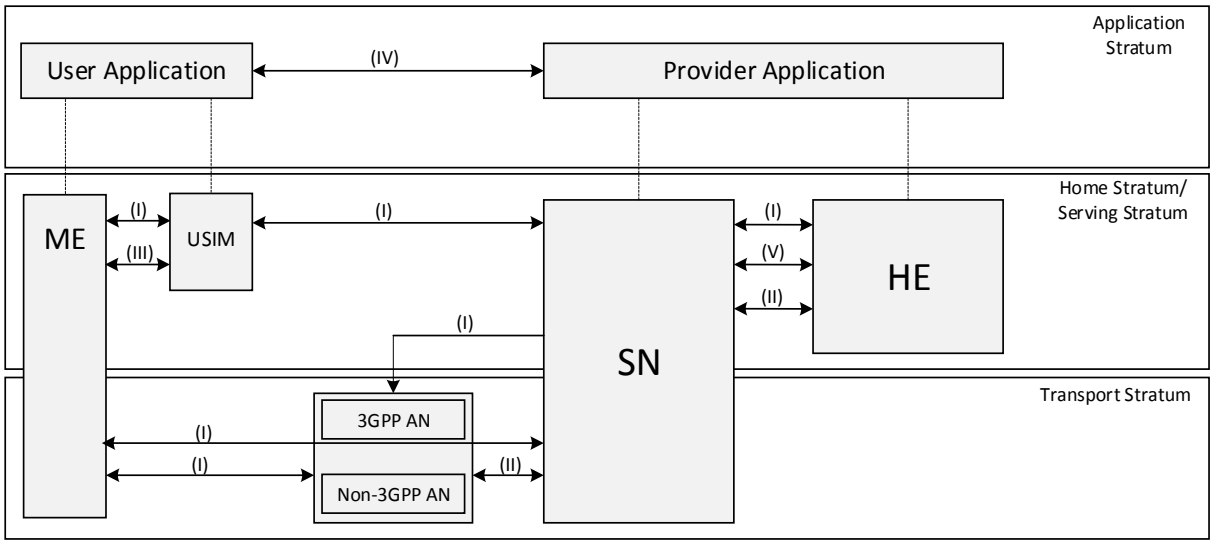


Рисунок 4.3 – Базовая структура безопасности в сетях 5G

Безопасность доступа к сети (I): набор функций безопасности, которые позволяют UE аутентифицировать и безопасно получать доступ к услугам через сеть, включая доступ 3GPP и доступ не-3GPP, и, в частности, защищать от атак на (радио) интерфейсы. Кроме того, он включает в себя доставку контекста безопасности от SN (Serving Network) к AN (Access Network) для безопасности доступа.

Внутрисетевая безопасность (II): набор функций безопасности, которые обеспечивают безопасную передачу пользовательского трафика и сигнализации внутри сети, как визитной, так и домашней HE (Home Environment).

Безопасность домена пользователя (III): набор функций безопасности, обеспечивающих доступ пользователя к мобильному оборудованию.

Безопасность домена приложения (IV): набор функций безопасности, которые позволяют приложениям в пользовательском домене и в домене поставщика безопасно обмениваться сообщениями. Безопасность домена приложения не специфицирована.

Безопасность домена SBA (Service-Based Architecture) (V): набор функций безопасности, который позволяет сетевым функциям архитектуры SBA безопасно обмениваться данными внутри обслуживающего сетевого домена и с другими сетевыми доменами. К таким функциям относятся аспекты безопасности регистрации, обнаружения и авторизации сетевых функций, а также защита интерфейсов на основе услуг.

Функция мониторинга безопасности (VI): набор функций, которые позволяют пользователю получать информацию о том, работает функция безопасности или нет.

