# Конструктивно-технологическое обеспечение средств связи

Сети стандарта GSM/GPRS

# Общие аспекты безопасности 2G

- Конфиденциальность пользовательского идентификатора (IMSI);
- Аутентификация пользовательского идентификатора (IMSI);
- Конфиденциальность пользовательских данных на физическом уровне;
- Конфиденциальность передаваемых пользовательских данных;
- Конфиденциальность сигнальной информации

# Безопасность сети GSM

- Основу системы безопасности GSM составляют три алгоритма:
  - A3 - алгоритм аутентификации, защищающий телефон от клонирования;
  - A8 - алгоритм генерации криптоключа, по сути дела однонаправленная функция, которая берет фрагмент выхода от A3 и превращает его в сеансовый ключ для A5;
  - A5 - собственно алгоритм шифрования оцифрованной речи для обеспечения конфиденциальности переговоров. В GSM используются две основные разновидности алгоритма: A5/1 и A5/2

- Мобильные станции (телефоны) снабжены смарт-картой, содержащей A3 и A8, а в самом телефоне имеется ASIC-чип с алгоритмом A5. Базовые станции также снабжены ASIC-чипом с A5 и "центром аутентификации", использующим алгоритмы A3-A8 для идентификации мобильного абонента и генерации сеансового ключа.

# Рекомендации по безопасности (etsi.org)

| | | |
|---|---|---|
| GSM 02.09 | Аспекты секретности | Определяет характеристики безопасности, применяемые в сетях GSM. Регламентируется их применение в подвижных станциях и сетях |
| GSM 03.20 | Секретность, связанная с функциями сети | Определяет функции сети, необходимые для обеспечения характеристик безопасности, рассматриваемых в рекомендациях GSM 02.09 |
| GSM 03.21 | Алгоритмы секретности | Определяет криптографические алгоритмы в системе связи |
| GSM 02.17 | Модули подлинности абонентов (SIM) | Определяет основные характеристики модуля SIM |

# Идентификационный модуль абонента (SIM)

- Ключевой особенностью стандарта GSM является Subscriber Identity Module – SIM-карта. SIM-карта содержит всю информацию об условиях абонирования и вставляется в ME, чтобы дать возможность абоненту пользоваться услугами сети GSM. Без SIM-карты MS также может работать, но только в режиме экстренных вызовов.
- SIM-карта хранит в себе три вида абонентской информации:
  - **Фиксированные данные:** данные, которые постоянно хранятся в карте и прошиваются на IMSI, ключ аутентификации, алгоритмы для обеспечения безопасности связи.
  - **Временные данные о сети:** LA, запрещённые PLMN.
  - **Данные, касающиеся услуг.**

# Требования к информации, хранящейся в SIM

## Обязательные данные

- Административная информация: описывает режим работы SIM, например, обычный режим или режим утвержденного типового образца (тестовый режим).
- Идентификация IC карты: уникальная информация, идентифицирующая SIM.
- **ICCID** - международный идентификатор карты. Это уникальный физический номер карты (тип серийного заводского номера). Этот номер печатается на пластмассовой части чипа.
- **IccID**=89701+99+010000000001 – всего 19 цифр;
- **Расшифровка:**
  расшифровка основана на рек. **ITU-T E.118**:
  **89** - пластиковая карта для телекоммуникаций
- **7** - Россия (рек. **ITU-T E.164**)
  **01** - федеральная сеть GSM-900
  **99** – сеть оператора
- **01** - регион

# Необязательные данные SIM

- International Mobile Subscriber Identity (**IMSI**): идентификационный номер, используемый сетью для идентификации абонента. IMSI=MCC+MNC+MSIN=250+99+91$X_1 \ldots X_8$;
- Информация о местоположении: LAI, которая периодически обновляется.
- Ключ шифрования ($K_c$)
- Порядковый номер ключа шифрования
- Последние частоты, использованные при выборе сот
- Запрещённые PLMN
- Языковая поддержка: язык, выбранный абонентом

Информация о местоположении, $K_c$ и порядковый номер ключа шифрования $K_c$ обновляются при обслуживании каждого входящего соединения.

Кроме того SIM позволяет администрировать вызовы и предоставлять доступ к данным в соответствии со следующими требованиями обеспечения безопасности связи:

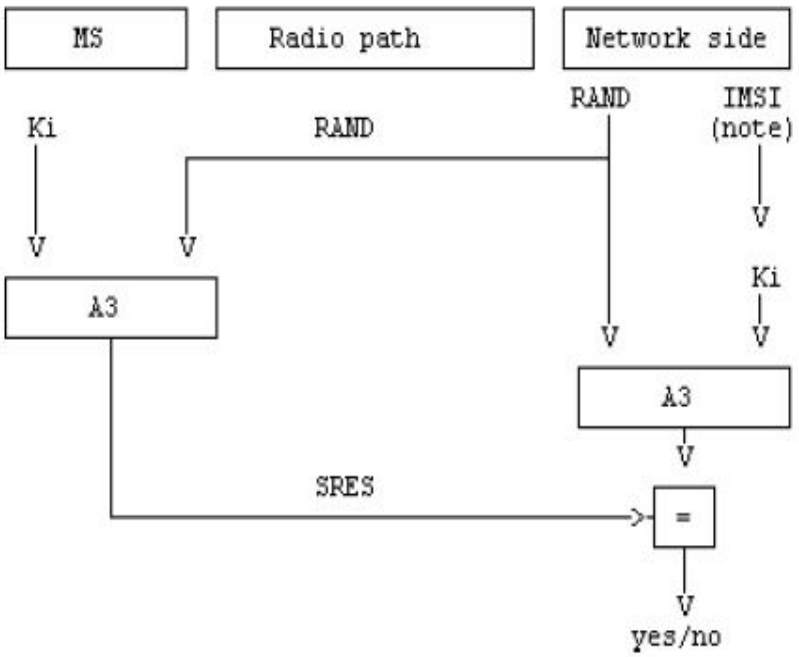
- Personal Identification Number (PIN) – PIN код
- Индикатор активации / деактивации PIN кода
- Счетчик количества неправильно введенных PIN кодов
- PIN Unlock Key (PUK) - PUK код
- Счетчик количества неправильно введенных PUK кодов
- Ключ аутентификации абонента (Ki)

# Аутентификация

- Выполняется, как правило, в 3х случаях:

1. Начальная стадия звонка
2. Процедура Location Update
3. Получение доступа к доп.сервисам сети

# Аутентификация (принцип)




- Сеть передает случайный номер (RAND) на подвижную станцию.

