Зарегистрировано в Минюсте России 31 июля 2018 г. N 51741

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 25 июня 2018 г. N 319

ОБ УТВЕРЖДЕНИИ ПРАВИЛ ПРИМЕНЕНИЯ ОБОРУДОВАНИЯ КОММУТАЦИИ СЕТЕЙ ПОДВИЖНОЙ РАДИОТЕЛЕФОННОЙ СВЯЗИ. ЧАСТЬ VII. ПРАВИЛА ПРИМЕНЕНИЯ ОБОРУДОВАНИЯ КОММУТАЦИИ СТАНДАРТА LTE

В соответствии со статьей 41 и пунктом 2.1 статьи 12 Федерального закона от 7 июля 2003 г. N 126-ФЗ "О связи" (Собрание законодательства Российской Федерации, 2003, N 28, ст. 2895; N 52, ст. 5038; 2004, N 35, ст. 3607; N 45, ст. 4377; 2005, N 19, ст. 1752; 2006, N 6, ст. 636; N 10, ст. 1069; N 31, ст. 3431, ст. 3452; 2007, N 1, ст. 8; N 7, ст. 835; 2008, N 18, ст. 1941; 2009, N 29, ст. 3625; 2010, N 7, ст. 705; N 15, ст. 1737; N 27, ст. 3408; N 31, ст. 4190; 2011, N 7, ст. 901; N 9, ст. 1205; N 25, ст. 3535; N 27, ст. 3873, ст. 3880; N 29, ст. 4284, ст. 4291; N 30, ст. 4590; N 45, ст. 6333; N 49, ст. 7061; N 50, ст. 7351, ст. 7366; 2012, N 31, ст. 4322, ст. 4328; N 53, ст. 7578; 2013, N 19, ст. 2326; N 27, ст. 3450; N 30, ст. 4062; N 43, ст. 5451; N 44, ст. 5643; N 48, ст. 6162; N 49, ст. 6339, ст. 6347; N 52, ст. 6961; 2014, N 6, ст. 560; N 14, ст. 1552; N 19, ст. 2302; N 26, ст. 3366, ст. 3377; N 30, ст. 4229, ст. 4273; N 49, ст. 6928; 2015, N 29, ст. 4342, ст. 4383, ст. 4389; 2016, N 10, ст. 1316, ст. 1318; N 15, ст. 2066; N 18, ст. 2498; N 26, ст. 3873; N 27, ст. 4213, ст. 4221; N 28, ст. 4558; 2017, N 17, ст. 2457; N 24, ст. 3479; N 31, ст. 4742; N 50, ст. 7557; 2018, N 17, ст. 2419) и пунктом 4 Правил организации и проведения работ по обязательному подтверждению соответствия средств связи, утвержденных постановлением Правительства Российской Федерации от 13 апреля 2005 г. N 214 (Собрание законодательства Российской Федерации, 2005, N 16, ст. 1463; 2008, N 42, ст. 4832; 2012, N 6, ст. 687), приказываю:

1. Утвердить прилагаемые Правила применения оборудования коммутации сетей подвижной радиотелефонной связи. Часть VII. Правила применения оборудования коммутации стандарта LTE.

2. Признать утратившими силу:

приказ Министерства связи и массовых коммуникаций Российской Федерации от 06.06.2011 N 130 "Об утверждении Правил применения оборудования коммутации сетей подвижной радиотелефонной связи. Часть VII. Правила применения оборудования коммутации стандарта LTE" (зарегистрирован Министерством юстиции Российской Федерации 28 июня 2011 г., регистрационный N 21216);

пункт 3 Изменений, которые вносятся в приказы Министерства информационных технологий и связи Российской Федерации и Министерства связи и массовых коммуникаций Российской Федерации, утвержденных приказом Министерства связи и массовых коммуникаций Российской Федерации от 14.12.2015 N 543 "О внесении изменений в некоторые приказы Министерства информационных технологий и связи Российской Федерации и Министерства связи и массовых коммуникаций Российской Федерации" (зарегистрирован Министерством юстиции Российской Федерации 18 января 2016 г., регистрационный N 40606).