4.3 Технологии безопасности в сетях 5G (New Radio)

Концепция безопасности мобильных сетей связи пятого поколения основывается на использовании соответствующих технологий, которые были приняты в стандарте 4G-LTE. На рисунке 4.4 в архитектуре построения ядра сети 5G темным цветом выделены функциональные объекты, реализующие механизмы обеспечения безопасности:

1. Security Anchor Function (SEAF) – якорная функция безопасности;
2. Authentication Server Function (AUSF) – функция сервера аутентификации;

3. Authentication Credential Repository and Processing Function (ARPF) – функция репозитория и обработки учетных данных аутентификации;

4. Security Context Management Function (SCMF) – функция, которая управляет контекстом безопасности;

5. Security Policy Control Function (SPCF) – функция управления политикой безопасности;

6. Subscription Identifier De-concealing Function (SIDF) – функция извлечения идентификатора пользователя.

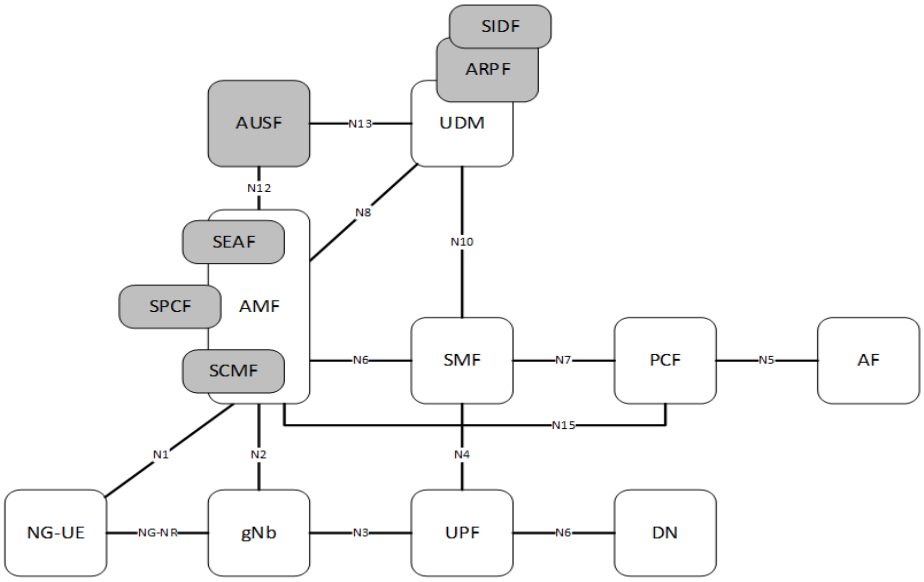


Рисунок 4.4 – Общая архитектура построения ядра сети 5G

На первом этапе развёртывания сетей NR подразумевается совмещение функций SEAF, SCMF и SPCF с модулем управления доступом и мобильностью (AMF); функций ARPF и SIDF с унифицированной базой данных (UDM).

Якорная функция безопасности (SEAF) во взаимодействии с AUSF обеспечивает аутентификацию пользовательского терминала (UE) при его регистрации в сети (attach) для любой технологии доступа.

Функция аутентификации (AUSF) играет роль сервера аутентификации, получая запросы от SEAF и транслируя их в ARPF. Она может быть совмещена с репозиторием учетных данных аутентификации (ARPF).

Репозиторий учетных данных аутентификации (ARPF) обеспечивает хранение персональных секретных ключей (KI) и параметров криптографи-

ческих алгоритмов, а также генерацию векторов аутентификации в соответствии с алгоритмами 5G-AKA или EAP-AKA'.

Функция управления контекстом безопасности (SCMF) обеспечивает управление жизненным циклом контекста безопасности (5G security context).

Модуль управления политикой безопасности (SPCF) обеспечивает согласование и применение политик безопасности в отношении конкретных терминалов пользователя (UE). При этом в расчет принимаются возможности сети, возможности UE и требования конкретной услуги (например, уровни защиты, которые должны быть обеспечены абонентам услуг критических коммуникаций и абонентам беспроводного ШПД могут сильно отличаться).

