РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 722 508**(13) **C1**

(51) МПК
H04L 29/06 (2006.01)
H04W 12/04 (2009.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 9/083 (2020.02); H04L 63/0414 (2020.02); H04W 12/04 (2020.02)

(21)(22) Заявка: **2020107748, 17.07.2018**

(24) Дата начала отсчета срока действия патента:
17.07.2018

Дата регистрации:
01.06.2020

Приоритет(ы):
(30) Конвенционный приоритет:
25.07.2017 US 62/536632

(45) Опубликовано: **01.06.2020** Бюл. № **16**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **25.02.2020**

(86) Заявка PCT:
EP 2018/069432 (17.07.2018)

(87) Публикация заявки PCT:
WO 2019/020439 (31.01.2019)

Адрес для переписки:
101000, Москва, ул. Мясницкая, д. 13, стр. 5, ООО "Союзпатент"

(72) Автор(ы):
ТОРВИНЕН, Веса (FI),
НАКАРМИ, Прайвол, Кумар (SE),
БЕН ХЕНДА, Ноамен (SE),
КАСТЕЛЬАНОС САМОРА, Давид (ES),
ВИФВЕССОН, Моника (SE),
СААРИНЕН, Пази (SE)

(73) Патентообладатель(и):
ТЕЛЕФОНАКТИЕБОЛАГЕТ ЛМ ЭРИКССОН (ПАБЛ) (SE)

(56) Список документов, цитированных в отчете о поиске: **WO 2016/209126 A1, 29.12.2016. US 2013/003971 A1, 03.01.2013. WO 2016/048574 A1, 31.03.2016. RU 2424624 C2, 20.07.2011. US 9338164 B1, 10.05.2016.**

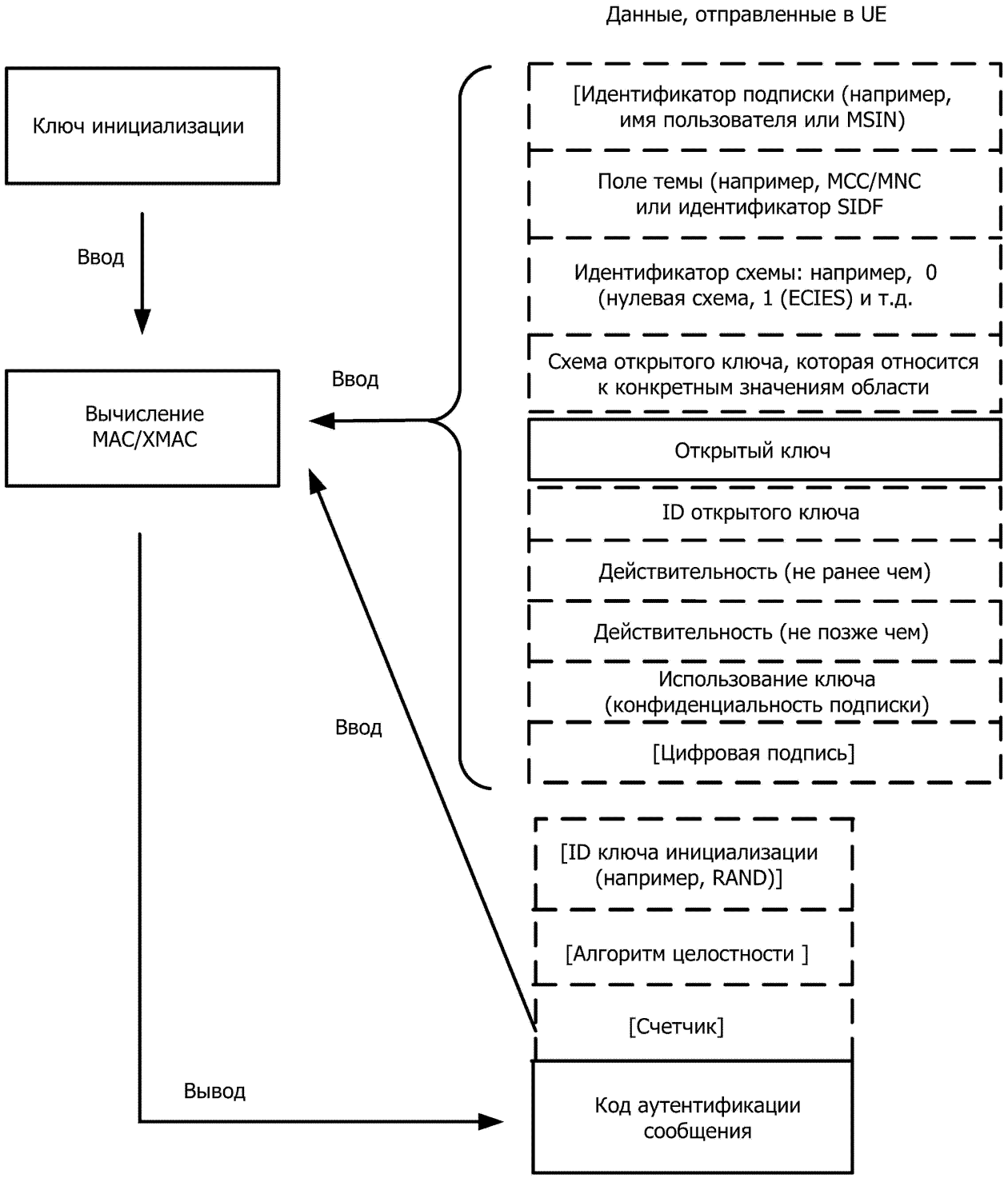
(54) СКРЫТЫЙ ИДЕНТИФИКАТОР ПОДПИСКИ АБОНЕНТА

(57) Реферат:

Изобретение относится к области поддержания конфиденциальности долгосрочного идентификатора подписки пользовательского оборудования. Технический результат изобретения заключается в обеспечении безопасности при взаимодействии между UE и сетью связи. Способ содержит этапы, на которых: принимают скрытый идентификатор подписки абонента (SUCI), содержащий зашифрованную часть, в которой зашифрована по меньшей мере часть идентификатора постоянной подписки абонента (SUPI), и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования SUPI в SUCI; определяют сервер дешифрования, подлежащий использованию для дешифрования зашифрованной части SUCI; отправляют SUCI на сервер дешифрования и принимают в ответ SUPI. 4 н. и 13 з.п. ф-лы, 22 ил.

RU 2722508 C1

RU 2722508 C1



Фиг. 15

RU 2722508 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 722 508**(13) **C1**

(51) Int. Cl.
H04L 29/06 (2006.01)
H04W 12/04 (2009.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 9/083 (2020.02); H04L 63/0414 (2020.02); H04W 12/04 (2020.02)

(21)(22) Application: **2020107748, 17.07.2018**

(24) Effective date for property rights:
17.07.2018

Registration date:
01.06.2020

Priority:
(30) Convention priority:
25.07.2017 US 62/536632

(45) Date of publication: **01.06.2020** Bull. № **16**

(85) Commencement of national phase: **25.02.2020**

(86) PCT application:
EP 2018/069432 (17.07.2018)

(87) PCT publication:
WO 2019/020439 (31.01.2019)

Mail address:
101000, Moskva, ul. Myasnitskaya, d. 13, str. 5, OOO "Soyuzpatent"

(72) Inventor(s):
TORVINEN, Vesa (FI),
NAKARMI, Prajwol, Kumar (SE),
BEN HENDA, Noamen (SE),
CASTELLANOS ZAMORA, David (ES),
WIFVESSON, Monica (SE),
SAARINEN, Pasi (SE)

(73) Proprietor(s):
TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (SE)

RU 2722508 C1

(54) SUBSCRIBER SUBSCRIPTION CONCEALED IDENTIFIER

(57) Abstract:

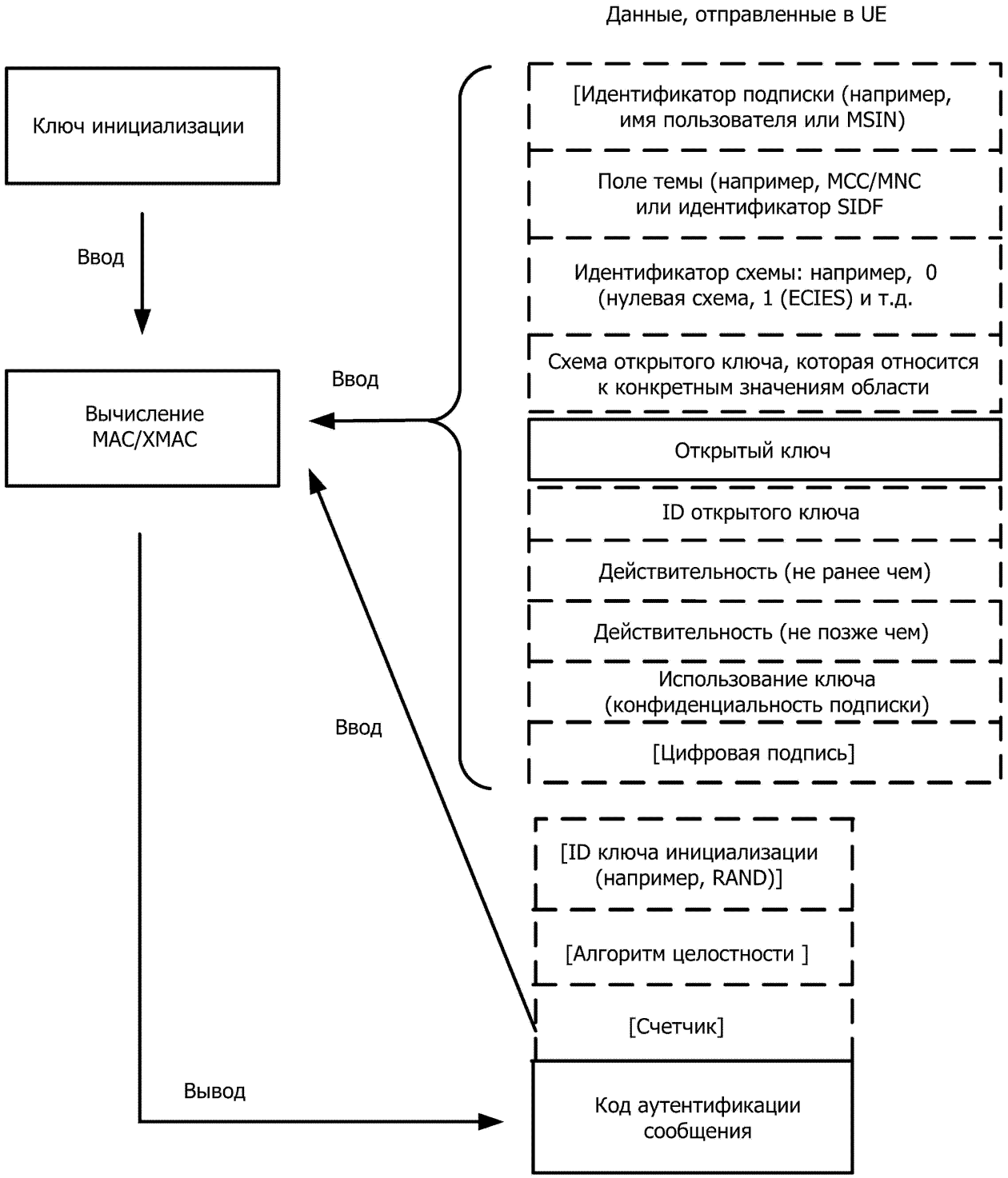
FIELD: data processing.

SUBSTANCE: invention relates to maintaining confidentiality of a long-term user equipment subscription identifier. Method comprises steps of: receiving a subscriber subscription concealed identifier (SUCI), comprising an encrypted part, in which at least part of subscriber subscription permanent identifier (SUPI) is encrypted, and a part with unencrypted text which contains a home network identifier and an encryption scheme identifier which identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI; determining a decryption server to be used to decrypt the encrypted portion of the SUCI; sending SUCI to decryption server and receiving SUPI in response.

EFFECT: technical result of the invention is to ensure security when interacting between UE and a communication network.

17 cl, 22 dwg

RU 2722508 C1



Фиг. 15

Область техники, к которой относится изобретение

Изобретение относится к способам, выполняемым сервером аутентификации, сервером дешифрования и пользовательским оборудованием (UE), соответственно. Кроме того, раскрыты также UE, серверы дешифрования, серверы аутентификации, компьютерная программа и схема памяти.

Уровень техники

Поддержание конфиденциальности долгосрочного идентификатора подписки пользовательского оборудования (UE) (например, международного идентификатора мобильного абонента (IMSI)) является важной задачей. Системы 3GPP предыдущих поколений (например, 4G/LTE, 3G/UMTS, 2G/GSM) включали в себя частичный механизм для конфиденциальности долгосрочного идентификатора подписки с использованием одного или нескольких идентификаторов краткосрочной подписки. Глобальный временный уникальный идентификатор абонента (GUTI) и временный идентификатор сотовой радиосети (C-RNTI) являются примерами краткосрочных идентификаторов подписки в системах 4G/LTE. Однако унаследованный частичный механизм может предоставлять долгосрочный идентификатор подписки в незашифрованном тексте через радиоинтерфейс. Например, так называемые «IMSI-перехватчики» могут просто запросить долгосрочный идентификатор подписки у UE, например, используя сообщения запроса идентификатора и ответные сообщения.

В настоящее время в рамках проекта партнерства третьего поколения (3GPP) обсуждается то, как можно повысить безопасность, например, конфиденциальность, в сетях связи. Что касается 5G, в 3GPP TS 33.501 V0.2.0 упоминается идентификатор постоянной подписки абонента (SUPI) и отмечается, что SUPI может быть скрытым, например, в форме псевдонима или открытого ключа с зашифрованным SUPI.

Раскрытие сущности изобретения

Задача изобретения состоит в том, чтобы обеспечить безопасность при взаимодействии между UE и сетью связи.

Первый аспект изобретения относится к способу, выполняемому сервером аутентификации в домашней сети UE для получения SUPI. Способ содержит:

прием скрытого идентификатора подписки абонента (SUCI), который содержит

зашифрованную часть, в которой зашифрована по меньшей мере часть SUPI, и

часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования SUPI в SUCI,

определение сервера дешифрования, используемого для дешифрования зашифрованной части SUCI;

отправку SUCI на сервер дешифрования, и

прием в ответ на это SUPI.

Часть с незашифрованным текстом SUCI может содержать идентификатор открытого ключа для открытого ключа домашней сети.

Сервер дешифрования может быть одним из множества серверов дешифрования, и определение сервера дешифрования может быть основано на информации, принятой от UE. В данном случае информация может представлять собой идентификатор открытого ключа для открытого ключа домашней сети. Идентификатор открытого ключа может содержаться в части с незашифрованным текстом SUCI.

Информация может представлять собой идентификатор схемы шифрования, и определенный сервер дешифрования затем поддерживает дешифрование в соответствии со схемой шифрования.

В варианте осуществления способ может дополнительно содержать прием SUCI из UE как часть процедуры регистрации для регистрации UE в сети беспроводной связи.

В варианте осуществления способ может дополнительно содержать прием SUCI из UE посредством запроса аутентификации от функции безопасности с привязкой.

Сервер аутентификации может быть одним из множества серверов дешифрования.

Способ может дополнительно содержать отправку SUCI и запроса вектора аутентификации для аутентификации UE в определенный сервер дешифрования в одном и том же сообщении.

Способ может дополнительно содержать прием вектора аутентификации и SUPI из определенного сервера дешифрования в одном и том же ответном сообщении.

SUPI может содержать идентификационный номер абонента мобильной связи (MSIN), код страны мобильной связи (MCC) и код сети мобильной связи (MNC). В данном варианте осуществления MSIN может быть зашифрован в зашифрованной части SUCI, и MCC и MNC представляют собой идентификатор домашней сети в части с незашифрованным текстом SUCI. В альтернативном варианте осуществления SUPI может быть идентификатором доступа к сети.