3. Признать не подлежащими применению:

подпункт 5 пункта 9.1 Правил применения оборудования коммутации систем подвижной радиотелефонной связи. Часть II. Правила применения оборудования коммутации сети подвижной радиотелефонной связи стандарта GSM 900/1800, утвержденных приказом Министерства информационных технологий и связи Российской Федерации от 31.05.2007 N 58 "Об утверждении Правил применения оборудования коммутации систем подвижной радиотелефонной связи. Часть II. Правила применения оборудования коммутации сети подвижной радиотелефонной связи стандарта GSM 900/1800" (зарегистрирован Министерством юстиции Российской Федерации 22 июня 2007 г., регистрационный N 9675);

подпункт 5 пункта 10.1 подпункт "в" пункта 10.3 Правил применения оборудования коммутации систем подвижной радиотелефонной связи. Часть V. Правила применения оконечно-транзитных узлов связи сетей подвижной радиотелефонной связи стандарта UMTS, утвержденных приказом Министерства информационных технологий и связи Российской Федерации от 27.08.2007 N 101 "Об утверждении Правил применения оборудования коммутации систем подвижной радиотелефонной связи. Часть V. Правила применения оконечно-транзитных узлов связи сетей подвижной радиотелефонной связи стандарта UMTS" (зарегистрирован Министерством юстиции Российской Федерации 29 августа 2007 г., регистрационный N 10066).

4. Установить, что настоящий приказ вступает в силу по истечении ста восьмидесяти дней после дня его официального опубликования, за исключением подпунктов 5 и 6 пункта 15 Правил применения оборудования коммутации сетей подвижной радиотелефонной связи. Часть VII. Правила применения оборудования коммутации стандарта LTE, утвержденных настоящим приказом, которые вступают в силу с 1 декабря 2019 года.

5. Направить настоящий приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

Министр
К.Ю.НОСКОВ

Утверждены
приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ПРАВИЛА ПРИМЕНЕНИЯ ОБОРУДОВАНИЯ КОММУТАЦИИ СЕТЕЙ ПОДВИЖНОЙ РАДИОТЕЛЕФОННОЙ СВЯЗИ. ЧАСТЬ VII. ПРАВИЛА ПРИМЕНЕНИЯ ОБОРУДОВАНИЯ КОММУТАЦИИ СТАНДАРТА LTE

I. Общие положения

1. Правила применения оборудования коммутации сетей подвижной радиотелефонной связи.

Часть VII. Правила применения оборудования коммутации стандарта LTE (далее - Правила) разработаны в целях обеспечения целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации.

2. Правила устанавливают требования к оборудованию коммутации стандартов LTE и (или) LTE-Advanced (далее - стандарт LTE), включая оборудование коммутации IMS, при оказании услуг передачи данных и телефонного соединения, в том числе требования к протоколам, обеспечивающим взаимодействие с узлами связи стандартов GSM 900/1800 и UMTS, а также к оборудованию коммутации стандарта LTE для взаимодействия с беспроводным доступом, отличным от стандартов GSM 900/1800, UMTS, LTE (далее - non-3GPP) и принадлежащим домашнему или визитному оператору сети подвижной радиотелефонной связи (далее - доверенный беспроводный доступ TWAN) или принадлежащим другой сети связи общего пользования (далее - ненадежный беспроводный доступ UTWAN).

3. Оборудование коммутации стандарта LTE идентифицируется как сложное телекоммуникационное оборудование коммутации сетей подвижной радиотелефонной связи и согласно пункту 8 Перечня средств связи, подлежащих обязательной сертификации, утвержденного постановлением Правительства Российской Федерации от 25 июня 2009 г. N 532 (Собрание законодательства Российской Федерации, 2009, N 26, ст. 3206; 2015, N 6, ст. 954), подлежит обязательной сертификации в порядке, установленном Правилами организации и проведения работ по обязательному подтверждению соответствия средств связи, утвержденными постановлением Правительства Российской Федерации от 13 апреля 2005 г. N 214 (Собрание законодательства Российской Федерации, 2005, N 16, ст. 1463; 2008, N 42, ст. 4832; 2012, N 6, ст. 687).