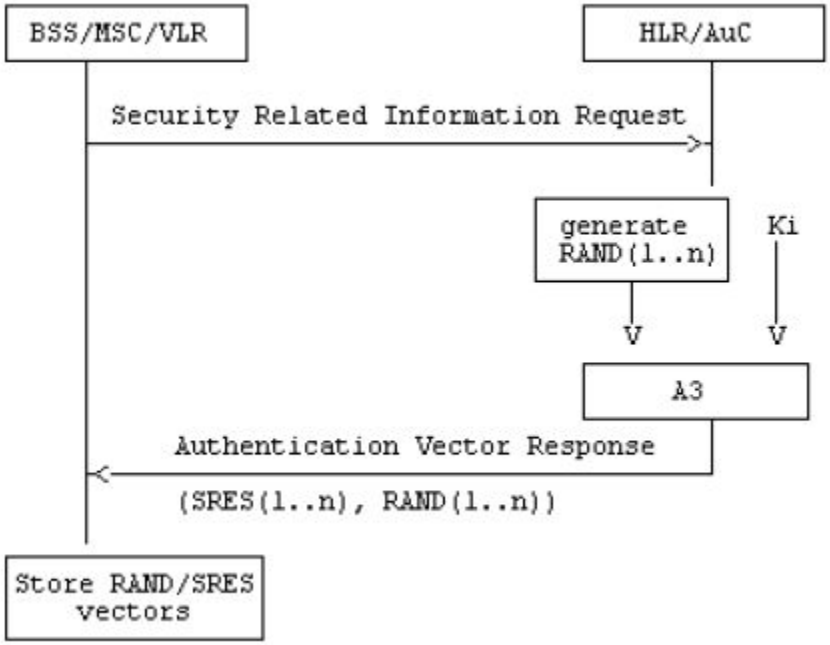
  Подвижная станция определяет значение отклика (SRES), используя RAND (128), Ki и алгоритм A3:

  SRES = Ki [RAND] (32).

  Подвижная станция посылает вычисленное значение SRES в сеть, которая сверяет значение принятого SRES со значением SRES, вычисленным сетью.

  Если оба значения совпадают, подвижная станция может осуществлять передачу сообщений.