Второй аспект изобретения относится к способу, выполняемому сервером дешифрования, для передачи SUPI на сервер аутентификации. Способ содержит:

прием из сервера аутентификации SUCI, который содержит зашифрованную часть, в которой зашифрована по меньшей мере часть SUPI, и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE, чтобы зашифровать SUPI в SUCI, и который поддерживается сервером дешифрования;

дешифрование зашифрованной части SUCI с использованием схемы шифрования, указанной идентификатором схемы шифрования, для получения SUPI; и

отправку SUPI на сервер аутентификации.

Часть с незашифрованным текстом SUCI может также содержать идентификатор ключа, используемый для идентификации ключа дешифрования, используемого для дешифрования SUPI. Идентификатор ключа может также использоваться для идентификации сервера дешифрования.

Ключ, соответствующий идентификатору ключа, может быть открытым ключом домашней сети UE.

В варианте осуществления второго аспекта прием SUCI содержит прием SUCI и запрос вектора аутентификации для аутентификации UE в одном и том же сообщении.

Отправка вектора аутентификации и SUPI на сервер аутентификации может быть выполнена в одном и том же сообщении.

Третий аспект относится к способу, выполняемому UE. Способ содержит:

выработку SUCI, который содержит зашифрованную часть, в которой зашифрована по меньшей мере часть SUPI, и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования SUPI в SUCI;

передачу SUCI на сервер аутентификации для пересылки SUCI на сервер дешифрования, способный дешифровать SUPI.

SUCI может передаваться в запросе на регистрацию в сети беспроводной связи.

Выработка SUCI может быть выполнена с использованием защищенного от несанкционированного доступа аппаратного компонента UE для выработки SUCI. В данном случае выработка SUCI может содержать выработку SUCI на основе закрытого ключа, выбранного из множества закрытых ключей, хранящихся в защищенном от

несанкционированного доступа аппаратном компоненте.

В варианте осуществления выработка SUCI содержит отправку значения времени в защищенный от несанкционированного доступа аппаратный компонент для использования при выработке SUCI.

В варианте осуществления выработка SUCI содержит выработку SUCI из закрытого ключа, содержащего SUPI.

В варианте осуществления передача SUCI на сервер аутентификации содержит передачу SUCI на сервер аутентификации в ответ на сообщение запроса идентификатора, полученное от функции управления аутентификацией и мобильностью (AMF), как часть процедуры регистрации UE в сети беспроводной связи. В данном варианте осуществления способ может дополнительно содержать передачу запроса регистрации в AMF, причем запрос регистрации содержит глобальный временный уникальный идентификатор абонента 5G и прием в ответ на это сообщения запроса идентификатора.

Способ согласно третьему аспекту может дополнительно содержать успешную аутентификацию на сервере аутентификации после передачи SUCI и приема ответного сообщения о принятии регистрации.

В варианте осуществления первого, второго и третьего аспектов схема шифрования может быть схемой нулевого шифрования.

В варианте осуществления первого, второго и третьего аспектов схема шифрования может, в качестве альтернативы нулевой схеме или любой другой схеме шифрования, представлять собой интегрированную схему шифрования на основе эллиптических кривых, ECIES, и в данном варианте осуществления часть с незашифрованным текстом SUCI может содержать эфемерный открытый ключ UE для использования в ECIES.

Четвертый аспект относится к серверу аутентификации для домашней сети UE для получения SUPI. Сервер аутентификации содержит схему обработки и схему памяти. Схема памяти содержит инструкции, исполняемые схемой обработки, в результате чего сервер аутентификации выполнен с возможностью:

приема скрытого идентификатора подписки абонента (SUCI), который содержит зашифрованную часть, в которой зашифрована по меньшей мере часть SUPI, и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования SUPI в SUCI,

определения сервера дешифрования, чтобы использовать его для дешифрования зашифрованной части SUCI;

отправки SUCI на сервер дешифрования, и

приема в ответ на это SUPI.

Пятый аспект относится к серверу аутентификации для домашней сети UE для получения SUPI. Сервер аутентификации выполнен с возможностью:

приема скрытого идентификатора подписки абонента (SUCI), который содержит зашифрованную часть, в которой зашифрована по меньшей мере часть SUPI, и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования SUPI в SUCI,

определения сервера дешифрования для того, чтобы использовать его для дешифрования зашифрованной части SUCI;

отправки SUCI на сервер дешифрования, и

приема в ответ на это SUPI.

Шестой аспект относится к серверу аутентификации для домашней сети UE для

получения SUPI. Сервер аутентификации содержит:

модуль интерфейса, выполненный с возможностью приема SUCI, который содержит зашифрованную часть, в которой зашифрована по меньшей мере часть SUPI, и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования SUPI в SUCI,

модуль определения, выполненный с возможностью определения сервера дешифрования, используемого для дешифрования зашифрованной части SUCI; и где

модуль интерфейса дополнительно выполнен с возможностью отправки SUCI на сервер дешифрования и получения в ответ на это SUPI.

Изобретение также относится к серверу аутентификации согласно любому из аспектов с четвертого по шестой выполненному с возможностью выполнения любого из вариантов осуществления способа согласно первому аспекту.

Седьмой аспект относится к серверу дешифрования для передачи SUPI на сервер аутентификации. Сервер дешифрования содержит схему обработки и схему памяти. Схема памяти содержит инструкции, исполняемые схемой обработки, в результате чего сервер дешифрования выполнен с возможностью:

приема, из сервера аутентификации, SUCI, который содержит зашифрованную часть, в которой зашифрована по меньшей мере часть SUPI, и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует используемую схему шифрования с помощью UE для шифрования SUPI в SUCI, который поддерживается сервером дешифрования;

дешифрования зашифрованной части SUCI с использованием схемы шифрования, указанной идентификатором схемы шифрования, для получения SUPI; и

отправки SUPI на сервер аутентификации.

Восьмой аспект относится к серверу дешифрования для передачи SUPI на сервер аутентификации. Сервер дешифрования выполнен с возможностью:

приема, из сервера аутентификации, SUCI, который содержит зашифрованную часть, в которой зашифрована по меньшей мере часть SUPI, и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует используемую схему шифрования с помощью UE для шифрования SUPI в SUCI, который поддерживается сервером дешифрования;

дешифрования по меньшей мере части SUCI с использованием схемы шифрования, указанной идентификатором схемы шифрования, с тем чтобы получить SUPI; и

отправки SUPI на сервер аутентификации.

Девятый аспект относится к серверу дешифрования для передачи SUPI на сервер аутентификации. Сервер дешифрования содержит:

модуль приема, выполненный с возможностью приема из сервера аутентификации SUCI, который содержит зашифрованную часть, в которой зашифрована по меньшей мере часть SUPI, и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования SUPI в SUCI, и который поддерживается сервером дешифрования;

модуль дешифрования, выполненный с возможностью дешифрования по меньшей мере части SUCI с использованием схемы шифрования, указанной идентификатором схемы шифрования, для получения SUPI; и

модуль отправки, выполненный с возможностью отправки SUPI на сервер аутентификации.

Изобретение также относится к серверу дешифрования согласно любому из шестого, восьмого и девятого аспектов, выполненному с возможностью выполнения любого из вариантов осуществления второго аспекта.

Десятый аспект относится к UE, которое содержит схему обработки и схему памяти. Схема памяти содержит инструкции, исполняемые схемой обработки, в результате чего UE выполнено с возможностью:

выработки SUCI, который содержит зашифрованную часть, в которой зашифрована по меньшей мере часть SUPI, и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования SUPI в SUCI; и

передачи SUCI на сервер аутентификации для пересылки SUCI на сервер дешифрования, способный дешифровать SUPI.

Одиннадцатый аспект относится к UE, выполненному с возможностью:

выработки SUCI, который содержит зашифрованную часть, в которой зашифрована по меньшей мере часть SUPI, и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования SUPI в SUCI; и

передачи SUCI на сервер аутентификации для пересылки SUCI на сервер дешифрования, способный дешифровать SUPI.

Двенадцатый аспект относится к UE, которое содержит:

модуль выработки, выполненный с возможностью выработки SUCI, который содержит зашифрованную часть, в которой зашифрована по меньшей мере часть SUPI, и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования SUPI в SUCI, и

модуль передачи, выполненный с возможностью передачи SUCI на сервер аутентификации для пересылки SUCI на сервер дешифрования, способный дешифровать SUPI.

Согласно варианту осуществления первого, третьего и двенадцатого аспектов часть с незашифрованным текстом SUCI может содержать идентификатор открытого ключа для открытого ключа домашней сети.

SUPI может содержать идентификационный номер абонента мобильной связи.

SUPI может быть идентификатором доступа к сети.

Изобретение также относится к пользовательскому оборудованию согласно любому из десятого, одиннадцатого и двенадцатого аспектов, выполненному с возможностью выполнения любого из вариантов осуществления третьего аспекта.

13-й аспект относится к компьютерной программе, содержащей инструкции, которые при их исполнении по меньшей мере в одной схеме обработки серверного устройства предписывают по меньшей мере одной схеме обработки выполнять способ в соответствии с любым из вариантов осуществления с первого по третий аспекты.

14-й аспект относится к схеме памяти, содержащей компьютерную программу.

Краткое описание чертежей

На фиг.1 показана примерная сеть беспроводной связи.

На фиг.2 показан пример, в котором UE выполняет шифрование своего долгосрочного идентификатора подписки как часть процедуры подключения.

На фиг.3 показан пример скрытого идентификатора подписки абонента (SUCI).

На фиг.4 показан пример закрытого ключа.

На фиг.5 показана схема обеспечения конфиденциальности открытого ключа 3GPP.

На фиг.6 показан пример процедуры регистрации.

На фиг.7 показан пример, в котором 5G-USIM/UICC UE вырабатывает SUCI.

На фиг.8 показан пример, в котором 5G-USIM/UICC не имеет закрытого ключа.

На фиг.9 показан пример, в котором ME вырабатывает SUCI.

На фиг.10 показан пример, в котором ME уведомляется об обновленном закрытом ключе.

На фиг.11 показан пример, в котором ME обнаруживает, что 5G-USIM/UICC была заменена.

На фиг.12 показан пример данных верификации закрытого ключа.

На фиг.13 показан пример процесса регистрации UE, в котором UE не имеет действительного закрытого ключа.

На фиг.14 показан пример процесса регистрации UE, в котором закрытый ключ UE должен быть обновлен.

На фиг.15 показан пример того, как закрытый ключ и данные верификации закрытого ключа связаны друг с другом.

На фиг.16 показан вариант осуществления аппаратных средств, например, для сервера аутентификации.

На фиг.17 показан вариант осуществления сервера аутентификации.

На фиг.18 показан вариант осуществления сервера аутентификации.

На фиг.19 показан вариант осуществления, например, сервера дешифрования.

На фиг.20 показан вариант осуществления сервера дешифрования.

На фиг.21 показан вариант осуществления UE.

На фиг.22 показан вариант осуществления UE.

Осуществление изобретения

На фиг.1 показана примерная сеть 30 беспроводной связи, которая включает в себя UE 1, обслуживающую сеть 2 и домашнюю сеть 3. UE и домашняя сеть коммуникативно связаны друг с другом и обмениваются сигналами через обслуживающую сеть. UE сконфигурировано с идентификатором подписки, идентифицирующим подписку, поддерживаемую домашней сетью, и осуществляет доступ к домашней сети, используя обслуживающую сеть.

Типичные примеры UE 1 включают в себя оборудование мобильной связи (ME), терминал мобильной связи, смартфон, персональный компьютер, портативный компьютер, настольный компьютер, рабочую станцию, планшетный компьютер, носимый компьютер и/или интеллектуальный бытовой электроприбор. Согласно конкретным вариантам осуществления UE может содержать общее хранилище памяти как часть ME и защищенный от несанкционированного доступа аппаратный компонент, обеспечивающий безопасное хранение, такой как универсальный модуль идентификации абонента (5G-USIM), универсальная карта с интегральной схемой (UICC), например, с установленным на ней 5G-USIM, и/или другое защищенное устройством хранения. Согласно таким вариантам осуществления любая из возможностей, приписываемых UE, обычно может быть выполнена с использованием защищенного от несанкционированного доступа аппаратного компонента UE.

Обслуживающая сеть 2 включает в себя одно или несколько физических устройств и/или сред передачи сигналов, способных обмениваться сигналами связи с UE 1 и домашней сетью 3. В частности, обслуживающая сеть может включать в себя аппаратные средства, которые предусматривают одну или несколько точек доступа (например,

базовую станцию, eNodeB, фемтосоту и/или точку беспроводного доступа), сети доступа, серверы аутентификации, функции управления доступом и мобильностью (AMF), функции безопасности с привязкой (SEAF), функции сервера аутентификации (AUSF) и/или любую их комбинацию (не показано). В частности, сервер аутентификации может предусматривать одну или несколько AMF, SEAF AUSF и/или любую их комбинацию. Детали этих сетевых объектов будут обсуждены более подробно ниже.

Домашняя сеть 3 включает в себя одно или несколько физических устройств и/или сред передачи сигналов, способных обмениваться сигналами связи с UE 1 через обслуживающую сеть 2. В частности, домашняя сеть может включать в себя один или несколько: серверов дешифрования, серверов аутентификации (например, как описано выше), серверов инициализации ключей, функций дешифрования идентификатора подписки абонента (SIDF), функции инициализации закрытых ключей (PKPF), унифицированное управление данными (UDM) и/или любую их комбинацию (не показано). В частности, сервер дешифрования может предоставлять один или несколько SIDF, PKPF и/или любую их комбинацию. Характерные особенности этих сетевых объектов также будут обсуждены более подробно ниже.

Примеры обслуживающей и/или домашней сети включают в себя (но не ограничиваются ими) одну или более: локальных сетей; сетей беспроводной связи; сотовых сетей; сетей на базе Интернет-протокола; сетей Ethernet; оптических сетей и/или сетей с коммутацией каналов. Такие сети могут включать в себя любое количество сетевых устройств, таких как маршрутизаторы, шлюзы, коммутаторы, концентраторы, брандмауэры и т.п. (не показаны), которые поддерживают обмен такими сигналами связи.

Хотя на фиг.1 обслуживающая сеть и домашняя сеть показаны по отдельности, в некоторых вариантах осуществления настоящего раскрытия домашняя сеть 3 является обслуживающей сетью 2, то есть в случае, когда UE не находится в роуминге. Кроме того, хотя примеры конкретных функций в домашней сети или в обслуживающей сети были указаны выше, эти конкретные функции могут иметь место в другой домашней сети или обслуживающей сети согласно конкретным вариантам осуществления. Кроме того, хотя на фиг.1 показано только одно UE 1, обслуживающая и домашняя сети могут поддерживать множество UE согласно конкретным вариантам осуществления.

Одним из примеров способа поддержания конфиденциальности долгосрочного идентификатора подписки UE является защита долгосрочного идентификатора подписки с использованием открытого ключа домашней сети. Открытый ключ домашней сети может быть инициализирован в UE 1 без сертификата, поэтому не требуются глобальная инфраструктура открытого ключа (PKI) или центр сертификации (CA) (то есть по той причине, что технология используется асимметрично между UE и функцией в домашней сети 3). В таком примере можно ожидать, что UE шифрует долгосрочный идентификатор подписки, который затем передается в домашнюю сеть с использованием открытого ключа домашней сети.