4. Правила распространяются на следующее оборудование стандарта LTE:

1) модуль управления мобильностью (Mobility Managemen Entity) (далее - MME);

2) обслуживающий шлюз (Serving Gateway) (далее - S-GW);

3) шлюз взаимодействия с сетями, использующими технологию с коммутацией пакетов (Packet Data Networks Gateway) (далее - PDN GW);

4) регистр идентификации оборудования (Equipment Identity Register) (далее - EIR);

5) сервер абонентских данных и/или центр аутентификации (Home Subscriber Server/Authentication Center) (далее - HSS/AuC);

6) обслуживающий узел поддержки GPRS (Serving GPRS Support Node) (далее - SGSN);

7) оборудование, реализующее функции реализации правил политики и тарификации (The Policy and Charging Rules Function) (далее - PCRF);

8) центр управления и технического обслуживания (далее - ЦУ и ТО);

9) оборудование коммутации IMS, выполняющее функции:

а) управления сеансом (далее - CSCF), при использовании прокси-сервера CSCF (далее - P-CSCF), обслуживающего CSCF (далее - S-CSCF), и запрашивающего CSCF (далее - I-CSCF);

б) сервера абонентских данных пользователей IMS (далее - HSS/IMS);

в) определения местонахождения подписки (далее - SLF);

г) управления медиашлюзами (далее - MGCF);

д) управления ресурсами мультимедиа (далее - MRFC);

е) процессора ресурсов мультимедиа (далее - MRFP);

ж) управления выбором сети (далее - BGCF);

з) управления пограничным взаимодействием (далее - IBCF);

и) учета данных для начисления платы (далее - CCF);

к) медиашлюза (далее - IMS-MGW);

л) переходного шлюза (далее - TrGw);

м) шлюза сигнализации (далее - SGF);

н) шлюза абонентского доступа (далее - IMS-AGW);

10) оборудование, реализующее функцию агента протокола Diameter (Diameter Agent) (далее - DA), для определения местонахождения пользователя, в случае наличия на сети оператора нескольких HSS.

11) оборудование 3GPP AAA сервер/прокси;

12) оборудование, реализующее функции доступа к оборудованию коммутации стандарта LTE из сети Интернет при использовании доступа UTWAN (далее - ePDG);

13) аппаратный модуль безопасности (далее - HSM) (в случае реализации криптографических алгоритмов аутентификации абонентов в отдельном аппаратном модуле безопасности).

При использовании оборудования IMS с территориально распределенной структурой с предоставлением услуг связи в различных территориально-административных образованиях интерфейсы IMS должны обеспечивать проведение оперативно-разыскных мероприятий независимо в каждом территориально-административном образовании в полном объеме.

5. Процедуру обязательной сертификации должно проходить как оборудование коммутации сетей подвижной радиотелефонной связи в составе входящего в него оборудования коммутации стандарта LTE, так и оборудование, приведенное в подпунктах 1 - 7, 9, 10, 13 пункта 4 Правил, в качестве самостоятельных средств связи, включая оборудование средств связи, в том числе программное обеспечение, обеспечивающее выполнение установленных действий при проведении оперативно-разыскных мероприятий.

Оборудование коммутации стандарта LTE должно обеспечивать возможность его использования одним или несколькими операторами сети подвижной радиотелефонной связи.

При использовании оборудования коммутации стандарта LTE несколькими операторами сети подвижной радиотелефонной связи каждый оператор должен обеспечивать возможность проведения оперативно-разыскных мероприятий в принадлежащем ему трафике.