Применение политик безопасности включает в себя: выбор AUSF, выбор алгоритма аутентификации, выбор алгоритмов шифрования данных и контроля целостности, определение длины и жизненного цикла ключей.

В целом концепция безопасности сетей 5G включает в себя следующие операции:

1. Аутентификацию пользователя со стороны сети.
2. Аутентификацию сети со стороны пользователя.
3. Согласование криптографических ключей между сетью и пользовательским терминалом.
4. Шифрование и контроль целостности сигнального трафика на уровне RRC (между UE и gNb).
5. Шифрование и контроль целостности сигнального трафика на уровне NAS (между UE и AMF).
6. Шифрование и контроль целостности пользовательского трафика (между UE и gNb).
7. Защиту идентификатора пользователя.
8. Защиту интерфейсов между различными элементами сети в соответствии с концепцией сетевого домена безопасности, в том числе защиту интерфейсов N2, N3 и Xn.
9. Изоляцию различных слоев архитектуры Network slicing и определение для каждого слоя собственных уровней безопасности.
10. Защиту сигнального и пользовательского трафика между eNb сети 4G-LTE и gNb сети 5G в рамках "Option 3" сценария миграции 4G к 5G, включая согласование криптографических ключей, шифрование и контроль целостности.
11. Аутентификацию пользователя и защиту трафика на уровне конечных сервисов (IMS, V2X – Vehicle to Everything, IoT).

Для пользователей сетей 5G введены 2 новых идентификатора.

1. Международный постоянный идентификатор подписки абонента – 5G SUPI (Subscription Permanent Identifier). Назначается каждому абоненту сети 5G и хранится в унифицированной базе данных UDM и USIM модуле пользователя. В качестве идентификатора SUPI может выступать международный идентификатор мобильного абонента IMSI (International Mobile Subscriber Identity), либо идентификатор доступа к сети NAI (Network Access Identifier).

2. Скрытый идентификатор пользователя SUCI (Subscription Concealed Identifier). Представляет собой зашифрованную копию международного постоянного идентификатора подписки абонента на услуги (5G SUPI) и позволяет избежать передачу 5G SUPI по сети в открытом виде даже при первичной регистрации пользовательского терминала в сети (Рисунок 4.5).

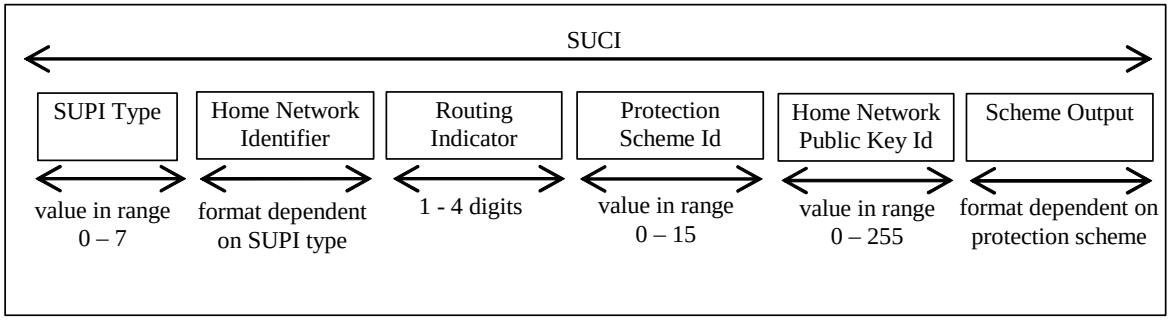


Рисунок 4.5 – Структура SUCI

SUCI состоит из следующих частей:

- тип SUPI, состоящий из значения в диапазоне от 0 до 7. Он идентифицирует тип SUPI;

- идентификатор домашней сети, идентифицирующий домашнюю сеть абонента;