На фиг.2 показан один такой конкретный пример, в котором UE выполняет шифрование своего долгосрочного идентификатора подписки как часть процедуры подключения. В соответствии с примером, показанным на фиг.2, UE 1 выполняет шифрование своего IMSI, оставляя свои части кода страны мобильной связи (MCC) и кода сети мобильной связи (MNC) в виде незашифрованного текста, и отправляет запрос на подключение в обслуживающую сеть 2 с зашифрованным IMSI в качестве своего идентификатора (этап 1). Обслуживающая сеть идентифицирует домашнюю сеть 3 UE с использованием незашифрованного текста MCC/MNC и запрашивает информацию

аутентификации из домашней сети UE, используя зашифрованный IMSI в качестве идентификатора UE (этап 2). Домашняя сеть дешифрирует IMSI из зашифрованного IMSI и извлекает соответствующую информацию аутентификации. В ответ на запрос информации аутентификации домашняя сеть отправляет информацию аутентификации UE вместе с открытым IMSI незашифрованным текстом в обслуживающую сеть (этап 3). Обслуживающая сеть выполняет процедуру аутентификации с UE для аутентификации UE (этап 4). Если процедура аутентификации завершена успешно, обслуживающая сеть отправляет сообщение принятия подключения в UE (этап 5).

В таком подходе открытый ключ домашней сети может быть предварительно инициализирован в USIM и/или может быть инициализирован с использованием процедуры инициализации беспроводной связи (OTA). Хотя подход, показанный на фиг.2, действительно защищает долгосрочный идентификатор подписки по меньшей мере в некоторых вариантах осуществления, некоторые такие варианты осуществления могут иметь один или несколько недостатков. Например, подход, показанный на фиг.2, может быть нарушен унаследованными USIM, которые, вероятно, нельзя изменить, некоторыми домашними операторами, которые не могут поддерживать инициализацию OTA, и/или USIM, которые не могут обновляться (например, из-за технических ограничений, отсутствия объема памяти или других ограничений).

Различные варианты осуществления настоящего раскрытия предусматривают альтернативы по меньшей мере некоторым аспектам конкретного варианта осуществления, показанного на фиг.2, которая соответствует фиг.3-8. Взаимодействие компонентов представлено в документе “Deliverable D3.6 5G-PPP Security enablers open specifications (v2.0)”. Конкретные варианты осуществления позволяют инициализировать открытый ключ домашней сети 3 (например, новый или обновленный) и сохранять его в UE 1, с тем чтобы UE 1 могло зашифровать свой идентификатор подписки с помощью этого открытого ключа. Кроме того, в конкретных вариантах осуществления базовая сеть (такая как сеть 5GC (базовая сеть 5G)) запускает инициализацию открытого ключа домашней сети по существующим процедурам трафика, определенным 3GPP (например, сигнализация регистрации/аутентификации, например, сообщения слоя без доступа между UE и узлом AMF/SEAF в связи с процедурой регистрации), без необходимости полагаться на дополнительную инфраструктуру и внеполосные процедуры, такие как выполнение процедуры обновления OTA.

Хотя различные варианты осуществления в данном документе будут описывать определенные признаки или действия, выполняемые UE 1, не следует предполагать, что такие признаки или действия выполняются любым конкретным компонентом UE, если не указано иное. Например, такие функции могут или не могут выполняться UICC, USIM, встроенной UICC, интегрированной UICC или другой схемой и/или программным обеспечением UE (например, основополосной схемой в ME), в зависимости от конкретного варианта осуществления.

Конкретные варианты осуществления включают в себя идентификатор постоянной подписки абонента (SUPI). SUPI представляет собой постоянный идентификатор 5G с незашифрованным текстом, уникальным на глобальном уровне, который выделяется каждому абоненту в системе 5G. SUPI может быть выполнен на основе IMSI или не на основе IMSI. Варианты осуществления, которые включают в себя SUPI на основе IMSI, могут использовать IMSI, как описано, например, в 3GPP TS 23.003 V15.0.0. Варианты осуществления, которые включают в себя SUPI не на основе IMSI, могут быть основаны на идентификаторе доступа к сети (NAI) в соответствии с идентификацией пользователя на основе IETF RFC 4282, описанной в 3GPP TS 23.003 V15.0.0. В некоторых вариантах

осуществления SUPI включает в себя адрес домашней сети (например, MCC и MNC в случае SUPI на основе IMSI). Такие варианты осуществления могут включать в себя определенные сценарии роуминга, например, путем предоставления обслуживающей сети 2 информации, полезной для идентификации домашней сети 3 UE. В случае, если SUPI представляет собой NAI, он может также содержать IMSI, но он также может быть не основан на IMSI.

Конкретные варианты осуществления дополнительно или альтернативно включают в себя скрытый идентификатор подписки абонента (SUCI), такой как показан в примере на фиг.3. SUCI является защищенной версией SUPI. SUCI включает в себя часть с незашифрованным текстом и зашифрованную часть.

Часть с незашифрованным текстом включает в себя идентификатор домашней сети, который идентифицирует домашнюю сеть UE 1. Например, SUCI может включать в себя MCC и MNC домашней сети. Часть с незашифрованным текстом может также включать в себя идентификатор открытого ключа, идентификатор схемы шифрования и/или связанные со схемой параметры, используемые для дешифрования зашифрованной части SUCI в соответствии со схемой шифрования, такой как эфемерный открытый ключ UE или другие параметры, предназначенные для использования в интегрированной схеме шифрования на основе эллиптических кривых (ECIES) или другой схеме шифрования. Термин эфемерный ключ известен специалистам в данной области техники и определяется как ключ, использование которого ограничено коротким периодом времени, таким как одно телекоммуникационное соединение (или сеанс), после которого все его следы удаляются. Как будет обсуждено ниже, идентификатор открытого ключа является идентификатором, который может использоваться в домашней сети для идентификации правильной SIDF в домашней сети, которая включает в себя множество SIDF. ECIES, идентификатор открытого ключа и SIDF будут описаны более подробно ниже. Специалисту будет понятно, что «часть с незашифрованным текстом» в контексте SUCI означает, что информация в ней является нескрытой/незашифрованной информацией.

Когда зашифрованная часть включена в SUCI, SUCI представляет собой защищенную версию SUPI. Зашифрованная часть включает в себя зашифрованный идентификатор подписки, такой как идентификационный номер абонента мобильной связи (MSIN) или имя пользователя. Имя пользователя может иметь все или часть символов, которые предшествуют символу ‘@’ в NAI, например, username@mnc<MNC>.mcc<MCC>.3gppnetwork.org. В этом примере все символы перед символом ‘@’ зашифрованы. В случае расширенного NAI (Decorated NAI), который имеет форму ‘homerealm!username@otherrealm’, зашифрована только часть имени пользователя в тексте слева от ‘@’, так как домашняя область (homerealm) может использоваться в качестве информации о маршрутизации. Таким образом, дешифрование зашифрованной части SUCI может выполняться для обучения соответствующего SUPI. ECIES является примером схемы шифрования с открытым ключом, которая может использоваться для выработки SUCI из SUPI и/или SUPI из SUCI. Как будет обсуждено далее, зашифрованная часть SUCI может использовать схему нулевого шифрования, например, если UE 1 не был инициализирован с помощью открытого ключа домашней сети.

SIDF представляет собой функцию, расположенную в домашней сети, которая отвечает за дешифрование SUCI. В частности, в архитектуре 5G SIDF может быть совмещена с унифицированным управлением данными (UDM). В качестве альтернативы можно отметить, что SIDF является частью UDM или предоставляется со стороны UDM. Дополнительно или альтернативно, SIDF может быть объектом, расположенным

отдельно от UDM и/или совмещенным с функцией сервера аутентификации (AUSF).

На фиг.4 показан пример закрытого ключа. Этот конкретный пример закрытого ключа включает в себя открытый ключ домашней сети. В некоторых вариантах осуществления закрытый ключ также включает в себя один или несколько параметров, связанных со схемой открытого ключа, долгосрочный идентификатор подписки, поле темы, указывающее сеть, домен или контекст, к которому относится закрытый ключ (например, темой может быть идентификатор домашней сети, такой как MCC/MNC), идентификатор схемы открытого ключа, конкретные значения, относящиеся к области, связанной со схемой открытого ключа (например, значения для области эллиптических кривых в случае схемы ECIES), идентификатор открытого ключа, как будет обсуждено более подробно ниже, сроки действия с указанием обоснований, когда закрытый ключ является действительным (например, недействительным до какого-либо момента времени и/или недействительным по истечении какого-либо момента времени), поле использования ключа, указывающее один или несколько способов использования ключа (например, конфиденциальность идентификатора подписки, конфиденциальность выбора среза и т.д.) и/или цифровую подпись, рассчитанную для части или всего закрытого ключа.

В частности, поле использования ключа может быть установлено для указания того, что ключ полезен для «конфиденциальности подписки», согласно вариантам осуществления настоящего раскрытия. Использование конфиденциальности, которое выходит за рамки настоящего раскрытия, может дополнительно или альтернативно указывать другое применение закрытого ключа. Например, закрытый ключ может использоваться для целей «конфиденциальности информации о помощи выбора среза сети (NSSAI)» вместо или в дополнение к целям «конфиденциальности подписки». Действительно, такие другие цели могут включать в себя аналогичные способы, устройства и системы в UE 1 и/или в домашней сети для начальной инициализации, обновления и других функций, описанных в данном документе. Хотя в некоторых вариантах осуществления один закрытый ключ может указывать многочисленные виды использования, другие варианты осуществления могут включать в себя соответствующие закрытые ключи для соответствующих видов использования, поле использования ключа каждого закрытого ключа указывает использование одного ключа (например, один из закрытых ключей может указывать «конфиденциальность подписки», а другой может указывать «конфиденциальность NSSAI»). Поле использования ключа может быть отформатировано как целое число, одно или несколько перечисляемых значений, буквенно-цифровая строка, битовая строка, строка с разделителями и/или, среди прочего, массив любого из вышеупомянутых форматов.

Схема обеспечения конфиденциальности открытого ключа 3GPP (схемы 3GPK) является стандартизированной схемой открытого ключа, которую UE 1 может поддерживать для взаимодействия между UE и, например, оператором мобильной связи. В отсутствие стандартизированной схемы поставщики UE, вероятно, должны будут координировать свои действия с такими операторами для реализации механизмов конфиденциальности. Согласно конкретным вариантам осуществления UE должно поддерживать любую разрешенную и/или стандартизированную схему, чтобы домашняя сеть могла свободно выбирать схему, не создавая какие-либо трудности взаимодействия. В частности, одной из таких схем является ECIES. Конкретные схемы могут быть приняты в качестве стандарта и снабжены идентификатором (также называемым «регистром») для взаимодействия. Для каждой такой схемы могут быть также указаны любые конкретные алгоритмы, которые будут поддерживаться. Например, в случае

ECIES могут быть указаны согласование ключей (KA), функция выведения ключей (KD) (KDF), симметричная целостность и симметричное шифрование. Кроме того, могут быть также указаны один или несколько параметров, относящихся к такой схеме, а также (в одном или нескольких случаях) их потенциальные статические значения. Например, в ECIES параметры домена эллиптических кривых (p, a, b, G, n, h) для кривой над простым полем и/или (m, f(x), a, b, G, n, h) для кривой над двоичным полем.

На фиг.5 показан пример схемы 3GPK. Каждой схеме, принятой в качестве стандарта, может быть присвоен конкретный идентификатор. Например, нулевой схеме может быть присвоен 0, ECIES может быть присвоена 1 и так далее. Идентификатор может быть, например, 4-битовым идентификатором. В других вариантах осуществления идентификатор схемы можно форматировать другими способами, включая, но не ограничиваясь этим, одно или более целых чисел, цифровых строк, буквенно-цифровых строк, битовых строк и/или других типов данных.

Согласно вариантам осуществления настоящего изобретения UE регистрируется в сети 30 беспроводной связи в соответствии с процедурой регистрации, такой как примерная процедура регистрации, показанная на фиг.6. В соответствии с примерной процедурой регистрации, показанной на фиг.6, UE использует открытый ключ домашней сети, чтобы скрыть долгосрочный идентификатор подписки. Хотя один или несколько конкретных интерфейсов, показанных на фиг.6, таких как те, которые обозначены буквой N, за которой следует числовое обозначение (например, N1, N12, N13), соответствуют стандарту 3GPP TS 23.501, сигнализация, выполняемая во всех таких интерфейсах, как описано в данном документе, а также в других интерфейсах (например, Nxx), не известна и не описана ни в одном известном документе уровня техники.

В соответствии с примером, показанным на фиг.6, UE 1 включает в себя временный идентификатор (например, 5G-GUT1) в запросе регистрации и отправляет запрос регистрации в AMF/SEAF 4 (этап 1). AMF/SEAF, не распознавая 5G-GUTI, передает сообщение запроса идентификатора в UE, чтобы запросить идентификатор UE (этап 2). UE отвечает на сообщение запроса идентификатора с помощью ответного сообщения идентификатора, содержащего SUCI (этап 3). AMF/SEAF запрашивает аутентификацию UE у AUSF 5 в домашней сети 3 и включает в себя SUCI в запрос аутентификации (этап 4). AUSF использует информацию, закодированную в SUCI, чтобы определить, какую из множества SIDF использовать для дешифрования по меньшей мере части SUCI (этап 5). В частности, AUSF может использовать идентификатор открытого ключа, переносимый в SUCI (или иным образом присутствующий в сообщении запроса аутентификации), чтобы идентифицировать правильную SIDF 6. В некоторых вариантах осуществления AUSF может дополнительно или альтернативно использовать идентификатор схемы, чтобы идентифицировать правильную SIDF. Другими словами, разные SIDF могут обрабатывать разные схемы шифрования (например, первый SIDF может обрабатывать ECIES, и второй SIDF может обрабатывать RSA), и AUSF может выбрать подходящий SIDF на основе того, какая схема идентифицирована SUCI. В еще одном альтернативном варианте осуществления информация, используемая для идентификации правильной SIDF 6, может быть параметром или ID, который указывает SIDF 6 и какой параметр/ID хранится или инициализируется в защищенном от несанкционированного вмешательства аппаратном компоненте 8.

Варианты осуществления настоящего раскрытия могут включать в себя множество SIDF, чтобы избежать, например, единой точки отказа для сетей, имеющих большое количество абонентов. Следовательно, распределенное развертывание SIDF может быть полезным для повышения отказоустойчивости, балансировки нагрузки и/или

общей пропускной способности сети. Дополнительно или альтернативно, разные экземпляры SIDF могут быть развернуты для обработки разных наборов открытых ключей домашней сети. Соответственно, идентификатор открытого ключа в SUCI может использоваться для выбора подходящего экземпляра(ов) SIDF, согласно одному или нескольким вариантам осуществления, представленным в данном документе. В качестве альтернативы, в конкретных вариантах осуществления, в которых развернута только одна SIDF, идентификатор открытого ключа может быть исключен из SUCI.

AUSF 5 отправляет SUCI в выбранную SIDF 6 (этап 6). Если SIDF расположена в UDM 7 (так что сообщение Nxx на этапе 6, показанном на фиг.6, является, например, сообщением N13), то одно и то же сообщение может использоваться для запроса вектора аутентификации или учетных данных аутентификации из UDM. SIDF дешифрирует SUCI для получения соответствующего SUPI и возвращает SUPI в AUSF (этап 7). Если SIDF находится в UDM, то одно и то же сообщение может использоваться для возврата вектора/учетных данных аутентификации в AUSF.

AUSF 5 и UE 1 обмениваются аутентификационными сообщениями, используя векторы/учетные данные аутентификации, принятые из UDM 7 (этап 8). Если AUSF еще не получила требуемый/требуемые вектор/учетные данные аутентификации из UDM (например, на этапе 7, описанном выше), AUSF может запросить вектор/учетные данные аутентификации из UDM перед инициированием аутентификации с помощью UE (не показано). В качестве альтернативы, AUSF может делегировать аутентификацию SEAF. В таких вариантах осуществления AUSF на этом этапе может просто пересылать SUPI в SEAF и положиться на SEAF для выполнения аутентификации на следующем этапе.

Продолжая рассматривать пример, в котором AUSF 5 успешно аутентифицирует UE 1, AUSF возвращает SUPI в AMF/SEAF 4 (этап 9). AMF/SEAF принимает регистрацию UE и передает сообщение о принятии регистрации в UE (этап 10).