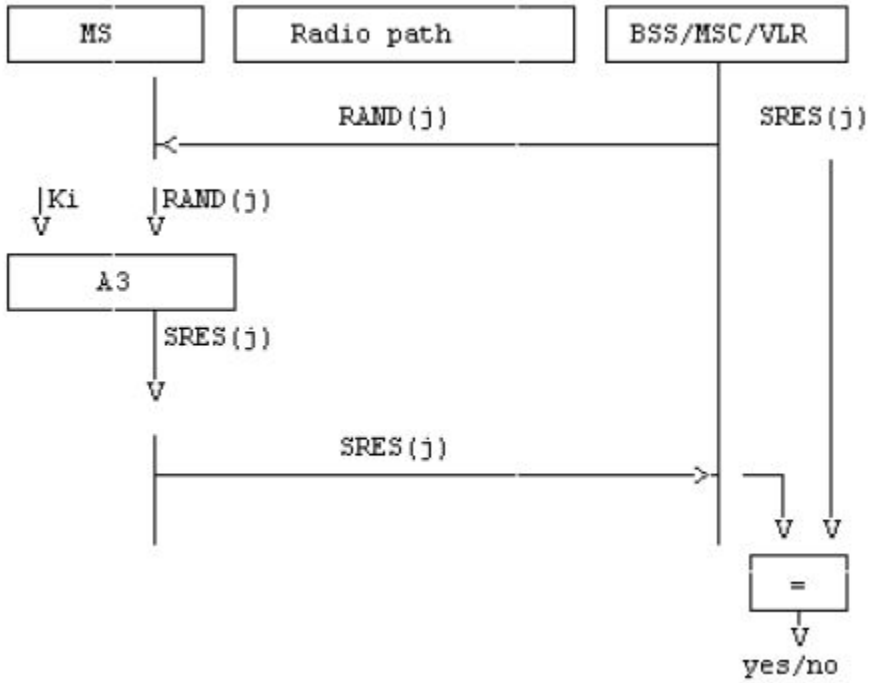
# Общая процедура аутентификации



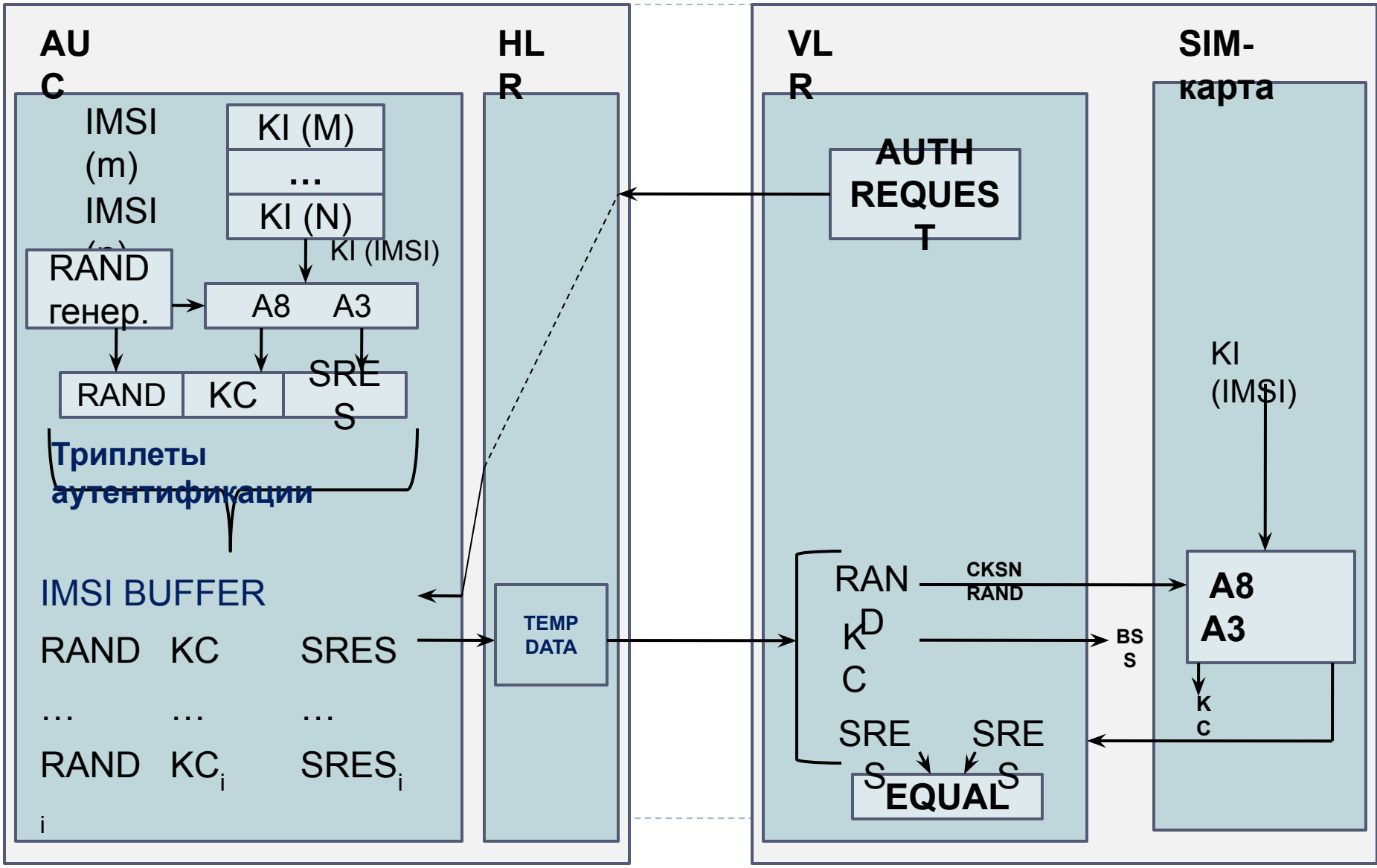

- Когда необходимо BSS/MSC/VLR делает запрос в HLR/AuC, , в котором хранится информация об АТ
- Информация представляет собой случайный номер RAND и контрольную сумму SRES, которые получены с применением алгоритма A3 для каждого случайного значения RAND и ключа Ki.
- RAND и Ki хранятся в VLR.

# Общая процедура аутентификации

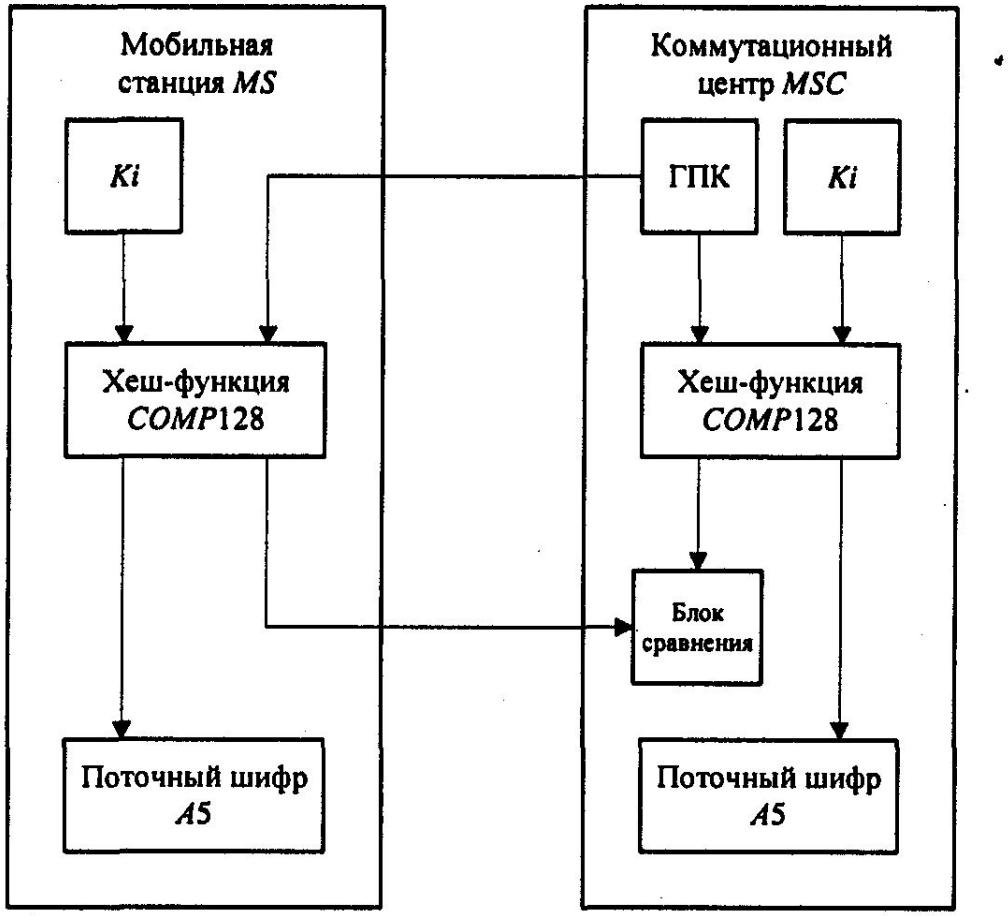
Когда MSC/VLR выполняет аутентификацию, включающую в себя процедуру обновления местоположения в рамках VLR, он посылает случайный номер RAND (128 бит), который комбинируется с Ki, шифруется алгоритмом A3 и сверяет полученный SPES (32 бит) с SRES AuC.



# АУТЕНТИФИКАЦИЯ



# Схема аутентификации с помощью алгоритма *A3*




- На стороне сети два входных параметра (RAND и Ki) и выходной параметр (SRES) должен использовать следующие форматы:
  - длина Ki: 128 бит;
  - длина RAND: 128 бит;
  - длина SRES: 32 бит.
  - «время жизни» алгоритма A3 должно быть меньше чем 500 мс.

# Модификации алгоритма COMP128

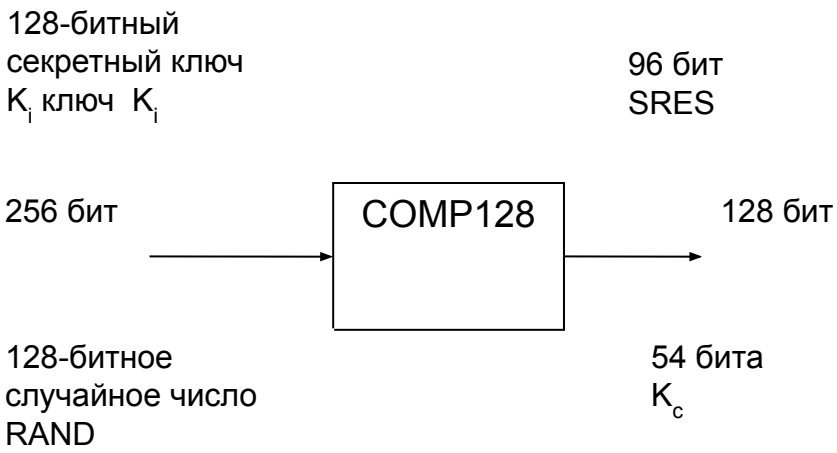



**Схема работы хеш-функции COMP128**

Алгоритмы *A3, A8* в своей работе базируются на крипто хеш – функции COMP128. структура этого алгоритма называется «формой бабочки». Состоит из 8 раундов в каждом раунде по 5 итераций

- COMP128 v.1 и COMP128 v.2 (вырабатывают 54 битный ключ),);
- COMP128 v.3 вырабатывает 64 битный сеансовый ключ;
- COMP128 v.4 данная версия основана на стандарте 3GPP алгоритме MILENAGE, который использует AES (RIJNDAEL).