II. Требования к оборудованию коммутации стандарта LTE

6. Электропитание оборудования коммутации стандарта LTE должно осуществляться в соответствии с требованиями к параметрам электропитания, установленными пунктами П. 9.1 - П. 9.4 приложения 9 к Правилам применения транзитных междугородных узлов автоматической коммутации. Часть I. Правила применения транзитных междугородных узлов связи, использующих систему сигнализации по общему каналу сигнализации N 7 (ОКС N 7), утвержденным приказом Министерства информационных технологий и связи Российской Федерации от 16.05.2006 N 59 (зарегистрирован Министерством юстиции Российской Федерации 29 мая 2006 г., регистрационный N 7879), с изменениями, внесенными приказом Министерства связи и массовых коммуникаций Российской Федерации от 23.04.2013 N 93 (зарегистрирован Министерством юстиции Российской Федерации 14 июня 2013 г., регистрационный N 28788) (далее - Правила N 59-06) или от сети переменного тока с номинальным напряжением 220 В, частотой 50 Гц.

Оборудование электропитающей установки (далее - ЭПУ) не входит в состав оборудования коммутации стандарта LTE и должно соответствовать Правилам применения оборудования электропитания средств связи, утвержденным приказом Министерства информационных технологий и связи Российской Федерации от 03.03.2006 N 21 (зарегистрирован Министерством юстиции Российской Федерации 27 марта 2006 г., регистрационный N 7638), с изменениями, внесенными приказом Министерства связи и массовых коммуникаций Российской Федерации от 23.04.2013 N 93 (зарегистрирован Министерством юстиции Российской Федерации 14 июня 2013 г., регистрационный N 28788).

7. Оборудование коммутации стандарта LTE должно сохранять работоспособность при отклонении напряжения электропитания от номинальных значений в допустимых пределах:

(48,0 - 72,0) В при номинальном напряжении 60 В;

(40,5 - 57,0) В при номинальном напряжении 48 В;

(187 - 242) В при напряжении переменного тока 220 В (частота - (47,5 - 50,5) Гц, коэффициент нелинейных искажений - не более 10%, кратковременное (длительностью до 3 секунд) изменение напряжения относительно номинального значения $\pm$ 40%).

8. В оборудовании коммутации стандарта LTE должна быть предусмотрена система сигнализации для контроля неисправностей в ЭПУ.

9. Требования к параметрам устойчивости к внешним климатическим и механическим воздействиям для оборудования коммутации стандарта LTE приведены в приложении N 3 к Правилам применения оборудования коммутации систем подвижной радиотелефонной связи. Часть II. Правила применения оборудования коммутации сети подвижной радиотелефонной связи стандарта GSM 900/1800, утвержденным Приказом Министерства информационных технологий и связи Российской Федерации от 31.05.2007 N 58 (зарегистрирован Министерством юстиции Российской Федерации 22 июня 2007 г., регистрационный N 9675), с изменениями, внесенными приказами Министерства связи и массовых коммуникаций Российской Федерации от 01.02.2012 N 29 (зарегистрирован Министерством юстиции Российской Федерации 22 февраля 2012 г., регистрационный N 23312), от 23.04.2013 N 93 (зарегистрирован Министерством юстиции Российской Федерации 14 июня 2013 г., регистрационный N 2878822) и от 14.12.2015 N 543 (зарегистрирован Министерством юстиции Российской Федерации 18 января 2016 г.,

регистрационный N 40606) (далее - Правила N 58-07).

10. Требования к системе нумерации и идентификации для оборудования коммутации стандарта LTE приведены в приложении N 1 к Правилам.