- индикатор маршрутизации, состоящий из 1–4 десятичных цифр, назначенных оператором домашней сети и предоставленных в USIM, которые позволяют вместе с идентификатором домашней сети маршрутизировать сигнализацию сети с SUCI на AUSF и UDM, способные обслуживать абонента;

- идентификатор схемы защиты, состоящий из значения в диапазоне от 0 до 15;

- идентификатор открытого ключа домашней сети, состоящий из значения в диапазоне от 0 до 255. Он представляет открытый ключ, предос-

тавленный HPLMN или SNPN, и используется для идентификации ключа, используемого для защиты SUPI. Это поле данных должно быть установлено в значение 0, когда используется нулевая схема защиты;

- выход схемы, состоящий из строки символов шифрованного идентификатора переменной длины в зависимости от используемой схемы защиты.

3. Для защиты SUPI используется криптографическая схема, основанная на эллиптических кривых (Elliptic Curve Integrated Encryption Scheme – ECIES). Публичный ключ, применяемый для шифрования SUPI, должен храниться в защищенной памяти USIM-карты; закрытый ключ – в функциональном элементе извлечения идентификатора пользователя (SIDF). При этом часть SUPI, содержащая мобильный код страны (MCC) и мобильный код сети (MNC) и задействованная для маршрутизации сигнального трафика не шифруется. 3GPP допускает возможность шифрования SUPI в пользовательском терминале (вариант по умолчанию) и USIM модуле. Сеть оператора связи и пользовательский терминал также должны поддерживать так называемую нулевую схему (null-scheme) при которой защита публичного идентификатора пользователя не осуществляется.

4. Глобальный временный уникальный идентификатор абонента 5G-GUTI (5G Globally Unique Temporary Identifier) назначается модулем управления доступом и мобильностью (AMF) вне зависимости от типа сети доступа (3GPP, non-3GPP). При "выходе в эфир" пользовательский терминал должен использовать именно 5G-GUTI (за исключением первичной регистрации в сети – Initial Attach, а также иных случаев, когда 5G-GUTI отсутствует). Формат 5G-GUTI показан на рисунке 4.6.

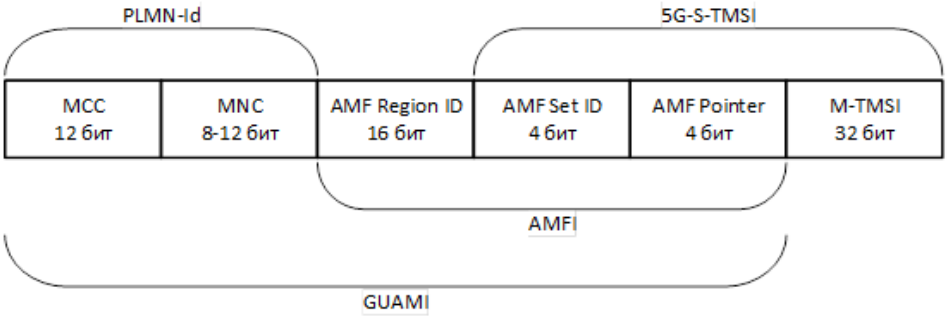


Рисунок 4.6 – Формат 5G-GUTI

Именно взаимная аутентификация абонента и сети является целью процедуры аутентификации и согласования ключей (Authentication and Key Agreement – AKA), а также генерация ключа функции безопасности KSEAF. Впервые сгенерированный ключ KSEAF, можно использовать для формирования нескольких контекстов безопасности, в том числе для 3GPP и non-

3GPP доступа. Release 16 3GPP определил два обязательных метода процедуры аутентификации и согласования ключей: EPS-AKA' и 5G-AKA.