# Алгоритм A8

- На стороне АТ алгоритм A8 хранится в SIM-карте (GSM 02.17).
- На стороне сети алгоритм A8 взаимодействует с алгоритмом A3.
- Входные параметры (RAND и Ki)  и выходные параметры (Kc) должны иметь следующие форматы:
  - длина Ki: 128 бит;
  - длина RAND: 128 бит;
  - длина Kc: 64 бит.

# Спецификация алгоритма A5

- Для двух входных параметров (COUNT и Kc) и выходных параметров (BLOCK1 и BLOCK2) должны использоваться следующие форматы:
  - длина Kc: 64 bits;
  - длина COUNT: 22 bits;
  - длина BLOCK1: 114 bits;
  - длина BLOCK2: 114 bits.
- Время получения параметров BLOCK1 и BLOCK2 должно быть меньше чем длительность TDMA кадра, т.е. 4.615 мс.

# Распределение ключей и идентификаторов в аппаратных средствах системы связи GSM

| NN п. п. | **Аппаратные средства** | **Вид секретной информации** |
|---|---|---|
| 1 | Подвижная станция (без SIM) | A5 |
| 2 | Модуль подлинности абонента (SIM) | A3; A8; IMSI; Ki; TMSI/LAI; Kc/CKSN |
| 3 | Центр аутентификации (AUC) | A3; A8; IMSI/Ki |
| 4 | Регистр местоположения (HLR) | Группы IMSI/RAND/SRES/Kc |
| 5 | Регистр перемещения (VLR) | Группы IMSI/RAND/SRES/Kc, IMSI/TMSI/LAI/Kc/CKSN |
| 6 | Центр коммутации (MSC) | A5, TMSI/IMSI/Kc |
| 7 | Контроллер базовой станции (BSC) | A5, TMSI/IMSI/Kc |

# Содержание

1. Безопасность доступа в UMTS. Взаимная аутентификация. Шифрование в сети UTRAN. Дополнительные средства обеспечения безопасности в системах 3GPP. Аспекты безопасности на уровне системы и сети.

# Рекомендации

- TS 22.101: Аспекты службы; принципы службы
- TS 33.102: Безопасность 3G; архитектура безопасности
- TS 33.106: Требования к санкционированному перехвату
- TS 33.107: Безопасность 3G; архитектура и функции санкционированного перехвата
- TS 33.108: Безопасность 3G; интерфейс передачи разговора для санкционированного перехвата (LI)
- TS 33.200: Безопасность сетевого домена – MAP
- TS 33.203: Безопасность 3G; безопасность доступа для служб, базирующихся на протоколе IP
- TS 33.210: Безопасность; безопасность сетевого домена (NDS); безопасность уровня IP-сети
- TS 35.205, .206, .207, .208 и .909: Безопасность 3G; спецификация комплекта алгоритмов MILENAGE: пример комплекта алгоритмов для функций аутентификации и генерации ключа 3GPP f1, f1*, f2, f3, f4, f5 и f5*; (.205: Общий; .206: Спецификация алгоритма; .207: Тестовые данные разработчика; .208: Тестовые данные проверки соответствия проекту; .909: Резюме и результаты проектирования и оценки) СИК

# Угрозы конфиденциальности сети подвижной связи 3G

- использование недекларированных возможностей программно-технических средств сети связи 3G;
- несанкционированный доступ к информационным ресурсам сети связи 3G из внешних сетей;
- преодоление мер криптозащиты данных при передаче в эфире и по сети;
- организация нелегального транзитного узла передачи данных (man-in-the-middle) и манипуляции с обрабатываемым таким узлом трафиком;
- внедрение вредоносных программ (вирусов, троянских программ, "червей");
- навязывание пользователю нежелательной информации (Спама);
- рекламное ПО, загружаемое и устанавливаемое на мобильное устройство без ведома пользователя и периодически отображающее рекламную информацию;
- получение обманным путем услуг сотовой связи без цели их надлежащей оплаты;
- несанкционированный доступ к ПО серверов и рабочих станций, а так же сервисным устройствам сети с подменой идентификатора или сетевого адреса;
- перехват сигналов в линиях связи;
- перехват и анализ сетевого трафика;
- несанкционированный перехват информации за счет ПЭМИН от технических средств, наводок по линиям электропитания, наводок по посторонним проводникам, перехват по акустическому каналу, перехват за счет нарушения установленных правил доступа (взлом);
- несанкционированный запуск приложений в ИВС и на оборудовании сети;
- несанкционированное изучение топологии защищенного объекта, определение запущенных приложений, служб и открытых портов;
- несанкционированный доступ к режиму конфигурирования оборудования;
- несанкционированный доступ к информационным ресурсам группового пользования с правами администратора и др.

# Общая архитектура безопасности

- **Защита доступа абонента к сети:** безопасный доступ к сети 3G на уровне радиоинтерфейса. Для обеспечения конфиденциальности доступа в сетях 3-го поколения в отличие от сетей 2-го поколения используется взаимная аутентификация абонента и сети (т. е. и абонент идентифицируется сетью, и сеть идентифицируется по отношению к абонентскому терминалу).
- **Защита доступа к внутренней сети,** т. е. комплекс мер, который позволяет элементам сети оператора безопасно обмениваться сигнальной информацией внутри сети (в данном случае - внутри именно проводной сети). Этот комплекс мер противостоит угрозе несанкционированного доступа к оборудованию сети и в достаточной мере осуществляется производителями сетевого оборудования и операторами связи.
- **Защита доступа к абонентскому оборудованию.** Сюда относятся меры, обеспечивающие безопасный доступ к абонентскому терминалу. Это может быть система авторизации, как на базе SIM-модуля, так и на базе терминального оборудования с возможным снятием биометрических показателей абонента. Вся ответственность за осуществление этих мер ложится на пользователя оборудования.
- **Защита интерфейсов приложений.** На этом уровне рассматривается комплекс мер по обеспечению безопасного обмена сообщениями приложений на стороне пользователя и на стороне оператора.
- **Прозрачность уровней обеспечения безопасности и возможность их изменения.** Сюда относится комплекс мер, который позволяет абоненту получать информацию о том, какие уровни безопасности в настоящий момент работают, а какие нет, и соответственно изменять этот список. Кроме этого, использование или предоставление услуг должно зависеть от задействованных мер обеспечения безопасности.

Меры, перечисленные в первых двух пунктах, присущи не только системе безопасности мобильной связи 3-го поколения. Комплексы этих мер регламентируются стандартами и гарантируются производителями сетевого и абонентского оборудования. Поэтому в целом учитывать их влияние стоит только при выборе того или иного стандарта мобильной связи.