11. Для оборудования, выполняющего функции MME, устанавливаются следующие требования к:

1) перечню хранящихся в MME данных об абонентских радиостанциях, поддерживающих стандарт LTE и находящихся в состояниях ECM-IDLE, ECM-CONNECTED или EMM-DEREGISTERED в зонах слежения (TA), обслуживаемых MME (приложение N 2 к Правилам);

2) перечню сообщений протокола S1-AP (S1 Application Part) при взаимодействии оборудования систем базовых станций стандарта LTE (eNodeB) с MME (приложение N 3 к Правилам);

3) перечню сообщений протокола SGsAP (SGs Application Part) при реализации интерфейса взаимодействия MME с сервером центра мобильной коммутации MSC сервер/VLR (интерфейс SGs) (приложение N 4 к Правилам);

4) перечню сообщений протокола Diameter при реализации интерфейса взаимодействия MME с DA или HSS (интерфейс S6a), MME с DA или EIR (интерфейс S13) (приложение N 5 к Правилам);

5) перечню сообщений протокола NAS при реализации интерфейса взаимодействия AC и MME (интерфейс S1-MME) (приложение N 6 к Правилам);

6) протоколу GTP (приложение N 7 к Правилам);

7) интерфейсам взаимодействия (приложение N 9 к Правилам);

8) протоколу SCTP при реализации в оборудовании коммутации стандарта LTE (пункт 2 приложения N 14 к Правилам N 58-07);

9) протоколу GTP (интерфейс Gn) при взаимодействии MME с SGSN, если SGSN при взаимодействии с MME не реализует протокол GTPv2-C (интерфейс S3) (приложение N 4 к Правилам применения оборудования коммутации систем подвижной радиотелефонной связи. Часть V. Правила применения оконечно-транзитных узлов связи сетей подвижной радиотелефонной связи стандарта UMTS, утвержденным приказом Министерства информационных технологий и связи Российской Федерации от 27.08.2007 N 101 (зарегистрирован Министерством юстиции Российской Федерации 29 августа 2007 г., регистрационный N 10066), с изменениями, внесенными приказами Министерства связи и массовых коммуникаций Российской Федерации от 01.02.2012 N 31 (зарегистрирован Министерством юстиции Российской Федерации 24 февраля 2012 г., регистрационный N 23324), от 23.04.2013 N 93 (зарегистрирован Министерством юстиции Российской Федерации 14 июня 2013 г., регистрационный N 28788), от 14.12.2015 N 543 (зарегистрирован Министерством юстиции Российской Федерации 18 января 2016 г., регистрационный N 40606) (далее - Правила N 101-07);

10) функциям MME при реализации non-3GPP доступа (пересылка ключа протокола GRE к S-GW через интерфейсы S10/S11 для передачи данных по восходящей линии связи в случае перемещения UE из узла CN);

11) перечню данных, хранящихся в MME при реализации non-3GPP доступа (приложение N 22 к Правилам).

12. Для оборудования, выполняющего функции S-GW, устанавливаются следующие требования к:

1) перечню данных об обслуживаемых в S-GW абонентских радиостанциях, поддерживающих стандарты LTE, GSM 900/1800, UMTS (приложение N 10 к Правилам);

2) протоколу GTP (приложение N 7 к Правилам);

3) интерфейсам взаимодействия (приложение N 9 к Правилам);

4) системе учета данных для начисления платы (приложение N 11 к Правилам);

5) протоколу PMIPv6 при реализации в оборудовании коммутации стандарта LTE (приложение N 8 к Правилам);

6) перечню сообщений протокола Diameter при реализации интерфейса взаимодействия S-GW с H-PCRF (V-PCRF) (интерфейс Gxc) в случае реализации интерфейсов S5 и S8 протоколом PMIPv6 (приложение N 5 к Правилам);

7) функциям S-GW при осуществлении non-3GPP доступа:

а) реализация функций локального узла управления мобильностью (далее - LMA) визитной (гостевой) сети подвижной радиотелефонной связи (далее - VPLMN) с TWAN при взаимодействии с TWAN по протоколу PMIPv6, когда UE находится в роуминге;

б) информирование PCRF о происходящих изменениях при переходе UE на новую технологию радиодоступа;

в) осуществление контроля трафика от UE;

г) реализация функций MAG в случае реализации интерфейсов взаимодействии с P-GW (интерфейсы S5 и S8) протоколом PMIPv6;