Как кратко обсуждалось выше, конкретные признаки UE 1 могут быть выполнены защищенным от несанкционированного доступа аппаратным компонентом 8 UE. На фиг.7 показан конкретный пример, в котором 5G-USIM/UICC 8a UE вырабатывает SUCI. Хотя в этом конкретном примере используется термин 5G-USIM/UICC, этот термин не должен рассматриваться как ограничивающий в отношении какой-либо версии или поставщика технологии USIM или UICC, и этот термин не должен рассматриваться как ограничивающий в отношении мобильных сетей любого поколения, например, 2G/3G/4G/5G.

В соответствии с примером, показанным на фиг.7, ME 9 запрашивает SUCI (этап 1). В некоторых таких вариантах осуществления этот запрос SUCI может включать в себя время. В других таких вариантах осуществления запрос может быть просто операцией считывания из 5G-USIM/UICC 8a. Согласно таким вариантам осуществления, в которых имеется несколько открытых ключей домашней сети, 5G-USIM/UICC выбирает правильный соответствующий закрытый ключ (например, основываясь на времени) и вырабатывает SUCI, используя выбранный закрытый ключ (этап 2). Альтернативно, если имеются такие варианты осуществления, в которых имеется только один закрытый ключ, 5G-USIM/UICC просто использует этот закрытый ключ. Затем 5G-USIM/UICC возвращает SUCI в ME (этап 3).

На фиг.8 показан пример, в котором 5G-USIM/UICC не имеет закрытого ключа или не поддерживает эту функцию.

В соответствии с примером, показанным на фиг.8, ME 9 запрашивает SUCI с помощью запроса (который в некоторых вариантах осуществления может включать в себя время) аналогично тому, как описано выше со ссылкой на фиг.7. Однако в этом примере 5G-

USIM/UICC 8a не имеет закрытого ключа или не распознает команду, так как она поддерживает функцию (этап 2). Соответственно, 5G-USIM/UICC возвращает сообщение об ошибке (или пустые данные) в ME (этап 3).

В качестве альтернативы примеру, показанному на фиг.8, ME 9 может знать, что 5G-USIM/UICC 8a не имеет закрытого ключа или не поддерживает закрытый ключ другими средствами согласно конкретным вариантам осуществления. Например, ME может получить версию и/или информацию о поставщике 5G-USIM/UICC и определить, основываясь на этой информации, что закрытый ключ не поддерживается или не присутствует. В качестве другого примера, ME может определить, что закрытый ключ не поддерживается или присутствует в 5G-USIM/UICC, на основании некоторого другого ответного сообщения от 5G-USIM/UICC.

На фиг.9 показан пример, в котором ME 9 вырабатывает SUCI, но сам закрытый ключ хранится в 5G-USIM/UICC 8a.

В соответствии с примером, показанным на фиг.9, ME 9 не имеет закрытого ключа и запрашивает его у 5G-USIM/UICC 8a (этап 1). В некоторых вариантах осуществления запрос включает в себя время. В других вариантах осуществления запрос является операцией прямого считывания из памяти 5G-USIM/UICC. Затем 5G-USIM/UICC выбирает закрытый ключ (например, на основе времени, если оно указано в запросе) (этап 2). 5G-USIM/UICC возвращает закрытый ключ в ME (этап 3). В этот момент ME может в некоторых вариантах осуществления (но не обязательно во всех вариантах осуществления) сохранить закрытый ключ и/или SUPI в энергонезависимой памяти ME (этап 4). Затем ME вырабатывает SUCI на основе SUPI и закрытого ключа (этап 5).

На фиг.10 показан пример, в котором ME 9 получает уведомление, если закрытый ключ обновляется в 5G-USIM/UICC 8a. В этом сценарии ME подписывается на изменения ключей конфиденциальности и получает уведомления, когда доступны обновления. В этом сценарии предполагается, что ME хранит закрытый ключ или запрашивает закрытый ключ 5G-USIM/UICC, чтобы получить последний закрытый ключ.

В соответствии с примером, показанным на фиг.10, ME 9 отправляет запрос 5G-USIM/UICC 8a с запросом подписаться на обновления закрытого ключа (этап 1). В некоторых вариантах осуществления запрос может включать в себя SUPI. 5G-USIM/UICC принимает подписку и передает в ответ на это подтверждение ME (этап 2). Когда домашняя сеть обновляет закрытый(е) ключ(и) или доставляет один или несколько новых ключей в 5G-USIM/UICC (этап 3), 5G-USIM/UICC уведомляет ME о том, что один или несколько новых закрытых ключей являются доступными (этап 4). Хотя на фиг.10 показано сообщение уведомления, включающее в себя закрытый(е) ключ(и), согласно другим вариантам осуществления, ME может альтернативно считывать ключ из 5G-USIM/UICC на основе уведомления. ME подтверждает уведомление (этап 5). ME затем сохраняет новый ключ(и) конфиденциальности в энергонезависимой памяти ME (этап 6). ME может заменить существующие данные закрытого ключа, если MCC/MNC/MSID идентичны в ранее сохраненных данных закрытого ключа.

На фиг.11 показан пример, в котором питание UE включено, и ME 9 обнаруживает, что 5G-USIM/UICC 8a был заменен (например, другим 5G-USIM/UICC или просто удален и повторно вставлен в соответствии с различными вариантами осуществления). Хотя в конкретных вариантах осуществления предусмотрена такая же замена другой 5G-USIM/UICC, как удаление и повторная вставка (например, по соображениям безопасности), другие варианты осуществления могут реагировать по-разному в зависимости от того, какой из этих двух сценариев обнаружен.

В соответствии с примером, показанным на фиг.10, включается питание UE 1 (этап

1). ME 9 отправляет сообщение 5G-USIM/UICC 8a (этап 2), и 5G-USIM/UICC отвечает способом, который не согласуется с тем, когда UE было предварительно включено (этап 3). Например, ответное сообщение может включать в себя SUPI, который отличается от любого ранее замеченного со стороны ME.

ME 9 определяет, что 5G-USIM/UICC 8a была заменена (этап 4). Например, 5G-USIM/UICC может несколько отличаться от предыдущего раза, когда было включено питание UE 1, указывая на то, что 5G-USIM/UICC была заменена на другую. В качестве альтернативы ME может обнаружить, что 5G-USIM/UICC был заменен с использованием энергонезависимой памяти, которая обновляется механическим, электрическим или программным механизмом, таким как оптический датчик, переключатель, датчик веса, датчик давления и/или электрическая схема, которая срабатывает при извлечении и/или вставке 5G-USIM/UICC, например, независимо от того, была ли удалена и повторно вставлена одна и та же или другая 5G-USIM/UICC.

ME 9 удаляет ранее сохраненный закрытый ключ из энергонезависимой памяти (если он есть). Дополнительно или альтернативно, если ME сохранил SUPI старой 5G-USIM/UICC с закрытым ключом в своей памяти, ME может принять решение относительно удаления закрытого ключа из энергонезависимой памяти на основании сравнения SUPI, возвращенного новой 5G-USIM/UICC 8a с SUPI, сохраненным со старым закрытым ключом.

В представленных выше конкретных вариантах осуществления описаны способы, по которым устройства в системе беспроводной связи могут безопасно обмениваться идентификатором подписки, включая выработку и использование конкретных структур данных и соответствующих схем шифрования/дешифрования. В частности, описанные выше варианты осуществления позволяют выполнять этот безопасный обмен как часть регистрации UE 1 в сети 30 беспроводной связи. Во многих таких вариантах осуществления предполагается, что UE инициализируется с помощью действительного закрытого ключа.

Чтобы гарантировать, что UE 1 фактически имеет действительный закрытый ключ, в дополнительных вариантах осуществления настоящего раскрытия описаны способы инициализации UE. Конкретные варианты осуществления, относящиеся к инициализации, могут включать в себя данные верификации закрытого ключа (MAC-P). Как показано в примере на фиг.12, MAC-P включает в себя код аутентификации сообщения (MAC). MAC вычисляется на основе закрытого ключа и ключа инициализации (что будет объяснено более подробно ниже). Например, MAC может быть вычислен по различным полям закрытого ключа, включая, но не ограничиваясь этим, открытый ключ домашней сети и связанные с ним параметры, как описано выше, в сочетании с ключом инициализации.

Согласно некоторым вариантам осуществления MAC-P может также включать в себя идентификатор ключа инициализации (например, RAND) и/или идентификатор алгоритма защиты целостности. Согласно некоторым вариантам осуществления, в которых MAC-P не включает в себя идентификатор алгоритма защиты целостности, алгоритм защиты целостности, который должен использоваться, может быть идентифицирован отдельно от MAC-P, или может использоваться заданная функция получения ключа (KDF), такая, например, как HMAC-SHA-256. MAC-P может дополнительно или альтернативно включать в себя поле счетчика, которое может использоваться для идентификации MAC-P из множества MAC-P (например, в случаях, когда вычисляется более одного MAC-P с использованием одного и того же ключа инициализации). Взаимосвязь между закрытым ключом (например, как показано на

фиг.4) и MAC-P (например, как показано на фиг.12) дополнительно поясняется ниже со ссылкой на фиг.15.

Ключ инициализации является закрытым общим ключом между UE 1 и PKPF 10 (смотри фиг.13), что более подробно описано ниже. Ключ инициализации является специфичным для UE, то есть ключом, который в домашней сети 3 связан с UE и/или 5G USIM, UICC 8a или любым другим аппаратным средством в UE/ME, в котором разрешено хранение SIM/USIM. В некоторых вариантах осуществления ключ инициализации может быть получен из главного ключа домашней сети, например, KAUSF в сети 5G или будущей сети, созданного, например, в 5G AKA, EAP-AKA' и EAP-TLS (расширяемый протокол аутентификации - безопасность транспортного уровня), который создается при аутентификации UE 1 в сети. В некоторых таких вариантах осуществления AUSF может иметь главный ключ домашней сети. Кроме того, новый главный ключ домашней сети может быть создан при повторной аутентификации UE.

В соответствии с одним примером ключ инициализации может быть создан из ключа шифрования (CK), ключа целостности (IK) (например, путем применения KDF, такого как HMAC-SHA-256, или другой безопасной односторонней хэш-функции, такой как SHA-256, или конкатенации CK и IK). Ключ инициализации, в качестве альтернативы прямой выработке из главного ключа или CK/IK, может быть выработан из CK' и IK' так же, как он вырабатывается из CK и IK в способе EAP-AKA'. В другой альтернативе ключ инициализации может быть выработан из EMSK (расширенного главного ключа сеанса) в случае EAP-TLS, как указано в RFC5216. Так как один и тот же главный ключ домашней сети может использоваться для получения множества ключей, варианты осуществления настоящего раскрытия используют по меньшей мере один дополнительный стандартный параметр в сочетании с главным ключом домашней сети в качестве входных данных для получения ключа инициализации. Например, при использовании стандартной KDF в качестве входных данных может использоваться функциональный код (FC) (например, как указано в TS 33.220, например, TS33.220 V15.0.0), чтобы создать ключ инициализации, который можно отличить от других ключей, созданных с использованием главного ключа домашней сети.

В соответствии с другим примером ключ инициализации может быть ключом, который является таким же как эфемерный общий ключ или получается из эфемерного общего ключа, который совместно используется SIDF 6 и UE 1, в частности, когда используемая схема шифрования является гибридной схемой открытого ключа, такой как ECIES. Например, ECIES использует механизм открытого ключа (например, Диффи-Хелмана) для согласования ключей, которое приводит к общему ключу, который является эфемерным, между SIDF и UE. В целях безопасности этот эфемерный общий ключ дополнительно обрабатывается, как правило, с помощью функции получения ключа (например, SHA-256), чтобы получить еще одни полученные общие ключи между SIDF и UE (например, ключ шифрования и ключ MAC в ECIES). Один из этих других полученных общих ключей, как правило, используется для шифрования и называется эфемерным ключом шифрования. Применительно к вариантам осуществления настоящего изобретения один из этих других полученных общих ключей может использоваться, например, для выработки SUCI из SUPI. Кроме того, в некоторых вариантах осуществления в качестве ключа инициализации может использоваться другой ключ из полученных общих ключей (например, ключ MAC в ECIES), новый дополнительный ключ, полученный из одного из полученных общих ключей, или еще один ключ, полученный из эфемерного общего ключа. В некоторых вариантах осуществления, в которых SIDF имеет или может получить/сформировать ключ

инициализации, SIDF позволяет также вычислять MAC или MAC-P.

PKPF 10 представляет собой функцию, расположенную в домашней сети 3, которая отвечает за инициализацию закрытого ключа. Согласно конкретным вариантам осуществления PKPF может быть совмещена с AUSF 5, и, в частности, по меньшей мере в некоторых вариантах осуществления, в которых ключ инициализации получается из главного ключа домашней сети, она создается на основе первичной аутентификации между UE и сетью. В других вариантах осуществления PKPF может быть совмещена с другими объектами 5GC, такими как UDM 7. Согласно еще одним вариантам осуществления PKPF является своим собственным отдельным объектом. В некоторых вариантах осуществления SIDF 6 и PKPF реализованы вместе как одна функция, и нет необходимости передавать ключ инициализации. В некоторых других вариантах осуществления PKPF может получить ключ инициализации из SIDF. PKPF может также получать MAC/MAC-P из SIDF.

На фиг.13 показан пример процесса регистрации UE, в котором UE 1 не имеет действительного закрытого ключа. Например, конечный пользователь, возможно, вставил новый USIM/UICC в UE, и этот новый USIM/UICC не содержит закрытый ключ.

В соответствии с примером, показанным на фиг.13, UE 1 отправляет запрос регистрации в AMF/SEAF 4, включая SUCI, в запросе (этап 1). Так как в этом сценарии UE изначально не имеет закрытого ключа, UE использует способ нулевой схемы или нулевого шифрования для создания SUCI. Нулевая схема реализована таким образом, что она возвращает одинаковые выходные данные в качестве входных данных, и они применяются как при шифровании в UE, так и при дешифровании с помощью SIDF 6. Кроме того, так как UE не имеет закрытого ключа, который указывал бы на способ нулевой схемы или нулевого шифрования (который домашняя сеть может свободно выбирать согласно вариантам осуществления), согласно конкретным вариантам осуществления может использоваться явный или неявный индикатор того, что действительный закрытый ключ отсутствует в UE. Например, как обсуждено выше, SUCI может использовать нулевую схему шифрования для зашифрованной части, которая может неявно сигнализировать об отсутствии закрытого ключа. Альтернативно, индикатор «отсутствие закрытого ключа» может быть выражен, например, стандартизированным или общеизвестным значением идентификатора открытого ключа, флагом и/или индикатором типа сообщения (например, запросом регистрации типа «инициализация конфиденциальности» или «предначальная регистрация»).

AMF/SEAF 4, получив запрос на регистрацию, запрашивает аутентификацию UE у AUSF 5/PKPF 10 (этап 2). AUSF отправляет SUCI (и индикатор «отсутствие закрытого ключа», если он был включен в запрос аутентификации) в SIDF 6 (этап 3). Согласно вариантам осуществления, в которых SIDF совмещена с UDM 7 (например, сообщение Nxx представляет собой сообщение N13), то такое же сообщение может использоваться для запроса вектора/учетных данных аутентификации из UDM.

SIDF 6 видит, что SUCI находится в незашифрованном тексте и что в UE 1 отсутствует закрытый ключ. Согласно этому примеру, SIDF имеет локальную политику, согласно которой все SUCI должны быть защищены с использованием ECIES. Соответственно, SIDF возвращает SUPI в AUSF вместе с запросом на инициализацию закрытого ключа ECIES для UE (этап 4). В некоторых вариантах осуществления ответ включает в себя множество закрытых ключей, которые должны быть инициализированы в UE. Согласно вариантам осуществления, в которых SIDF находится в UDM 7, одно и то же сообщение может быть использовано для возврата вектора/учетных данных аутентификации в AUSF 5.