Четвертый и пятый комплексы мер специфичны для сетей 3-го поколения, и для их полноценного осуществления уже необходимо взаимодействие трех сторон: абонента, оператора и поставщика услуги (разработчика приложения).

# Уязвимые узлы сетей

- Абонентское оборудование, т.е.  сотовые телефоны, коммуникаторы, смартфоны, ноутбуки
- Радиолинк между мобильным аппаратом и сотовой базовой станцией
- Интерфейсы к другим мобильным сетям - в сетях GPRS/UMTS это интерфейс Gp
- Интерфейсы к сетям передачи данных - Интернету или частным сетям; в GPRS/UMTS сетях за это отвечает интерфейс Gi.
- Элементы управления и технические модули, такие как Home Location Register (HLR), который хранит данные об абоненте (интерфейс Ga в сети GPRS/UMTS).
- Сервера приложений (application servers) и сервера с контентом (content servers)
- Между- и внутрисетевые сигнальные протоколы и интерфейсы.

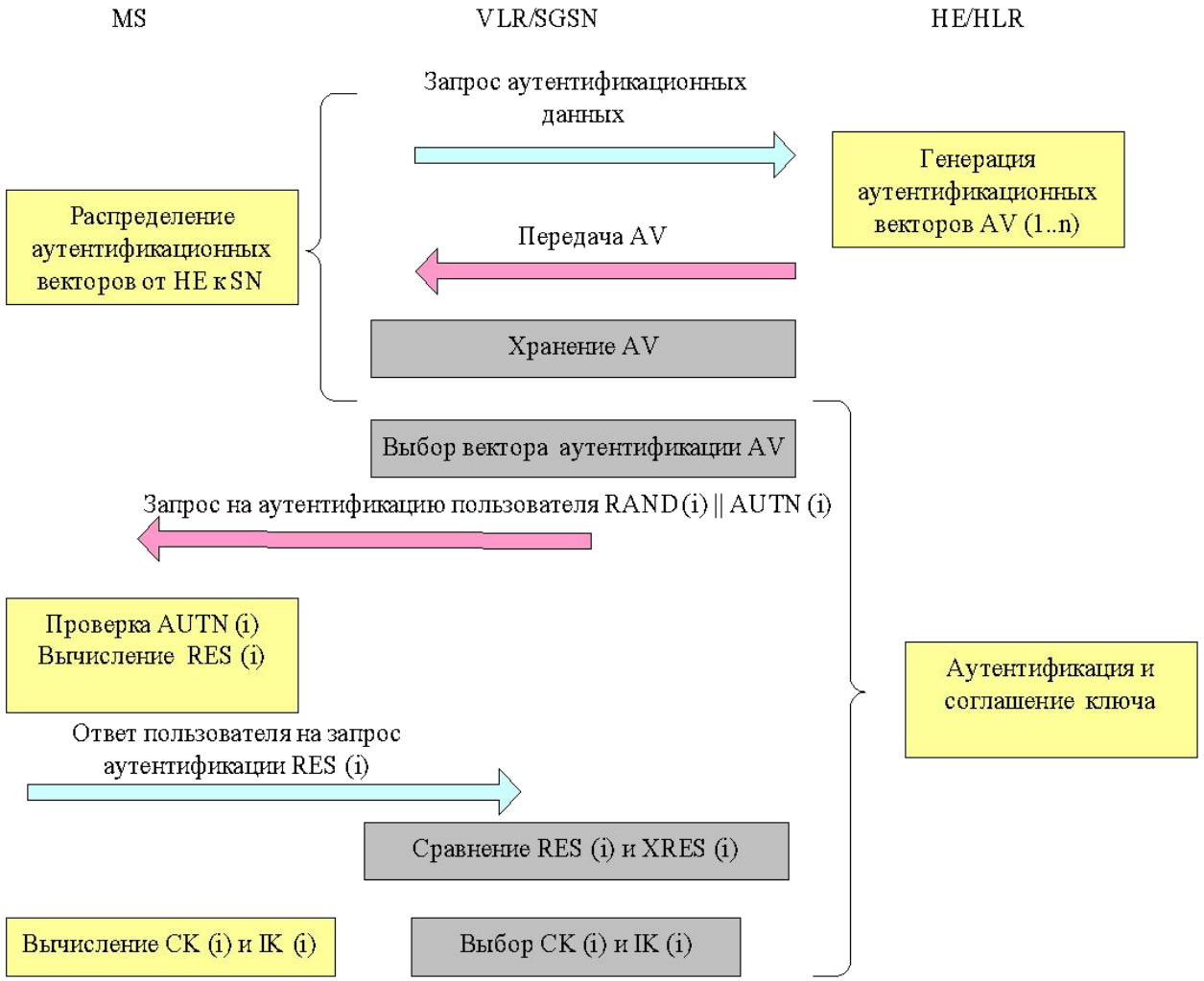
# Средства защиты UMTS

- Внедрена взаимная аутентификация AKA (Authentication and Key Agreement), которая включает в себя:
  - аутентификацию домашнего окружения по отношению к пользователю;
  - соглашение о ключе целостности (IK) между пользователем и обслуживающей сетью;
  - взаимное подтверждение “свежести” ключей шифрования (СК) и аутентификации между пользователем и обслуживающей сетью.
- Разработаны и внедрены алгоритмы шифрования с ключами большей длины, в основу которых положен модифицированный поточный шифр.
- Обеспечена целостность данных путем использования алгоритмов проверки целостности и аутентификация источника передачи данных.
- Разработаны механизмы для поддержания сетевой и межсетевой защиты.
- Разработаны механизмы целостности IMEI.
- Разработаны механизмы для отражения мошеннических действий в режиме роуминга.
- Введена индикация о статусе шифрования и о доступном уровне безопасности (2G, 3G).
- Обеспечена возможность конфигурируемости, которая предполагает следующее:
- пользователь определяет те средства защиты, которые должны быть включены для определенных услуг;
  - включение/выключение аутентификации “Пользователь ↔ USIM”;
  - прием/отказ входящих незашифрованных вызовов;
  - включение/выключение режима незашифрованных вызовов;
  - прием/отказ использования определенных алгоритмов шифрования.