д) принятие решения о маршрутизации пакетов по восходящей линии к P-GW, по нисходящей линии к UE или определение пакетов, предназначенных для S-GW;

е) реализация функций агента протокола DHCPv4 либо DHCPv6 при реализации интерфейса S5 или S8 протоколом PMIPv6;

ж) осуществление обмена сообщениями "Запрос доступности маршрутизатора" (Router Solicitation) (далее - RS) и "Ответ маршрутизатора" (Router Advertisement) (далее - RA) протокола NDP при реализации интерфейсов S5 и S8 протоколом PMIPv6;

з) осуществление обмена сообщениями "Запрос доступных соседей" (Neighbour Solicitation) и "Ответ соседа" (Neighbor Advertisement) протокола NDP при реализации интерфейсов S5 и S8 протоколом PMIPv6;

и) осуществление генерации и распределения ключей протокола GRE для каждого соединения передачи данных по нисходящей линии от P-GW к S-GW при реализации интерфейсов

S5 и S8 протоколом PMIPv6;

к) реализация функций LMA в отношении функций MAG протокола PMIPv6, реализованных в TWAN либо в ePDG;

л) осуществление генерации и распределения ключей протокола GRE для инкапсуляции пакетов данных для каждого соединения передачи данных по восходящей линии от S-GW при реализации интерфейсов S2a/S2b протоколом PMIPv6;

м) реализация функций взаимодействия протокола PMIPv6 в направлении P-GW и в направлении функций MAG, реализованных в TWAN (интерфейсы S8 и S2a) либо в ePDG (интерфейсы S8 и S2b). При этом S-GW реализует функции MAG по отношению к P-GW;

н) реализация функций соединения PMIPv6 в направлении P-GW и в направлении функций MAG, реализованных в TWAN либо в ePDG, для пользовательского уровня;

8) протоколу MIPv4 при взаимодействии S-GW с TWAN (интерфейс S2a) при реализации в оборудовании коммутации стандарта LTE (приложение N 17 к Правилам);

9) перечню данных, хранящихся в S-GW при реализации non-3GPP доступа (Приложение N 22 к Правилам).

13. Для оборудования, выполняющего функции P-GW, устанавливаются следующие требования к:

1) перечню данных об обслуживаемых в P-GW абонентских радиостанциях, поддерживающих стандарты LTE, GSM 900/1800, UMTS (приложение N 12 к Правилам);

2) протоколу GTP (приложение N 7 к Правилам);

3) перечню сообщений протокола Diameter при взаимодействии P-GW с PCRF (интерфейс Gx) в случае реализации интерфейсов S5, S8 протоколом GTP (приложение N 5 к Правилам);

4) интерфейсам взаимодействия (приложение N 9 к Правилам);

5) системе учета данных для начисления платы (приложение N 11 к Правилам);

6) протоколу PMIPv6 при реализации в оборудовании коммутации стандарта LTE (приложение N 8 к Правилам);

7) протоколу SCTP при реализации в оборудовании коммутации стандарта LTE (пункт 2 приложения N 14 к Правилам N 58-07);

8) протоколу GTP (интерфейсы Gn или Gp) при взаимодействии P-GW с SGSN, если SGSN при взаимодействии с P-GW не реализуется протокол GTPv2-C (интерфейс S3) (приложение N 4 к Правилам N 101-07);

9) функциям P-GW при реализации non-3GPP доступа:

а) реализация функций точки взаимодействия уровня пользователя при передвижении пользователя между сетями доступа стандартов GSM 900/1800, UMTS, LTE и non-3GPP;

б) реализация функции узла LMA при реализации интерфейсов S5 и S8, или S2a, или S2b протоколом PMIPv6;

в) реализация функции домашнего агента (далее - HA) при реализации интерфейса взаимодействия между P-GW и UE (интерфейс S2c) протоколом DSMIPv6 (протоколом DSMIPv6 должен создаваться туннель между UE и P-GW при реализации интерфейса S2c для пересылки пользовательского и сигнального трафика между UE и P-GW, обеспечивающим назначение IP-адресов для создания туннеля);