Согласно вариантам осуществления, в которых AUSF 5 еще не приняла вектор/учетные данные аутентификации от UDM 7, AUSF 5 может запросить упомянутый вектор/учетные данные аутентификации из UDM перед началом аутентификации с UE (не показано). В качестве альтернативы, согласно вариантам осуществления, в которых AUSF уже приняла вектор/учетные данные аутентификации от UDM, AUSF и UE обмениваются аутентификационными сообщениями с использованием упомянутых векторов/учетных данных аутентификации (этап 5). В качестве альтернативы, AUSF может делегировать аутентификацию AMF/SEAF 4.

Согласно этому примеру PKPF 10 совмещена с AUSF 5. Следовательно, после успешной аутентификации AUSF/PKPF создает ключ инициализации, который может использоваться для защиты сообщения ключ инициализации закрытого ключа для UE 1, то есть без необходимости обмена сигнализацией для передачи ключа инициализации. Согласно другим вариантам осуществления, в которых AUSF и PKPF не совмещены, AUSF может запросить, чтобы был выработан ключ инициализации PKPF, и PKPF в ответ на это может передать ключ инициализации в AUSF (не показано).

AUSF 5/PKPF 10 защищает закрытый(е) ключ(и) (полученный(е) от SIDF 6 на этапе 4) с помощью ключа инициализации путем вычисления MAC (например, как описано выше со ссылкой на фиг.12) и построения MAC-P (этап 6). В некоторых вариантах осуществления секретный ключ также может быть зашифрован. В некоторых вариантах осуществления AUSF/PKPF может принять MAC и/или MAC-P от SIDF, как описано выше, в частности по меньшей мере в некоторых вариантах осуществления, в которых ключ инициализации основан на эфемерном общем ключе, например, схемы EICES. В частности, как обсуждено выше, SIDF может вырабатывать MAC и/или MAC-P.

AUSF 5 затем возвращает SUPI, закрытый(е) ключ(и) и MAC-P в AMF/SEAF 4 (этап 7). В некоторых вариантах осуществления SUPI, закрытый(е) ключ(и) и/или MAC-P передаются в AMF/SEAF в одном и том же потоке сообщений, связанных с регистрацией, для регистрации UE 1 в сети 30 беспроводной связи. В некоторых вариантах осуществления SUPI, закрытый(е) ключ(и) и/или MAC-P передаются в AMF/SEAF в отдельном потоке сообщений (не показано).

Согласно вариантам осуществления, в которых AUSF 5 делегировала аутентификацию UE 1 в AMF/SEAF 4, AMF/SEAF может в этот момент аутентифицировать UE (не показано). В таких вариантах осуществления AMF/SEAF, возможно, ранее приняла SUPI, закрытый(е) ключ(и) и MAC-P, например, напрямую из SIDF 6 на этапе 4.

AMF/SEAF 4 принимает регистрацию UE 1 и пересылает закрытый(е) ключ(и) и MAC-P в UE, например, в сообщении о принятии регистрации (этап 8). UE затем пытается верифицировать MAC и в случае положительного результата сохраняет секретный(е) ключ(и). Для верификации MAC UE создает тот же ключ инициализации, что и AUSF 5/PKPF 10 выполнила ранее. Другими словами, когда UE вырабатывает ожидаемый MAC и затем сравнивает его с принятым MAC, MAC верифицируется, если ожидаемый MAC считается таким же, как принятый MAC.

В некоторых вариантах осуществления UE 1 затем отключается от сети (этап 9), например, чтобы начать новую процедуру регистрации с использованием инициализированного закрытого ключа для того, чтобы скрыть свой идентификатор абонента, согласно одному из вариантов осуществления, описанных выше. Таким образом, отключение и повторная регистрация могут помешать злоумышленнику, например, установить связь SUPI с временным идентификатором UE.

В некоторых вариантах осуществления UE 1 может потребоваться инициализация закрытого ключа из-за истечения срока действия или недействительности закрытого

ключа, который ранее был инициализирован в UE. На фиг.14 показан пример процесса регистрации UE, в котором закрытый ключ UE необходимо обновить, например, по какой-либо причине безопасности или эксплуатации. Некоторые причины того, что ранее инициализированный закрытый ключ, возможно, потребуется обновить, в соответствии с различными вариантами осуществления, могут заключаться в том, что ранее инициализированная конфиденциальность могла достичь (или достигает) даты истечения своего срока действия, в некоторых случаях безопасность в сети 30 беспроводной связи была нарушена некоторым образом, и/или секретный ключ подлежит регулярным обновлениям.

В соответствии с примером, показанным на фиг.14, UE 1 отправляет запрос регистрации в AMF/SEAF 4 (этап 1). Запрос на регистрацию включает в себя SUCI. В этом примере, так как UE имеет закрытый ключ, UE использует схему или способ шифрования (например, ECIES) для создания SUCI, например, согласно одному из вариантов осуществления, описанных выше.

AMF/SEAF 4 запрашивает аутентификацию UE у AUSF 5/PKPF 10 (этап 2). AUSF отправляет SUCI в SIDF 6 (этап 3). Как и в предыдущем примере, согласно некоторым вариантам осуществления, в которых SIDF совмещена с UDM 7, одно и то же сообщение может использоваться для запроса вектора/учетных данных аутентификации из UDM.

SIDF 6 видит, что SUCI зашифрован закрытым ключом, который необходимо обновить. Например, SIDF может обнаружить, что срок действия закрытого ключа истек или скоро истечет, или что закрытый ключ недействителен по любой другой причине, как обсуждалось ранее. SIDF возвращает SUPI в AUSF 5 вместе с запросом на инициализацию обновленного закрытого ключа ECIES для UE (этап 4). Согласно некоторым вариантам осуществления ответ может включать в себя несколько закрытых ключей. Кроме того, как обсуждалось ранее, согласно некоторым вариантам осуществления, в которых SIDF расположен в UDM, одно и то же сообщение может использоваться для возврата вектора/учетных данных аутентификации в AUSF.

AUSF 5 и UE 1 обмениваются аутентификационными сообщениями, используя векторы/учетные данные аутентификации, принятые из UDM 7 (этап 5). Как обсуждалось в предыдущих примерах, AUSF, возможно, получила требуемый вектор/учетные данные аутентификации от UDM уже на этапе 4 (например, в некоторых вариантах осуществления, в которых SIDF 6 расположена в UDM), или AUSF может запросить такой вектор/учетные данные аутентификации из UDM перед началом аутентификации с помощью UE.

Согласно вариантам осуществления, в которых PKPF 10 совмещена с AUSF 5, AUSF/PKPF может создавать ключ инициализации, используемый для защиты сообщения ключ инициализации закрытого ключа для UE 1, в результате успешной аутентификации. Например, процедура аутентификации может включать в себя создание главного ключа домашней сети, который может использоваться для получения ключа инициализации. Альтернативно, в вариантах осуществления, в которых PKPF и AUSF не совмещены, AUSF и PKPF могут обмениваться ключом инициализации посредством соответствующего обмена сообщениями (не показаны).

AUSF 5/PKPF 10 защищает закрытый(е) ключ(и) (принятый(е) из SIDF 6 на этапе 4) с помощью ключа инициализации путем вычисления MAC и построения MAC-P, например, в соответствии с примером, показанным на фиг.14 (этап 6). Как обсуждено выше, в некоторых вариантах осуществления AUSF/PKPF может принимать MAC и/или MAC-P из SIDF, как описано выше, в частности, по меньшей мере в некоторых вариантах осуществления, в которых ключ инициализации основан на эфемерном общем ключе,

например, на схеме EICES. В частности, как обсуждено выше, SIDF может вырабатывать MAC и/или MAC-P.

После успешной аутентификации AUSF 5 отправляет SUPI, закрытый(е) ключ(и) и MAC-P в AMF/SEAF 4 (этап 7), например, в одном и том же потоке сообщений, связанных с регистрацией. В других вариантах осуществления могут использоваться отдельные потоки сообщений для одного или нескольких из SUPI, закрытого ключа (ключей) или MAC-P. К тому же, как обсуждалось ранее, AUSF может делегировать аутентификацию UE SEAF, и в этом случае SUPI, закрытый(е) ключ(и) и MAC-P могут быть возвращены SEAF уже на этапе 4, и AUSF выполняет аутентификацию, как описано ранее.

AMF/SEAF 4 принимает регистрацию UE 1 и пересылает закрытый(е) ключ(и) и MAC-P в UE, например, в сообщении о принятии регистрации (этап 8). UE создает тот же ключ инициализации из первичной аутентификации, что и AUSF 5/PKPF 10, и верифицирует MAC в сообщении. Если верификация является успешной, UE сохраняет закрытый(е) ключ(и). Старый закрытый ключ также может быть удален.

Согласно еще одному примеру AUSF 5 вырабатывает MAC и MAC-P и отправляет закрытый(е) ключ(и) и MAC-P в UE 1 через UDM 7, который пересылает закрытый(е) ключ(и) и MAC-P в AMF, которая затем пересылает закрытый(е) ключ(и) и MAC-P в UE 1. В таком примере AUSF может быть домашней наземной сетью мобильной связи AUSF, и в этом случае AMF может быть AMF гостевой наземной сети мобильной связи общего пользования (VPLMN). В данном случае AUSF может делегировать аутентификацию в AMF VPLMN.

Как обсуждалось ранее, MAC может быть вычислен на основе закрытого ключа (например, как показано на фиг.4) и ключа инициализации для выработки MAC-P (например, как показано на фиг.12). В некоторых вариантах осуществления, в которых многочисленные закрытые ключи инициализируются в UE 1, один и тот же MAC может быть вычислен по всем ключам конфиденциальности, отправленным в одном и том же сообщении.

На фиг.15 показан пример того, как закрытый ключ и MAC-P связаны друг с другом, и какие параметры используются в качестве входных данных для расчета MAC (или ожидаемого MAC (XMAC), в зависимости от ситуации). Как показано на фиг.15, ключ инициализации и закрытый ключ используются для выработки MAC, который затем может использоваться в сочетании с другим закрытым ключом для обновления MAC, и так далее до тех пор, пока не будут обработаны все закрытые ключи. Как только все закрытые ключи будет обработаны, закрытый(е) ключ(и) и MAC могут быть отправлены в UE.

С учетом всего вышеизложенного, одно или несколько описанных выше устройств или функций могут быть реализованы с использованием примерных аппаратных средств, показанных на фиг.16. Примерные аппаратные средства включают в себя схему 11 обработки и схему 12 связи. Схема обработки коммуникативно связана со схемой связи, например, через одну или несколько шин. Схема обработки может содержать один или несколько микропроцессоров, микроконтроллеров, аппаратных схем, дискретных логических схем, аппаратных регистров, процессоров цифровых сигналов (DSP), программируемых пользователем вентильных матриц (FPGA), специализированных интегральных схем (ASIC) или их комбинаций. Например, схема обработки может представлять собой программируемые аппаратные средства, способные выполнять программные инструкции, хранящиеся, например, в виде машиночитаемой компьютерной программы 133 в схеме 13 памяти. Схема памяти в различных вариантах осуществления может содержать любые невременные машиночитаемые носители,

которые известны в данной области техники или которые могут быть выполнены энергозависимыми или энергонезависимыми, включая, но не ограничиваясь этим, твердотельные носители (например, SRAM, DRAM, DDRAM, ROM, PROM, EPROM, флэш-память, твердотельный накопитель и т.д.), съемные устройства памяти (например, защищенная цифровая карта памяти (SD), карта мини-SD, карта микро-SD, карта памяти, флэш-накопитель, флэш-накопитель USB, картридж ROM, универсальный дисковый накопитель), фиксированный диск (например, магнитный жесткий диск), или тому подобное, полностью или в любой комбинации. Согласно конкретным вариантам осуществления, в которых аппаратные средства используются для реализации UE 1, схема памяти может содержать защищенный от несанкционированного доступа компонент 8 аппаратных средств, обеспечивающий безопасное хранение, такой как 5G-USIM и/или UICC 8a.

Схема 12 связи может быть концентратором контроллера, выполненным с возможностью управления входными и выходными (I/O) трактами передачи данных аппаратных средств. Такие входные и выходные тракты передачи данных могут включать в себя тракты передачи данных для обмена сигналами по сети 30 беспроводной связи. Например, схема связи может содержать приемопередатчик, выполненный с возможностью отправки и приема сигналов сотовой связи внутри и/или между UE 1, обслуживающей сетью 2 и/или домашней сетью 3, например, по воздушной, электрической и/или оптической среде.

Схема 12 связи может быть реализована в виде единого физического компонента или в виде многочисленных физических компонентов, которые расположены непрерывно или раздельно, и любой из которых может быть коммуникативно связан с любым другим или может поддерживать связь с любым другим через схему 11 обработки. Например, схема связи может содержать схему передатчика, выполненную с возможностью отправки сигналов сотовой связи, и схему приемника, выполненную с возможностью приема сигналов сотовой связи (не показаны).

Согласно конкретным вариантам осуществления аппаратные средства, показанные на фиг.16, могут быть сконфигурированы с множеством компонентов. Эти компоненты могут включать в себя множество коммуникативно связанных аппаратных блоков и/или программных модулей. Один или несколько аппаратных блоков могут быть, например, частью схемы 11 обработки. Один или несколько программных блоков могут, например, храниться в схеме 13 памяти и исполняться схемой обработки. Например, такие аппаратные средства, которые показаны на фиг.16, могут использоваться для реализации сервера 14 аутентификации (например, AMF, SEAF 4, AUSF 5) в домашней сети 3 UE 1 и сконфигурированы с примерными компонентами, показанными на фиг.17, с тем чтобы получить идентификатор подписки, такой как SUPI, UE. Компоненты на фиг.17 включают в себя блок или модуль 15 определения и интерфейсный блок или модуль 16. Блок или модуль определения выполнен с возможностью определения сервера 19 дешифрования, который будет использоваться для дешифрования зашифрованной части SUCI, и на основе информации, принятой из UE, которая будет использоваться многочисленными серверами дешифрования для дешифрования по меньшей мере части скрытого идентификатора подписки абонента (SUCI), в которой зашифрован идентификатор подписки. Интерфейсный блок или модуль выполнен с возможностью отправки SUCI в определенный сервер дешифрования и приема в ответ на это идентификатора подписки, например, SUPI. Другими словами, интерфейсный блок выполнен с возможностью также принимать SUCI, выработанный UE, где SUCI содержит зашифрованную часть, в которой зашифрована по меньшей

мере часть SUPI, и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования SUPI в SUCI.

Такой сервер 14 аутентификации может быть дополнительно или альтернативно сконфигурирован с примерными компонентами, показанными на фиг.18, для инициализации UE 1. Компоненты, показанные на фиг.18, включают в себя блок или модуль 17 получения и блок или модуль 18 передачи. Блок или модуль получения выполнен с возможностью получения кода аутентификации сообщения (MAC) на основе ключа инициализации, характерного для UE 1, и закрытого ключа домашней сети 3 UE. Блок или модуль передачи выполнен с возможностью передачи закрытого ключа и MAC в UE.

Такой сервер 14 аутентификации может быть дополнительно выполнен с возможностью дополнительного или альтернативного выполнения любого из способов, описанных в данном документе, по отношению к серверу аутентификации, например, с использованием любого из вышеописанных аппаратных или программных компонентов сервера аутентификации.