# Функции, обеспечивающие безопасность информации в сетях 3G

- **Аутентификация** - процесс проверки подлинности личности (пользователя) с помощью секретного ключа. Аутентификация связана с применением модуля USIM. Он содержит персональный идентификатор абонента (PIN-код), персональный код разблокировки (PUK-код), индивидуальный ключ аутентификации пользователя, индивидуальный алгоритм его аутентификации, алгоритм для вычисления ключа шифрования. Для защиты USIM-карты от несанкционированного ее применения необходимо проводить процедуру ее блокирования. Пока USIM-карта заблокирована, пользоваться мобильным терминалом невозможно.
- **Конфиденциальность пользователя** - процесс, осуществляемый посредством использования специальных временных идентификаторов, сменяемых по мере перемещения пользователя от соты к соте.
- **Конфиденциальность передаваемых данных**. Ее реализуют посредством шифрования сведений на участке между мобильным терминалом и сетью. Шифрование информации - это процесс преобразования ее в недоступную для постороннего форму криптографическим методом. В сетях сотовой связи такую операцию производят с помощью программных средств.
- **Целостность данных** - невозможность скрытного изменения данных злоумышленником в процессе их передачи. Кроме того, пользователь услугами в сетях сотовой связи третьего поколения может на своем терминале производить выбор операций по обеспечению безопасности используемой им информации. К таким операциям относят: включение обязательной аутентификации при доступе пользователя к USIM-карте; запрещение доступа незашифрованных входных вызовов; выбор конкретных алгоритмов шифрования и др.

# Механизм AKA



# В состав  AV входят:

- RAND;
- XRES;
- CK;
- IK;
- AUTN (Authentication token - маркер аутентификации).

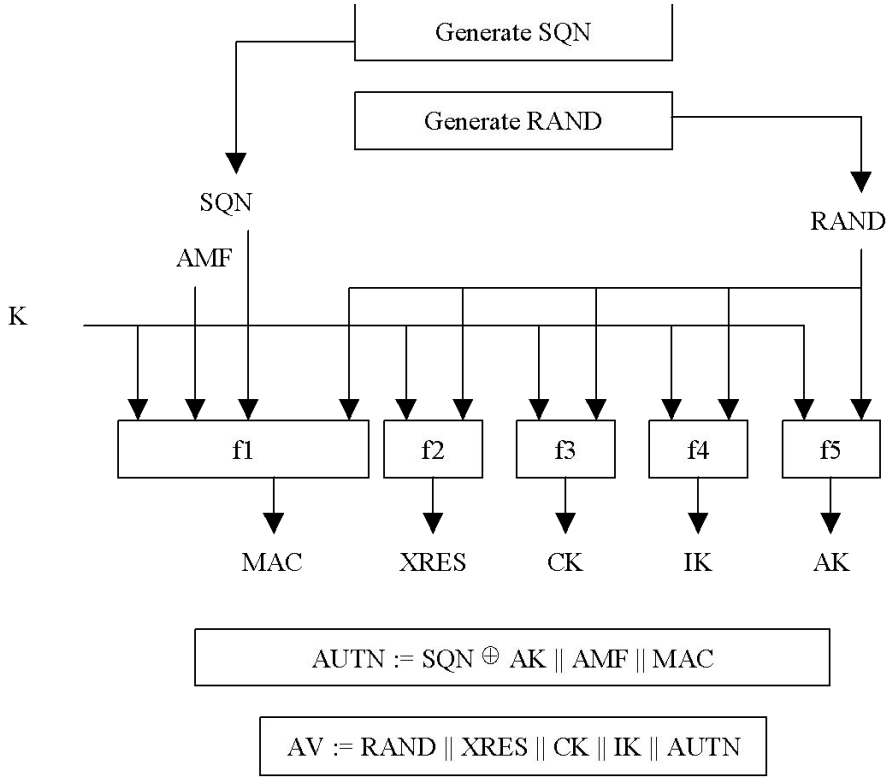
# генерируемые компоненты

- значение компоненты MAC = $f1_K$(SQN || RAND || AMF), где AMF (Authentication Management Field - Поле управления  аутентификацией);
- значение компоненты XRES = $f2_K$ (RAND);
- значение компоненты CK = $f3_K$ (RAND);
- значение компоненты IK = $f4_K$ (RAND);
- значение ключа анонимности AK = $f5_K$ (RAND).

# Функции AKA

- ***f1*** **-** функция используется для вычисления аутентификационного сообщения MAC (Message authentication code – код аутентификационного сообщения);
- ***f1**** - функция используется для вычисления аутентификационного сообщения MAC-S;
- ***f2*** - функция используется для вычисления аутентификационных сообщений RES (RESponse - ответ) и XRES (Expected user RESponse – ожидаемый ответ);
- ***f3*** **-** функция генерации ключа шифрования CK (Ciphering Key – ключ шифрования);
- ***f4*** - функция генерации ключа целостности IK (Integrity key – ключ целостности);
- ***f5*** - функция генерации ключа анонимности AK (Anonymity Key – ключ анонимности) в нормальном режиме;
- ***f5**-*** функция генерации ключа анонимности AK в режиме ресинхронизации

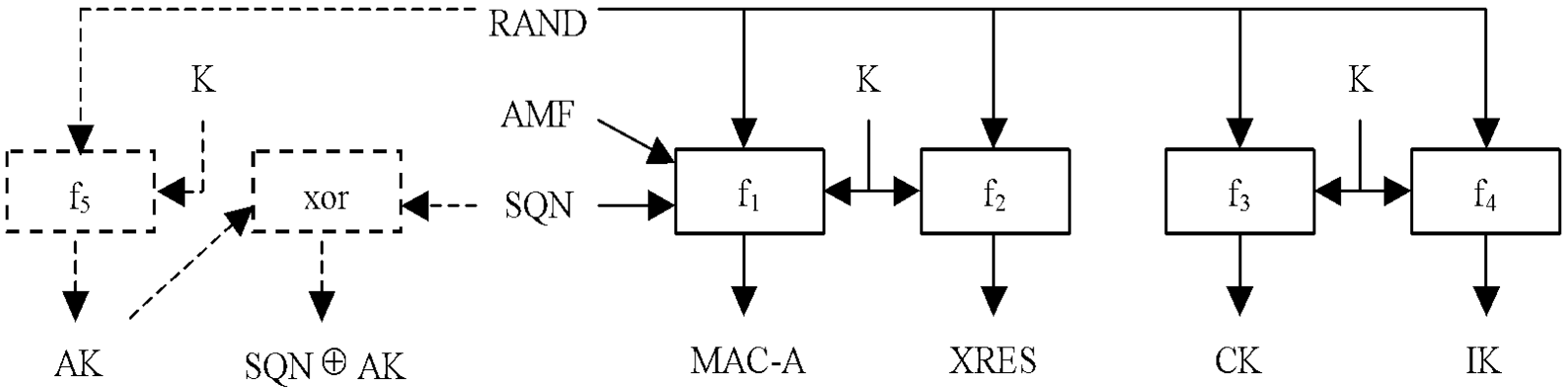
# Генерация пятикомпонентных аутентификационных векторов