Для аутентификации пользовательского терминала SEAF использует ранее созданный и еще незадействованный вектор аутентификации, либо направляет запрос "Authentication Initiation Request" (5G-AIR) в AUSF, устанавливая в качестве идентификатора пользователя SUCI (в случае первичной регистрации в сети), либо SUPI (при получении от UE валидного 5G-GUTI). Запрос аутентификации (5G-AIR), помимо идентификатора пользователя должен также включать в себя тип доступа (3GPP или non-3GPP), а также имя обслуживающей сети (SN-name).

Далее AUSF проверяет правомочность использования имени обслуживающей сети (SN-name) и если проверка успешна – транслирует полученный запрос в блок унифицированной базы данных (UDM), где функциональным модулем извлечения идентификатора пользователя (SIDF) выполняется расшифровка скрытого идентификатора пользователя (SUCI), после чего репозиторий учетных данных аутентификации (ARPF) осуществляется выбор соответствующего алгоритма аутентификации – 5G-AKA или EAP-AKA' (Extensible Authentication Protocol- Authentication and Key Agreement).

Как и в сетях LTE, в сетях NR обеспечивается взаимная аутентификация абонента и сети и происходит генерация ключей, которые участвуют в процедуре шифрации и защиты целостности передаваемой информации. Для этого в NR есть специально несколько протоколов.

Главным же из них является протокол аутентификации и генерации ключей (AKA). В данном протоколе задействован USIM, устройства абонентского доступа, функциональные узлы обслуживания и домен сети.

Особенностью протокола AKA является то, что функциональные узлы ядра сети, использующиеся в нем, виртуальны, как и другие функциональные узлы сети NR.

На рисунке 4.7 показан первый этап процедуры: запуск процедуры аутентификации.

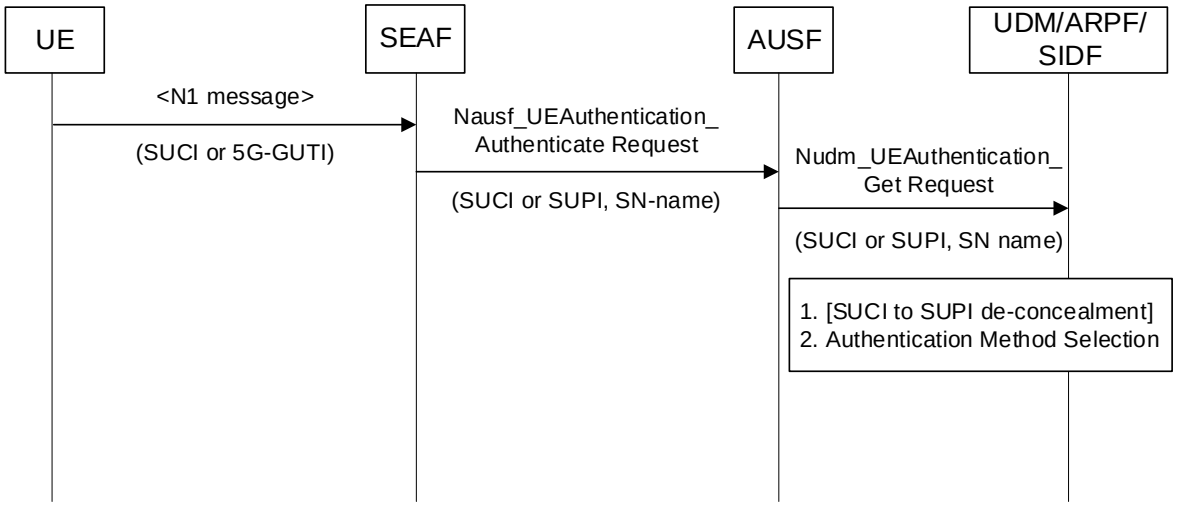


Рисунок 4.7 – Запуск процедуры аутентификации

Сама процедура аутентификации по алгоритму 5G-AKA приведена на рисунке 4.8, где

HE AV – вектор аутентификации, состоящий из RAND, AUTN, XRES* и K_{AUSF},

SE AV – вектор аутентификации, где XRES* заменено на HXRES* и K_{AUSF} на K_{SEAF}.