Другие аппаратные средства в соответствии с примером, показанным на фиг.16, могут использоваться для реализации сервера 19 дешифрования (например, SIDF 6) для передачи идентификатора подписки UE 1 на сервер 14 аутентификации и могут быть сконфигурированы с примерными компонентами, показанными на фиг.19. Компоненты, показанные на фиг.19, включают в себя блок или модуль 20 приема, блок или модуль 21 дешифрования и блок или модуль 22 отправки. Блок или модуль приема выполнен с возможностью приема из сервера аутентификации SUCI, который содержит зашифрованную часть, в которой зашифрована по меньшей мере часть SUPI, и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования SUPI в SUC, и который поддерживается сервером дешифрования. Блок или модуль дешифрования выполнен с возможностью дешифрования по меньшей мере части SUCI с использованием схемы шифрования, указанной идентификатором схемы шифрования, для получения SUPI. Блок или модуль отправки выполнен с возможностью отправки SUPI на сервер аутентификации.

Такой сервер 19 дешифрования может быть дополнительно или альтернативно сконфигурирован с примерными компонентами, показанными на фиг.20, для инициализации UE 1. Компоненты, показанные на фиг.20, включают в себя блок или модуль 23 выработки и блок или модуль 24 передачи. Блок или модуль выработки выполнен с возможностью выработки постоянного идентификатора подписки абонента (SUPI) и закрытого ключа для UE, реагирующего на прием из сервера 14 аутентификации скрытого идентификатора подписки абонента (SUCI) UE, который указывает, что UE не имеет действительного закрытого ключа. Блок или модуль передачи выполнен с возможностью передачи SUPI и закрытого ключа на сервер аутентификации. Таким образом, термин «сервер дешифрования» также может быть назван сервером дешифрования SUCI.

Такой сервер 19 дешифрования может быть дополнительно выполнен с возможностью дополнительного или альтернативного выполнения любого из способов, описанных в данном документе по отношению к серверу дешифрования, например, с использованием любого из вышеописанных аппаратных или программных компонентов сервера дешифрования.

Еще одни аппаратные средства в соответствии с примером, показанным на фиг.16,

могут использоваться для реализации UE 1 для безопасного уведомления сети 30 беспроводной связи об идентификаторе подписки и могут быть сконфигурированы с примерными компонентами, показанными на фиг.21. Компоненты, показанные на фиг.21, включают в себя блок или модуль 25 обработки и блок или модуль 26 передачи. Блок или модуль выработки выполнен с возможностью выработки SUCI, который содержит зашифрованную часть, в которой зашифрована по меньшей мере часть SUPI, и часть с незашифрованным текстом, которая содержит идентификатор домашней сети и идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования SUPI в SUCI. Блок или модуль передачи выполнен с возможностью передачи SUCI на сервер 14 аутентификации для пересылки SUCI на сервер 19 дешифрования, способный дешифровать SUPI.

Такое UE 1 может быть дополнительно или альтернативно сконфигурировано с помощью примерных компонентов, показанных на фиг.22, с тем чтобы получить закрытый ключ. Компоненты, показанные на фиг.22, включают в себя блок или модуль 27 приема и блок или модуль 28 верификации. Блок или модуль приема выполнен с возможностью приема закрытого ключа и кода аутентификации сообщения (MAC) из сервера 14 аутентификации. Блок или модуль верификации выполнен с возможностью верификации целостности закрытого ключа путем выработки ключа инициализации и использования ключа инициализации и закрытого ключа для воспроизведения MAC, принятого из сервера аутентификации, причем ключ инициализации является общим закрытым ключом между UE и сервером аутентификации.

Такое UE 1 может быть дополнительно выполнено с возможностью дополнительно или альтернативно выполнять любой из способов, описанных в данном документе по отношению к UE, например, с использованием любого из вышеописанных аппаратных или программных компонентов UE.

Различные способы и процессы, описанные в данном документе, могут быть реализованы способами, которые отличаются в некоторых деталях от обширных описаний, приведенных выше. Например, хотя этапы различных процессов или способов, описанных в данном документе, могут быть показаны и описаны как имеющие последовательность или временной порядок, этапы любых таких процессов или способов не ограничиваются выполнением в какой-либо конкретной последовательности или порядке, если не указано иное. Действительно, этапы в таких процессах или способах, как правило, могут выполняться в разнообразных различных последовательностях и порядках, в то же время, находясь в пределах объема настоящего раскрытия. Варианты осуществления, описанные в данном документе, следует рассматривать во всех отношениях как иллюстративные, а не ограничивающие. В частности, все изменения, находящиеся в диапазоне значений и эквивалентности перечисленных вариантов осуществления, прилагаемых ниже, предназначены для включения в них.

(57) Формула изобретения

1. Способ получения постоянного идентификатора подписки абонента (SUPI), выполняемый сервером аутентификации в домашней сети пользовательского оборудования (UE), причем SUPI является глобально уникальным идентификатором, назначенным абоненту, и SUPI содержит идентификатор домашней сети, идентифицирующий домашнюю сеть абонента, и идентификатор подписки, идентифицирующий подписку в домашней сети, причем способ содержит этапы, на которых:

принимают сервером аутентификации скрытый идентификатор подписки абонента

(SUCI), выработанный UE, причем SUCI содержит зашифрованную часть и часть с незашифрованным текстом, при этом a) зашифрованная часть SUCI, выработанного UE, содержит идентификатор подписки, идентифицирующий подписку в пределах домашней сети, но зашифрованная часть SUCI, выработанного UE, не включает в себя идентификатор домашней сети, и b) часть SUCI с незашифрованным текстом, выработанная UE, содержит i) идентификатор домашней сети, ii) идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования идентификатора подписки в SUCI, и iii) идентификатор открытого ключа для открытого ключа домашней сети, но часть с незашифрованным текстом SUCI, выработанного UE, не содержит идентификатор подписки;

определяют сервером аутентификации сервер дешифрования, подлежащий использованию для дешифрования зашифрованной части SUCI;

отправляют сервером аутентификации SUCI на сервер дешифрования и

после отправки сервером аутентификации SUCI на сервер дешифрования получают в ответ SUPI сервером.

2. Способ по п.1, в котором сервер дешифрования представляет собой один из множества серверов дешифрования и определение сервера дешифрования основано на информации, принятой от UE.

3. Способ по п.1, дополнительно содержащий этап, на котором принимают SUCI из UE как часть процедуры регистрации для регистрации UE в сети беспроводной связи.

4. Способ по п.1, дополнительно содержащий этап, на котором принимают SUCI из UE посредством запроса аутентификации от функции безопасности с привязкой.

5. Способ по п.1, дополнительно содержащий этап, на котором отправляют SUCI и запрос вектора аутентификации для аутентификации UE на определенный сервер дешифрования в одном и том же сообщении.

6. Способ по п.1, в котором

идентификатор домашней сети состоит из кода страны мобильной связи и кода сети мобильной связи и

идентификатор подписки представляет собой идентификационный номер абонента мобильной связи (MSIN).

7. Способ по п.1, в котором SUPI является идентификатором доступа к сети.

8. Способ по п.1, в котором схема шифрования представляет собой интегрированную схему шифрования на основе эллиптических кривых (ECIES).

9. Способ передачи постоянного идентификатора подписки абонента (SUPI) на сервер аутентификации, выполняемый сервером дешифрования, причем SUPI является глобально уникальным идентификатором, назначенным абоненту, и SUPI содержит идентификатор домашней сети, идентифицирующий домашнюю сеть абонента, и идентификатор подписки, идентифицирующий подписку в домашней сети, причем способ содержит этапы, на которых:

принимают сервером дешифрования из сервера аутентификации скрытый идентификатор подписки абонента (SUCI), выработанный UE, причем SUCI содержит зашифрованную часть и часть с незашифрованным текстом, при этом a) зашифрованная часть SUCI, выработанного UE, содержит идентификатор подписки, идентифицирующий подписку в домашней сети, но зашифрованная часть SUCI, выработанного UE, не включает в себя идентификатор домашней сети, и b) часть с незашифрованным текстом SUCI, выработанного UE, содержит i) идентификатор домашней сети, ii) идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования идентификатора подписки в SUCI, и iii) идентификатор открытого

ключа для открытого ключа домашней сети, но часть с незашифрованным текстом SUCI, выработанного UE, не содержит идентификатор подписки;

дешифруют сервером дешифрования зашифрованную часть SUCI с использованием схемы шифрования, указанной идентификатором схемы шифрования, для получения SUPI и

отправляют сервером дешифрования SUPI на сервер аутентификации.

10. Способ сокрытия постоянного идентификатора подписки абонента (SUPI), выполняемый пользовательским оборудованием (UE), причем SUPI является глобально уникальным идентификатором, назначенным абоненту, и SUPI содержит идентификатор домашней сети, идентифицирующий домашнюю сеть абонента, и идентификатор подписки, идентифицирующий подписку в домашней сети, причем способ содержит этапы, на которых:

вырабатывают при помощи UE скрытый идентификатор подписки абонента (SUCI), содержащий зашифрованную часть и часть с незашифрованным текстом, причем a) зашифрованная часть SUCI, выработанного UE, содержит идентификатор подписки, идентифицирующий подписку в домашней сети, но зашифрованная часть SUCI, выработанного UE, не включает в себя идентификатор домашней сети, и b) часть с незашифрованным текстом SUCI, выработанного UE, содержит i) идентификатор домашней сети, ii) идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования идентификатора подписки в SUCI, и iii) идентификатор открытого ключа для открытого ключа домашней сети, но часть с незашифрованным текстом SUCI, выработанного UE, не содержит идентификатор подписки; и

передают с помощью UE SUCI на сервер аутентификации для пересылки SUCI на сервер дешифрования, выполненный с возможностью дешифровать зашифрованную часть.

11. Способ по п.10, в котором SUCI передается в запросе на регистрацию в сети (30) беспроводной связи.

12. Способ по п.10, в котором на этапе выработки SUCI используют защищенный от несанкционированного доступа аппаратный компонент UE для выработки SUCI.

13. Способ по п.10, в котором на этапе передачи SUCI на сервер аутентификации передают SUCI на сервер аутентификации в ответ на сообщение запроса идентификатора, принятое от функции управления аутентификацией и мобильностью (AMF), как часть процедуры регистрации UE в сети беспроводной связи.

14. Способ по п.10, в котором схема шифрования представляет собой интегрированную схему шифрования на основе эллиптических кривых.

15. Пользовательское оборудование (UE) для сокрытия постоянного идентификатора подписки абонента (SUPI), причем SUPI является глобально уникальным идентификатором, назначенным абоненту, и SUPI содержит идентификатор домашней сети, идентифицирующий домашнюю сеть абонента, и идентификатор подписки, идентифицирующий подписку в домашней сети, причем UE содержит:

схему обработки и схему памяти, причем схема памяти содержит инструкции, исполняемые схемой обработки, при этом UE выполнено с возможностью:

выработки скрытого идентификатора подписки абонента (SUCI), содержащего зашифрованную часть и часть с незашифрованным текстом, причем a) зашифрованная часть SUCI, выработанного UE, содержит идентификатор подписки, идентифицирующий подписку в домашней сети, но зашифрованная часть SUCI, выработанного UE, не включает в себя идентификатор домашней сети, и b) часть с незашифрованным текстом

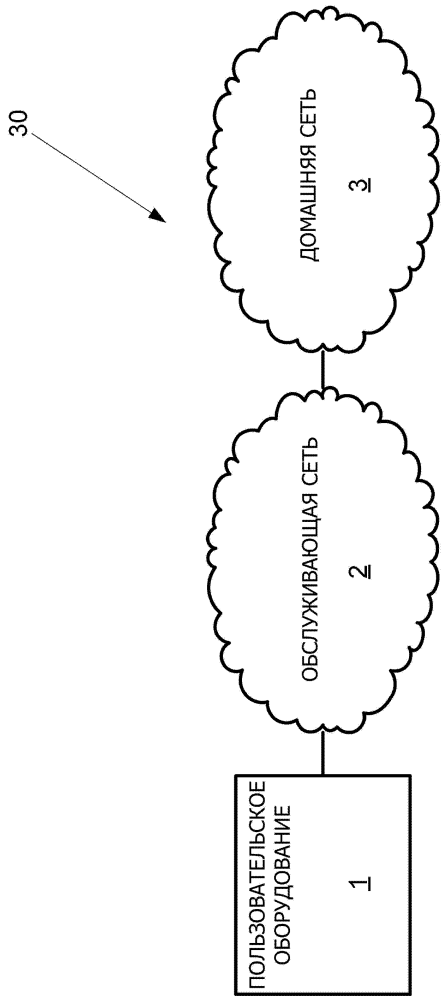
SUCI, выработанного UE, содержит i) идентификатор домашней сети, ii) идентификатор схемы шифрования, который идентифицирует схему шифрования, используемую UE для шифрования идентификатора подписки в SUCI, и iii) идентификатор открытого ключа для открытого ключа домашней сети, но часть с незашифрованным текстом SUCI, выработанного UE, не содержит идентификатор подписки; и

передачи SUCI на сервер аутентификации для пересылки SUCI на сервер дешифрования, выполненный с возможностью дешифровать SUPI.

16. UE по п.15, в котором SUPI содержит идентификационный номер абонента мобильной связи.

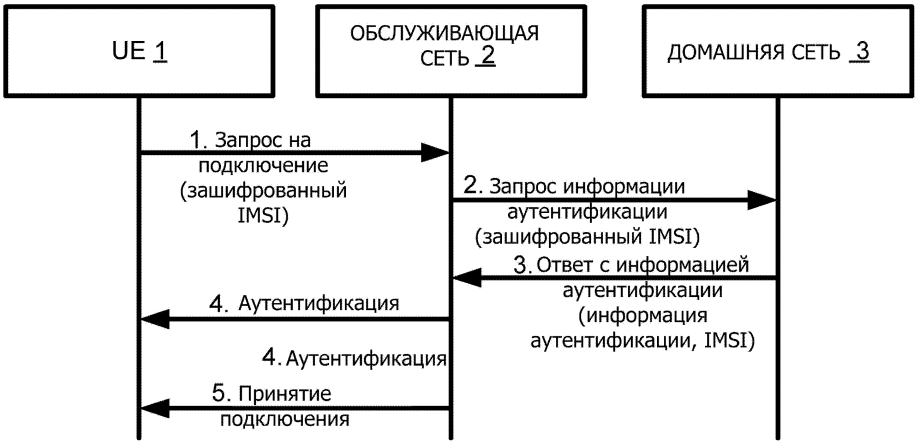
17. UE по п.15, в котором SUPI является идентификатором доступа к сети.