# Параметры аутентификации

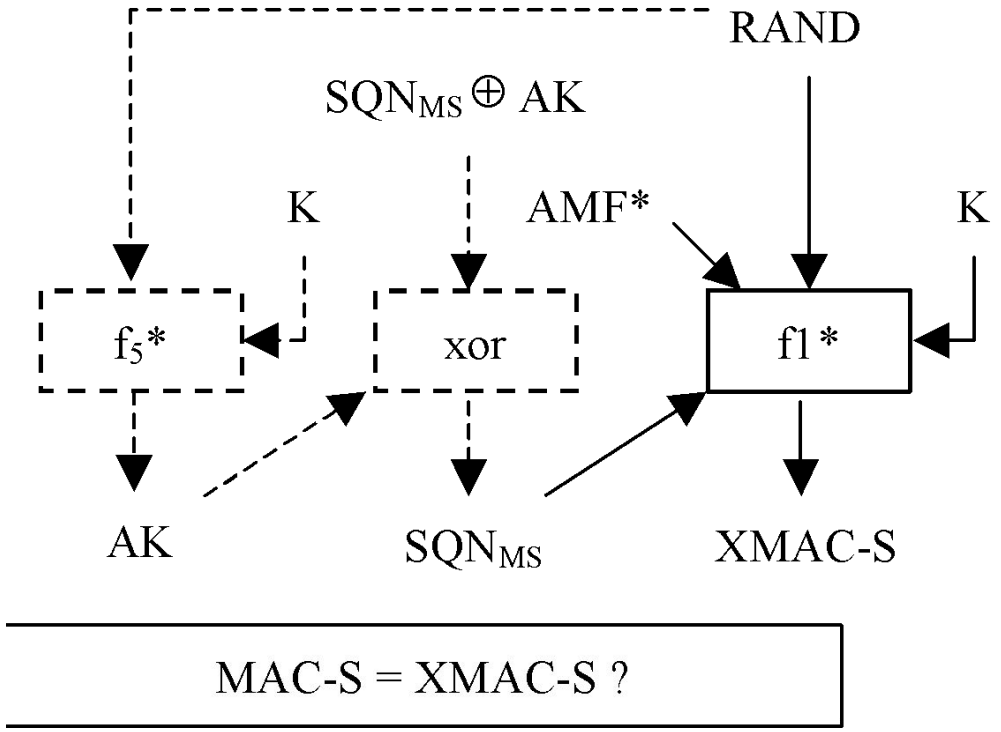
- Ключ аутентификации K - 128 бит
- Длина случайной последовательности RAND - 128 бит
- Последовательность номеров SQN - 48 бит
- Анонимный ключ AK - 48 бит
- Длина поля управления аутентификацией - 16 бит
- Длина MAC-кодов сообщения аутентификации AUTN и MAC-S в AUTS - 64 бит
- Ключ шифрования CK - 128 бит
- Ключ целостности IK - 128 бит
- Длина отклика аутентификации RES - переменная длина 4-16 октетов.

# Генерация пятикомпонентных векторов в AuC

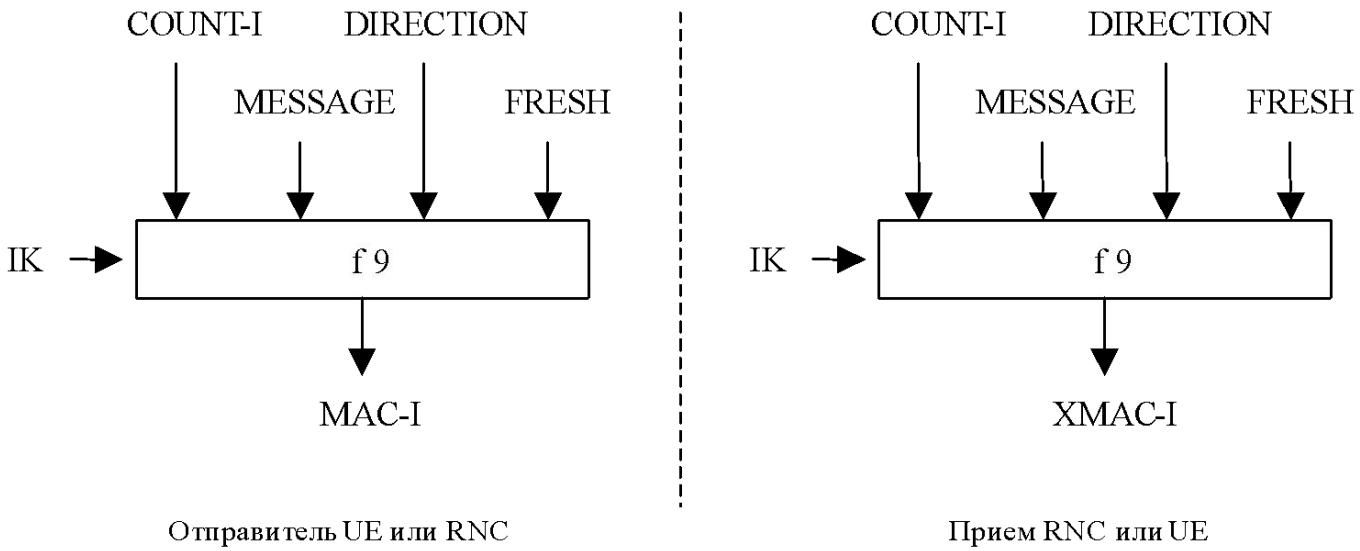



AUTN = SQN [⊕ AK] || AMF || MAC-A
Q = (RAND, XRES, CK, IK, AUTN)