Получив команду *Authentication Request*, USIM аутентифицирует сеть и отсылает ответ RES* для аутентификации абонента, которую осуществляют последовательно в SEAF и в AUSF. После успешной аутентификации абонента AUSF отсылает в SEAF системный идентификатор абонента 5G SUPI и начинается процесс генерации ключей шифрации и защиты подлинности.

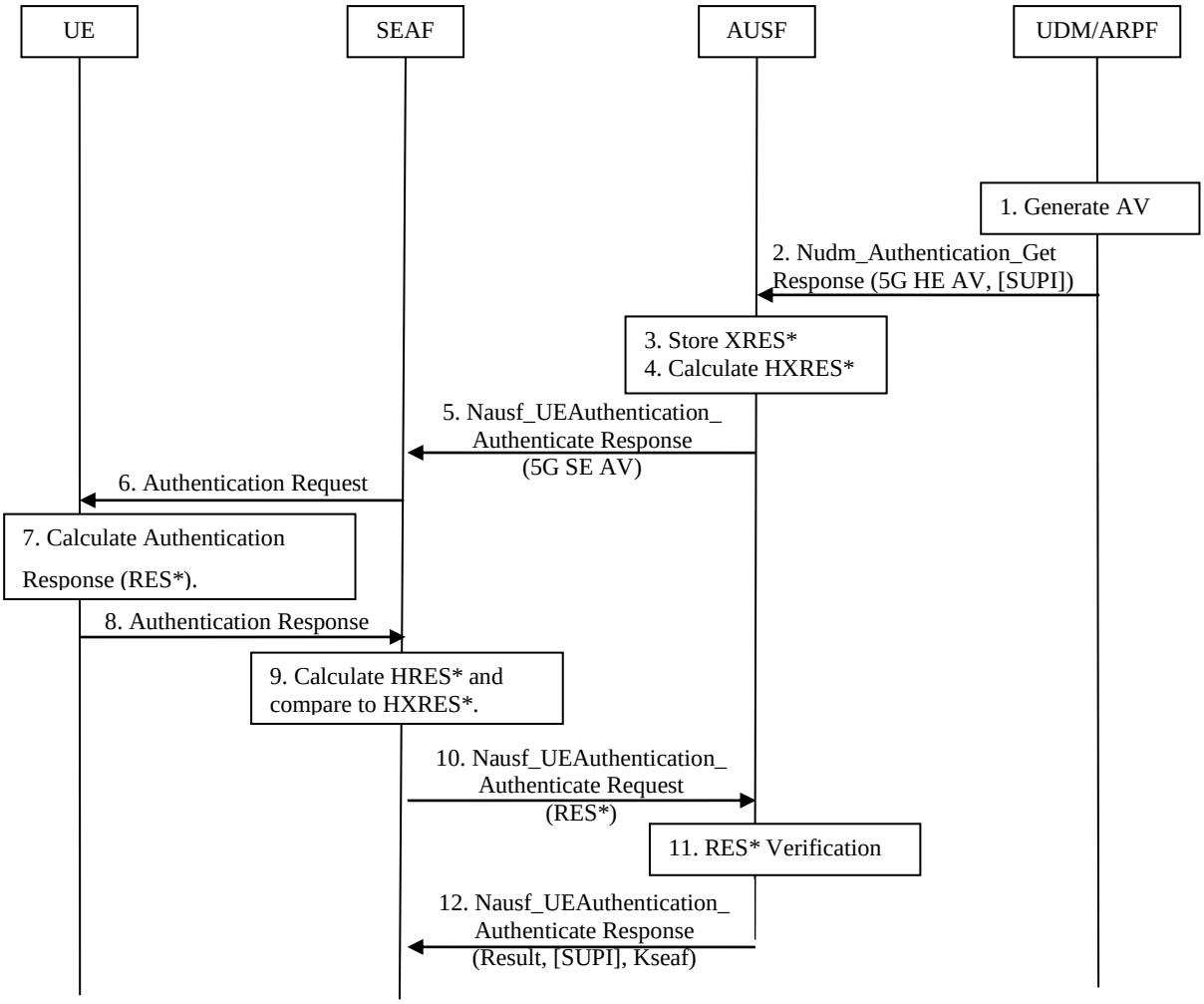


Рисунок 4.8 – Процедура аутентификации по алгоритму 5G-AKA

На рисунке 4.9 представлена иерархия ключей в сети 5G NR, а на рисунке 4.10 генерация ключей шифрации и защиты подлинности для UE.