1

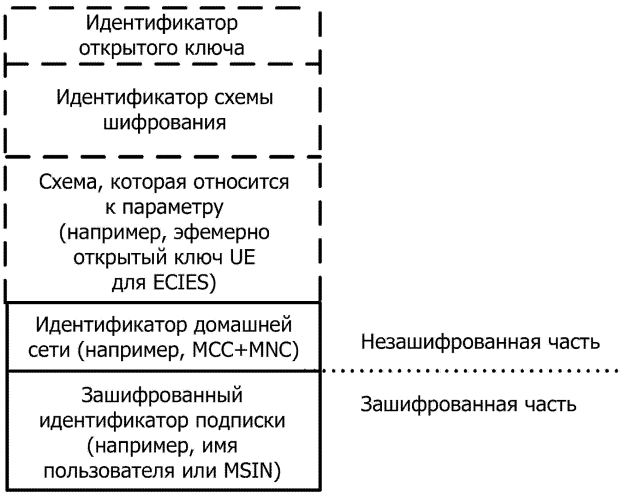

30
ДОМАШНЯЯ СЕТЬ
3
ОБСЛУЖИВАЮЩАЯ СЕТЬ
2
ПОЛЬЗОВАТЕЛЬСКОЕ ОБОРУДОВАНИЕ
1

Фиг. 1

2

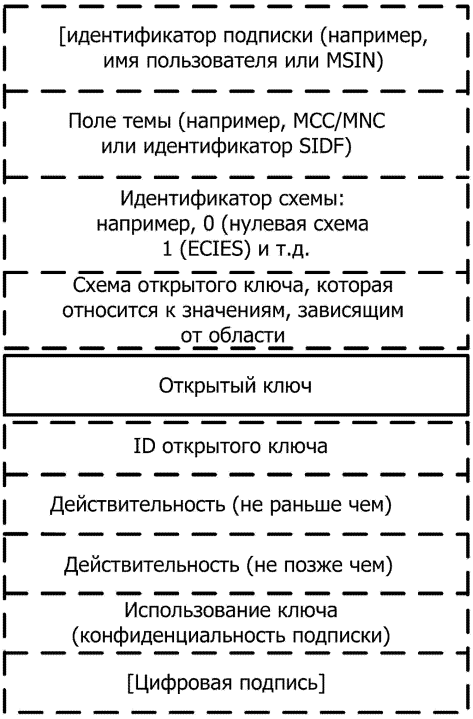

UE 1
ОБСЛУЖИВАЮЩАЯ СЕТЬ 2
ДОМАШНЯЯ СЕТЬ 3
1. Запрос на подключение (зашифрованный IMSI)
2. Запрос информации аутентификации (зашифрованный IMSI)
3. Ответ с информацией аутентификации (информация аутентификации, IMSI)
4. Аутентификация
4. Аутентификация
5. Принятие подключения

Фиг. 2

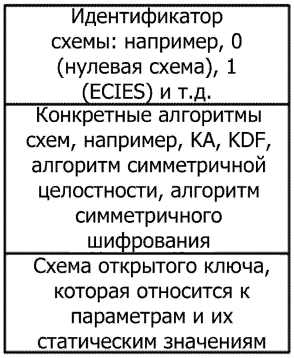

Идентификатор открытого ключа
Идентификатор схемы шифрования
Схема, которая относится к параметру (например, эфемерно открытый ключ UE для ECIES)
Идентификатор домашней сети (например, MCC+MNC)
Зашифрованный идентификатор подписки (например, имя пользователя или MSIN)
Незашифрованная часть
Зашифрованная часть

Фиг. 3

3

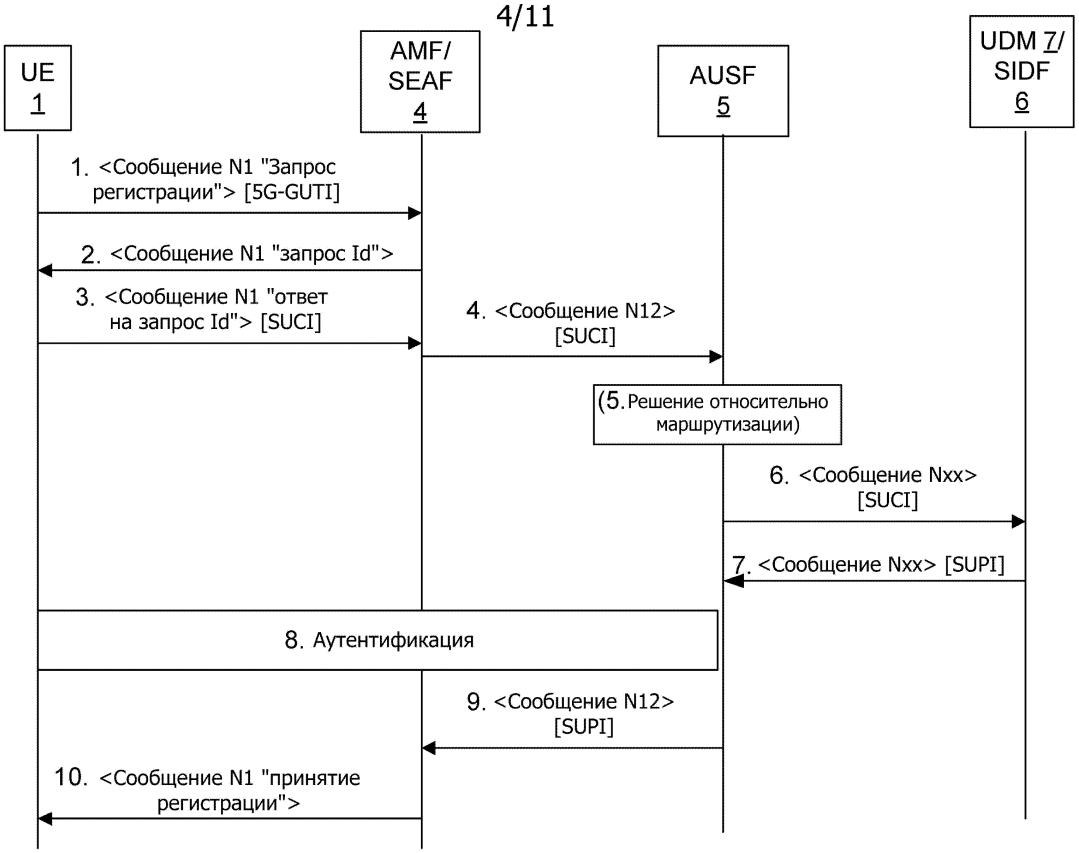

[идентификатор подписки (например, имя пользователя или MSIN)
Поле темы (например, MCC/MNC или идентификатор SIDF)
Идентификатор схемы: например, 0 (нулевая схема 1 (ECIES) и т.д.
Схема открытого ключа, которая относится к значениям, зависящим от области
Открытый ключ
ID открытого ключа
Действительность (не раньше чем)
Действительность (не позже чем)
Использование ключа (конфиденциальность подписки)
[Цифровая подпись]

Фиг. 4

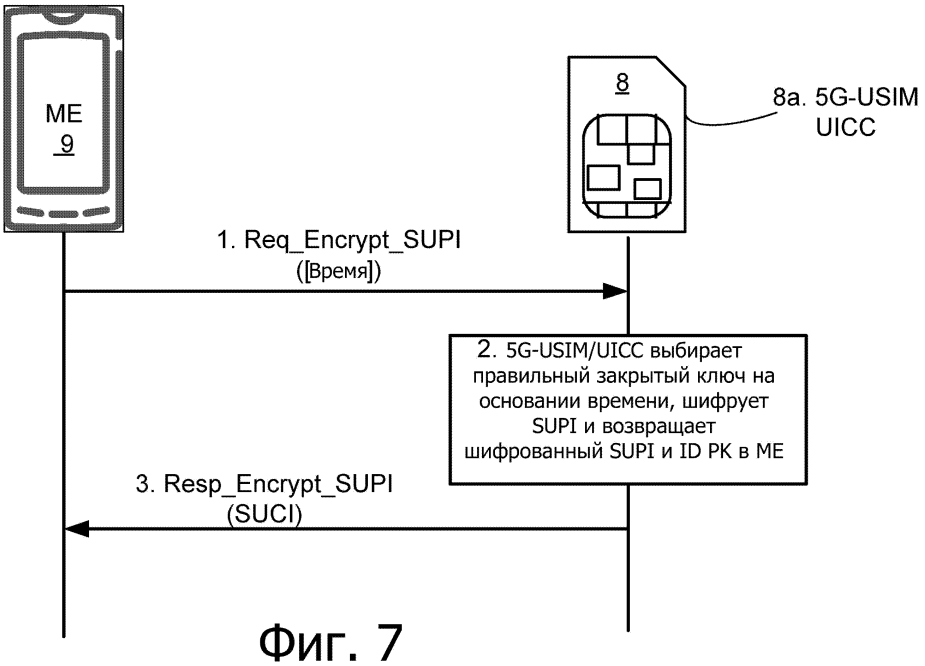

Идентификатор схемы: например, 0 (нулевая схема), 1 (ECIES) и т.д.
Конкретные алгоритмы схем, например, KA, KDF, алгоритм симметричной целостности, алгоритм симметричного шифрования
Схема открытого ключа, которая относится к параметрам и их статическим значениям

Фиг. 5

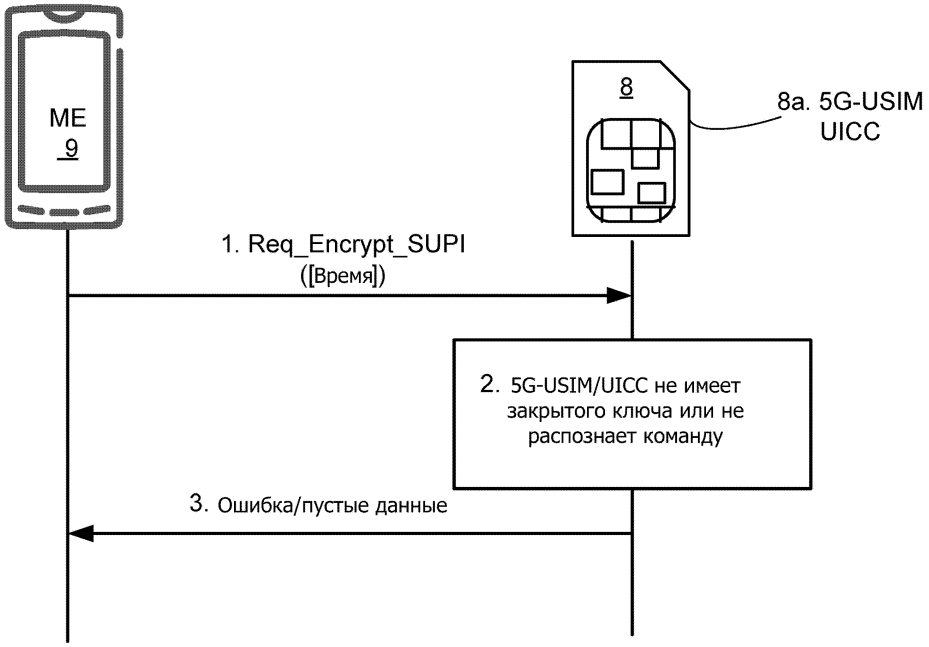
4


UE
1
AMF/
SEAF
4
AUSF
5
UDM 7/
SIDF
6
1. <Сообщение N1 "Запрос регистрации"> [5G-GUTI]
2. <Сообщение N1 "запрос Id">
3. <Сообщение N1 "ответ на запрос Id"> [SUCI]
4. <Сообщение N12> [SUCI]
(5. Решение относительно маршрутизации)
6. <Сообщение Nxx> [SUCI]
7. <Сообщение Nxx> [SUPI]
8. Аутентификация
9. <Сообщение N12> [SUPI]
10. <Сообщение N1 "принятие регистрации">
5

Фиг. 6

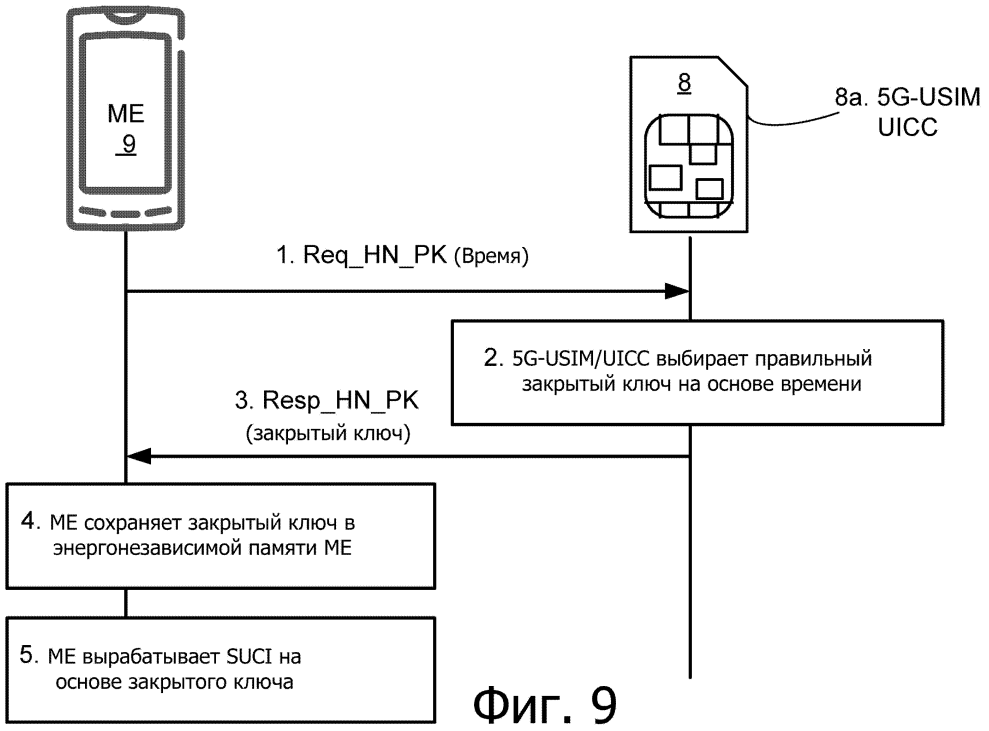

ME
9
8
8a. 5G-USIM
UICC
1. Req_Encrypt_SUPI
([Время])
2. 5G-USIM/UICC выбирает правильный закрытый ключ на основании времени, шифрует SUPI и возвращает шифрованный SUPI и ID PK в ME
3. Resp_Encrypt_SUPI
(SUCI)

Фиг. 7

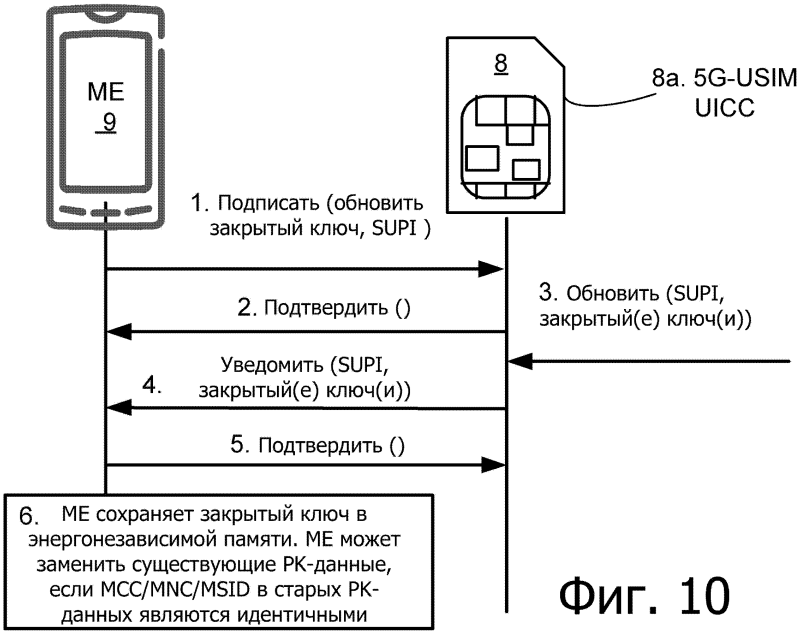

ME
9
8
8a. 5G-USIM
UICC
1. Req_Encrypt_SUPI
([Время])
2. 5G-USIM/UICC не имеет закрытого ключа или не распознает команду
3. Ошибка/пустые данные