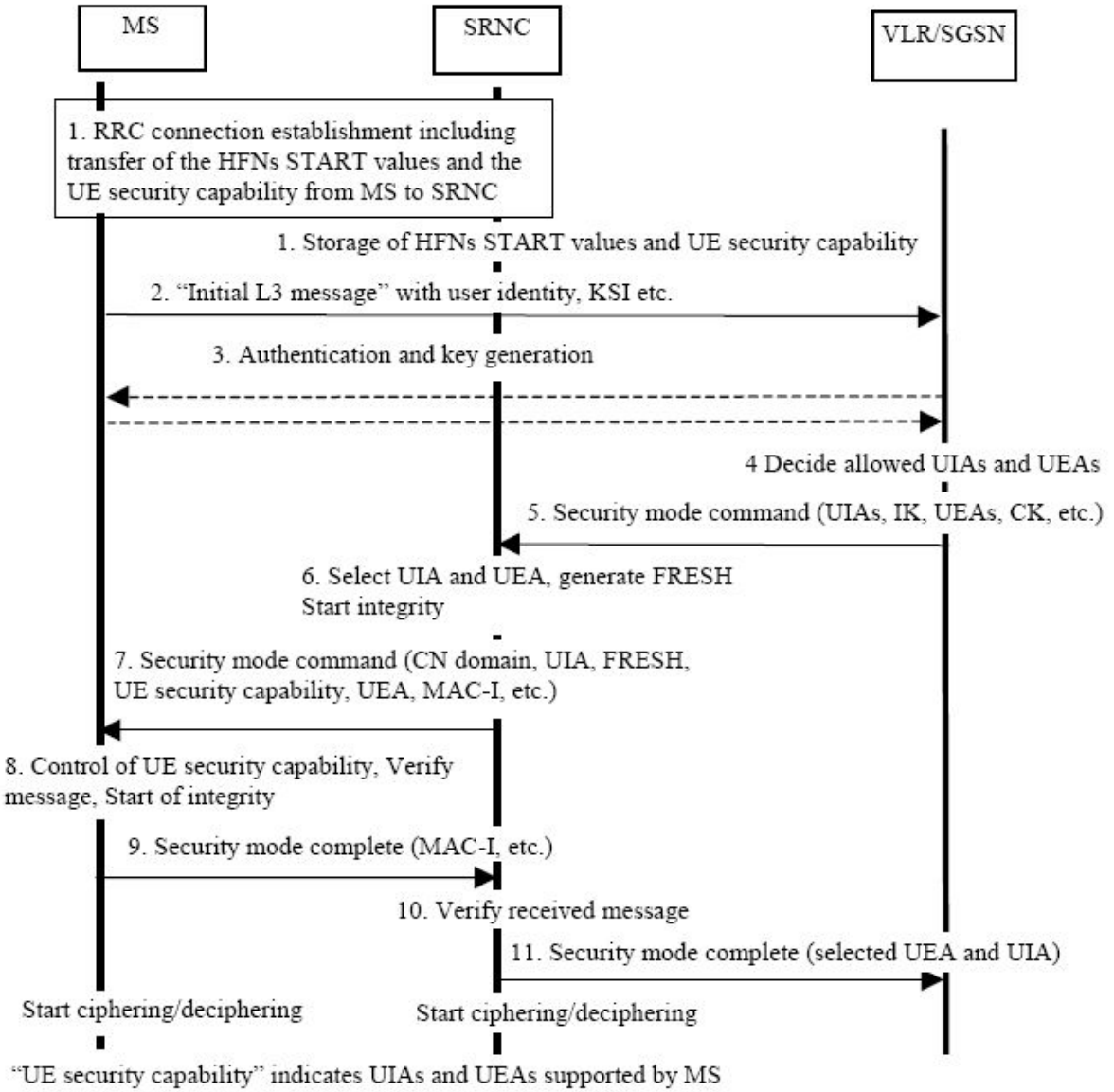
# Процесс ресинхронизации в VLR/AuC



# Процесс обеспечения целостности



# Аутентификация и установление соединения



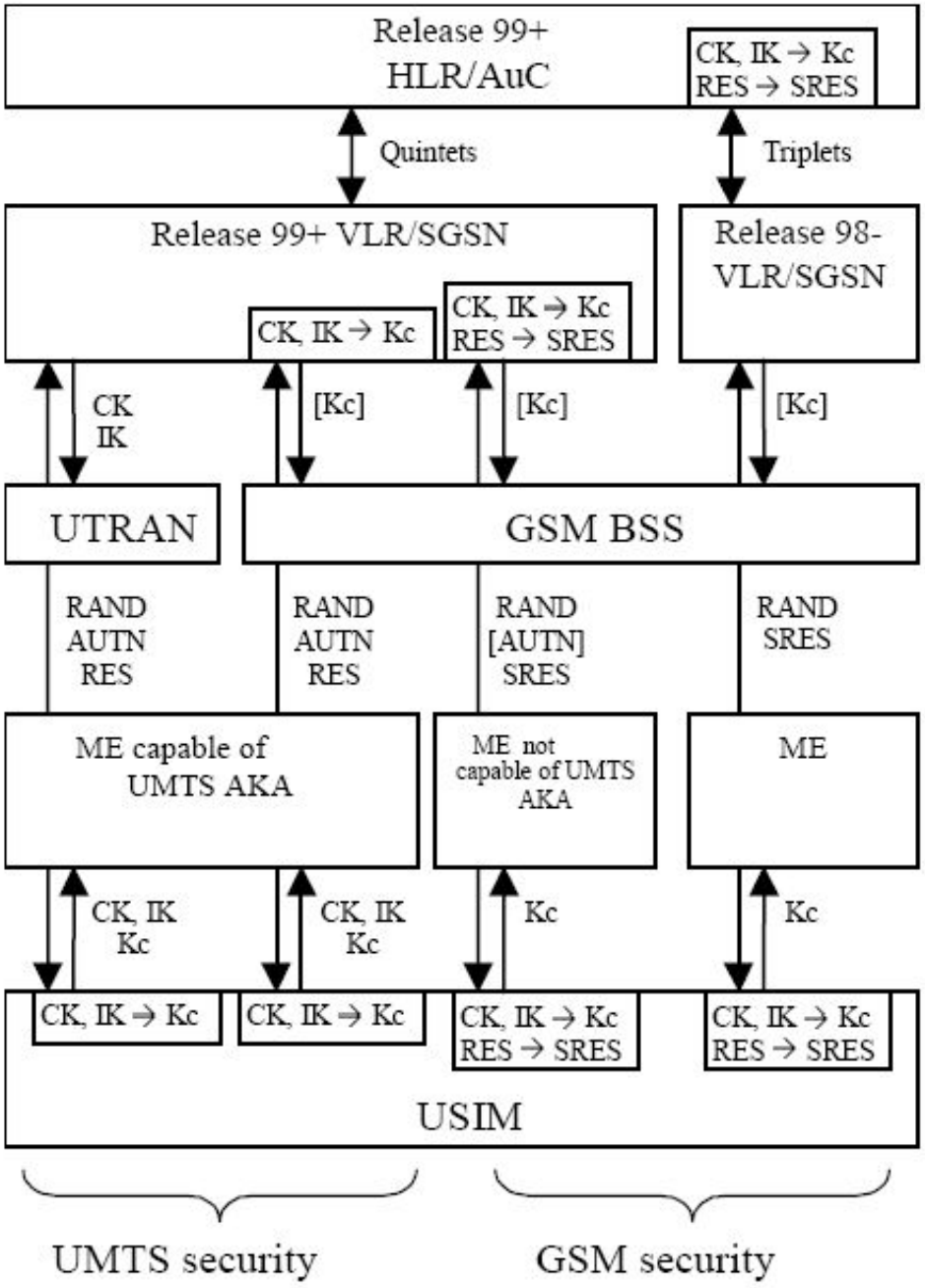



**Figure 18: Authentication and key agreement of UMTS subscribers**