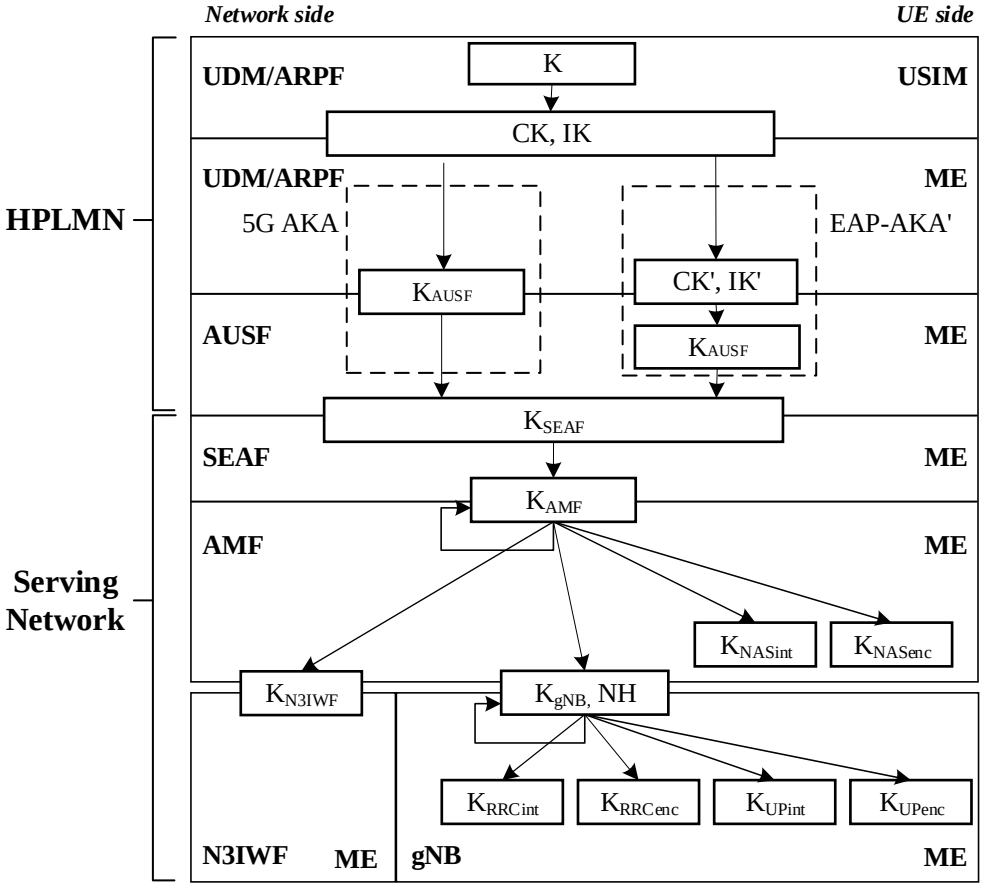


Рисунок 4.9 – Иерархия ключей в 5G NR