Фиг. 8

6

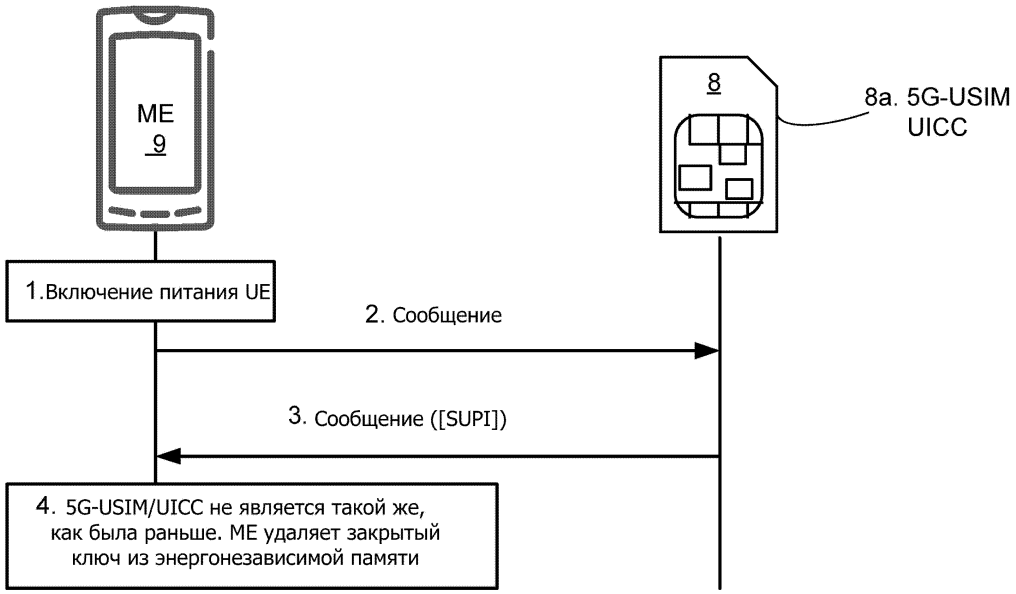

ME
9
8
8a. 5G-USIM
UICC
1. Req_HN_PK (Время)
2. 5G-USIM/UICC выбирает правильный закрытый ключ на основе времени
3. Resp_HN_PK
(закрытый ключ)
4. ME сохраняет закрытый ключ в энергонезависимой памяти ME
5. ME вырабатывает SUCI на основе закрытого ключа

Фиг. 9


ME
9
8
8a. 5G-USIM
UICC
1. Подписать (обновить закрытый ключ, SUPI)
2. Подтвердить ()
3. Обновить (SUPI, закрытый(е) ключ(и))
4. Уведомить (SUPI, закрытый(е) ключ(и))
5. Подтвердить ()
6. ME сохраняет закрытый ключ в энергонезависимой памяти. ME может заменить существующие PK-данные, если MCC/MNC/MSID в старых PK-данных являются идентичными

Фиг. 10

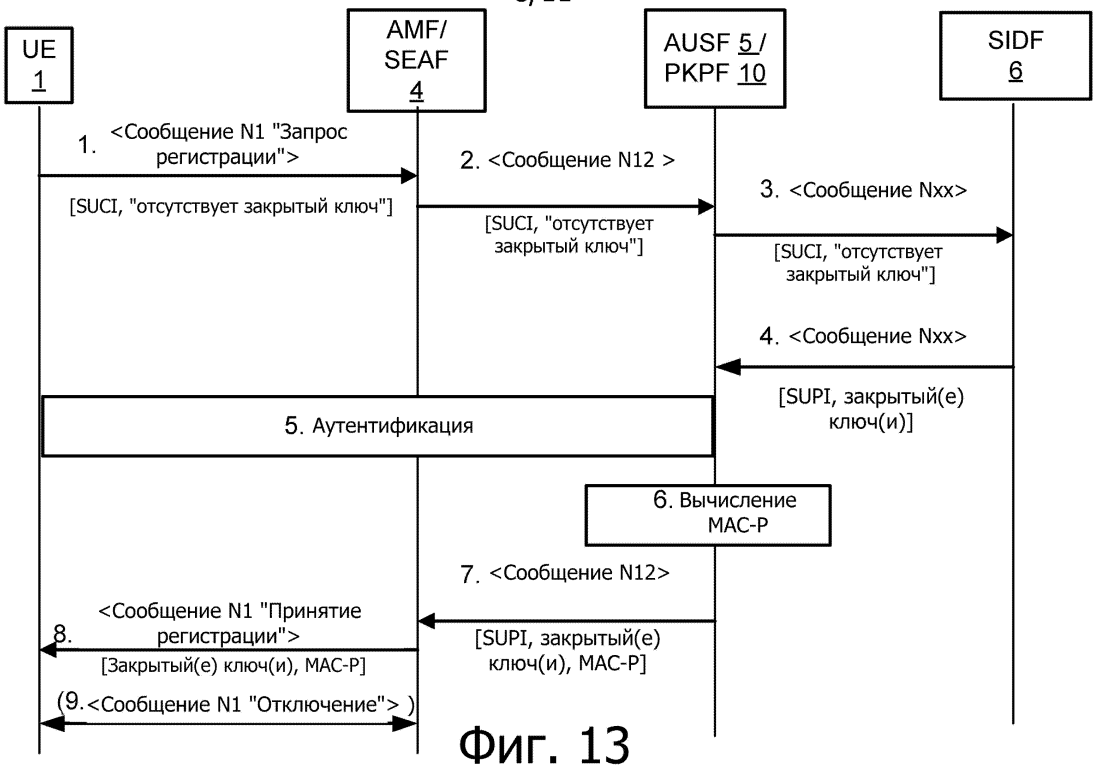
7



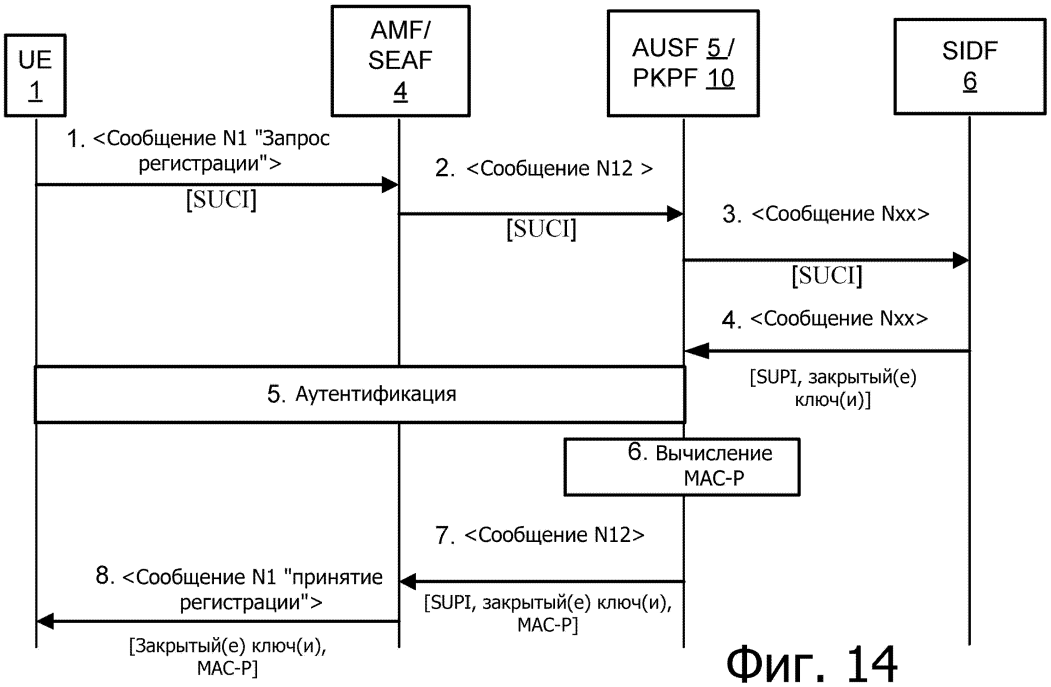
Фиг. 11

Фиг. 12

8

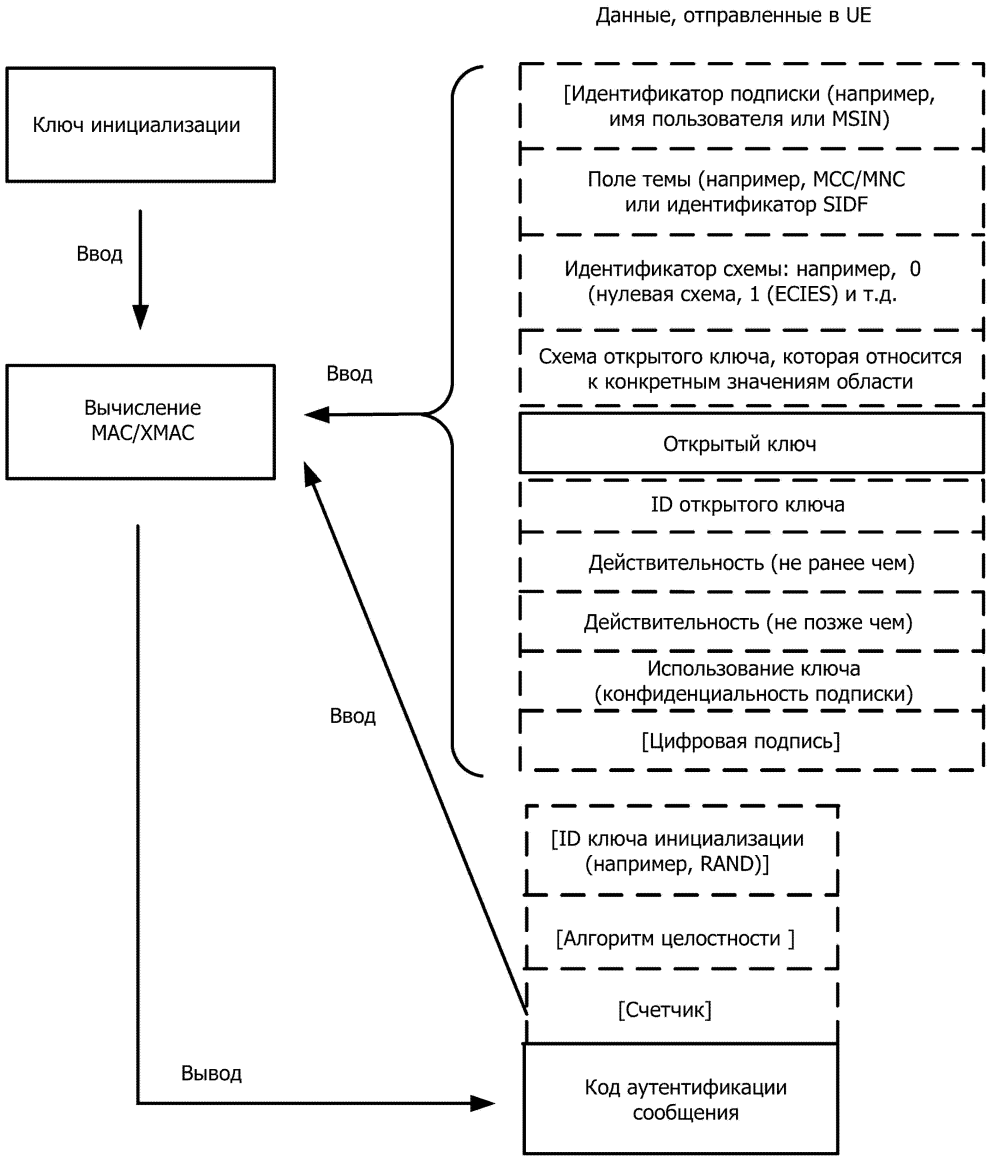


Фиг. 13

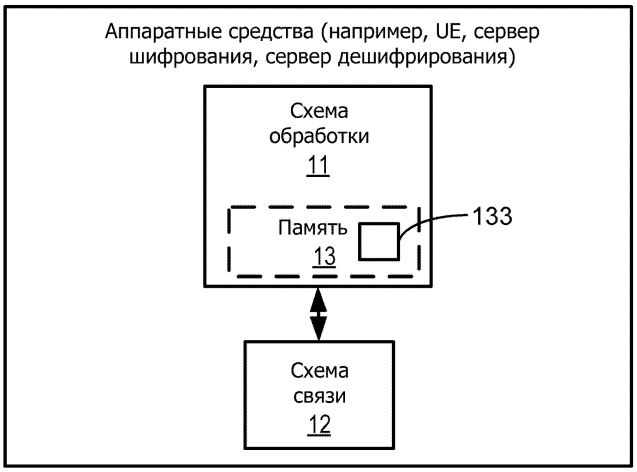


Фиг. 14

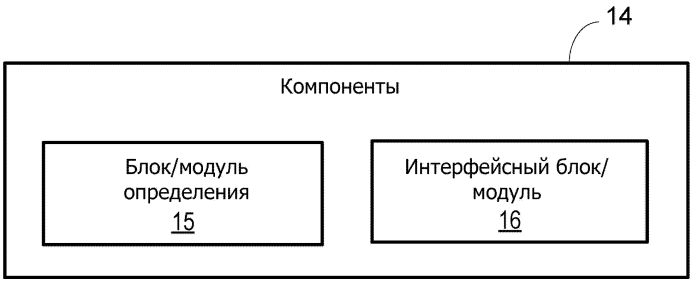
9


Данные, отправленные в UE
Ключ инициализации
Ввод
Вычисление MAC/XMAC
Ввод
Ввод
Вывод
[Идентификатор подписки (например, имя пользователя или MSIN)
Поле темы (например, MCC/MNC или идентификатор SIDF
Идентификатор схемы: например, 0 (нулевая схема, 1 (ECIES) и т.д.
Схема открытого ключа, которая относится к конкретным значениям области
Открытый ключ
ID открытого ключа
Действительность (не ранее чем)
Действительность (не позже чем)
Использование ключа (конфиденциальность подписки)
[Цифровая подпись]
[ID ключа инициализации (например, RAND)]
[Алгоритм целостности]
[Счетчик]
Код аутентификации сообщения

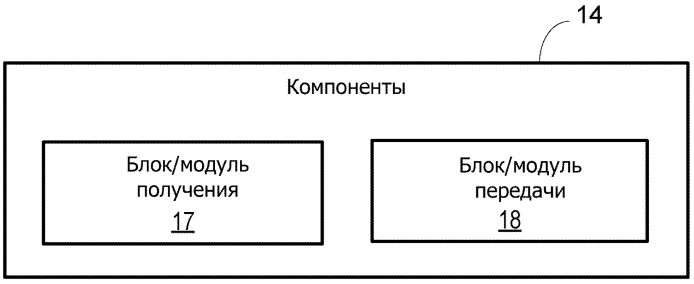
Фиг. 15



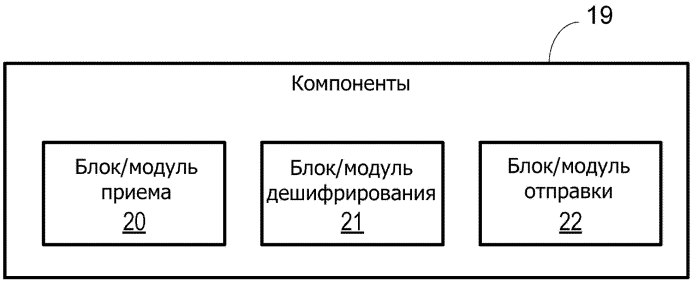
Фиг. 16



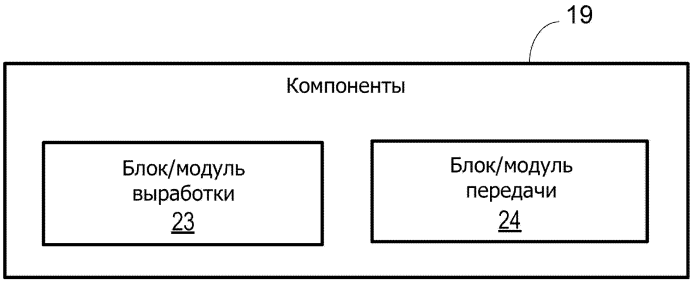
Фиг. 17



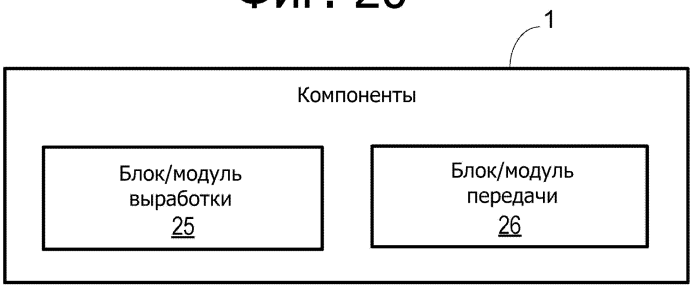
Фиг. 18



Фиг. 19



Фиг. 20



Фиг. 21

Фиг. 22