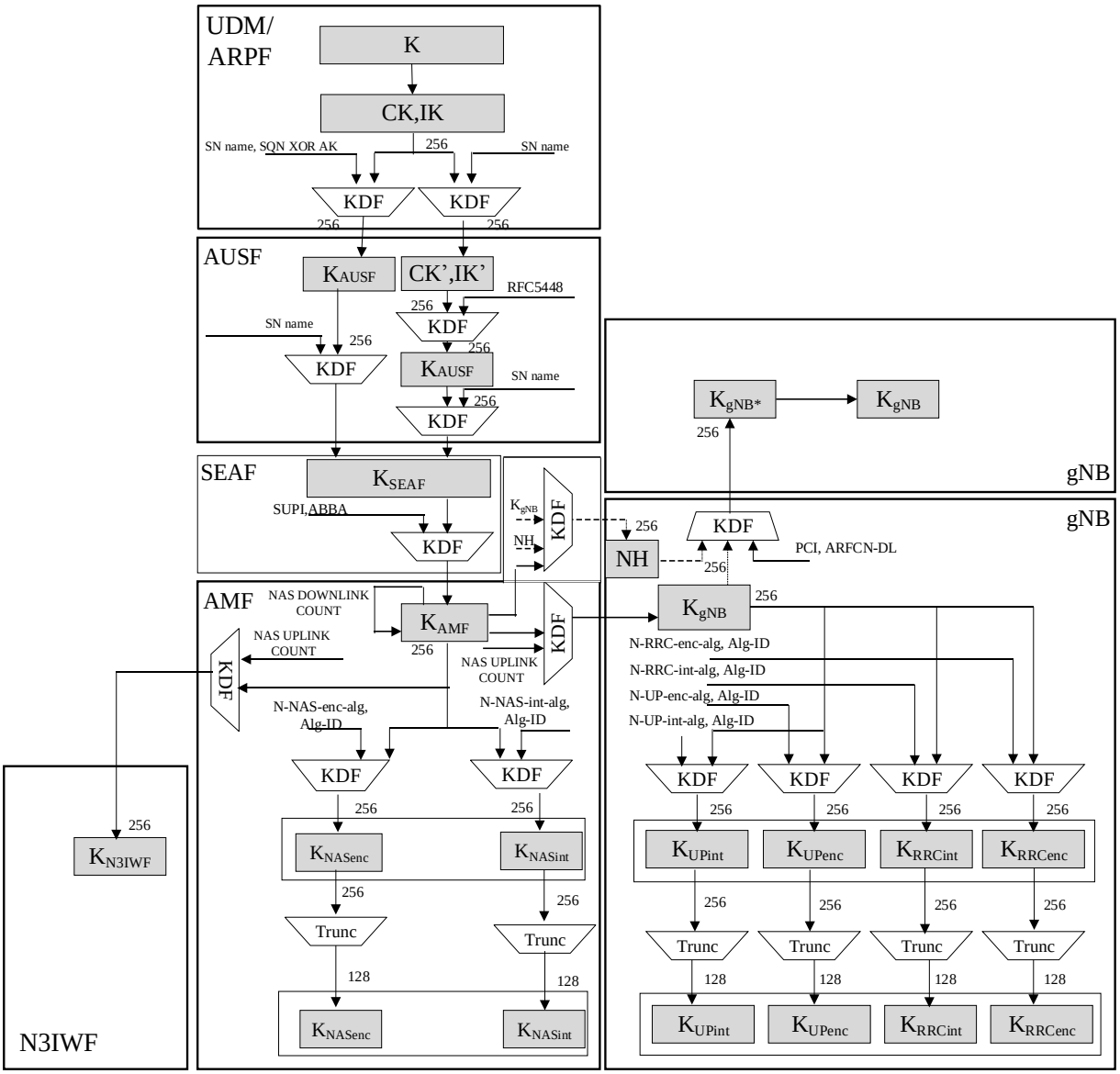


Рисунок 4.10 – Генерация ключей для UE