г) осуществление генерации и распределения ключей протокола GRE, используемых для инкапсуляции пользовательских данных, передаваемых по восходящей линии при реализации интерфейсов S5 и S8 или S2a, или S2b протоколом PMIPv6;

д) реализация функции домашнего агента при реализации интерфейса S2a протоколом MIPv4 (при регистрации должно осуществляться назначение UE временного IP-адреса с помощью протокола MIPv4 при этом временный IP-адрес должен являться адресом агента визитной сети (далее - FACoA);

е) реализация протокола GTP для уровня управления (GTPv2-C) и уровня пользователя (GTPv1-U) для обеспечения соединения PDN с UE (при реализации интерфейсов S2a или S2b протоколом GTP должен использоваться non-3GPP доступ);

ж) взаимодействие с 3GPP AAA сервером внешней сети передачи данных (интерфейс SGi) по протоколу RADIUS или Diameter;

з) взаимодействие с 3GPP AAA сервер/прокси (интерфейс S6b) по протоколу Diameter;

10) протоколу MIPv4 при взаимодействии P-GW с TWAN (интерфейс S2a) при реализации в оборудовании коммутации стандарта LTE (17 к Правилам);

11) протоколу DSMIPv6 при взаимодействии P-GW с UE (интерфейс S2c) при реализации в оборудовании коммутации стандарта LTE (приложение N 18 к Правилам);

12) протоколу IKEv2 при взаимодействии P-GW с UE (интерфейс S2c) при реализации в оборудовании коммутации стандарта LTE (приложение N 19 к Правилам);

13) протоколу IPSec при взаимодействии P-GW с UE (интерфейс S2c) (приложение N 20 к Правилам);

14) перечню сообщений протокола Diameter при реализации интерфейса S6b (приложение N 21 к Правилам);

15) перечню данных, хранящихся в P-GW, при реализации non-3GPP доступа (приложение N 22 к Правилам).

14. Для оборудования, выполняющего функции EIR, устанавливаются следующие требования к:

1) данным об абонентской радиостанции, хранящимся в EIR (приложение N 14 к Правилам);

2) перечню сообщений протокола Diameter при реализации интерфейса взаимодействия MME с EIR (интерфейс S13) (приложение N 5 к Правилам);

3) интерфейсам взаимодействия (приложение N 9 к Правилам);

4) протоколу SCTP при реализации в оборудовании коммутации стандарта LTE (пункт 2 приложения N 14 к Правилам N 58-07).

15. Для оборудования, выполняющего функции HSS/AuC, устанавливаются следующие требования к:

1) перечню хранящихся в HSS данных об абонентских радиостанциях, поддерживающих стандарт LTE (приложение N 13 к Правилам);

2) перечню сообщений протокола Diameter при реализации интерфейса взаимодействия HSS с MME (интерфейс S6a) (приложение N 5 к Правилам);

3) интерфейсам взаимодействия (приложение N 9 к Правилам);

4) протоколу SCTP при реализации в оборудовании коммутации стандарта LTE (пункт 2 приложения N 14 к Правилам N 58-07);

> КонсультантПлюс: примечание.
> Пп. 5 п. 15 вступает в силу с 01.12.2019.

5) осуществлению процедур аутентификации и идентификации абонентов с использованием средств криптографической защиты информации, имеющих подтверждение соответствия требованиям по безопасности информации класса КА для оборудования коммутации узлов связи, установленным федеральным органом исполнительной власти в области обеспечения безопасности;

> КонсультантПлюс: примечание.
> Пп. 6 п. 15 вступает в силу с 01.12.2019.

6) протоколу взаимодействия сервера абонентских данных HSS и/или центра аутентификации AuC с отдельным аппаратным модулем безопасности HSM, выполняющим криптографические функции аутентификации и идентификации абонентов (приложение N 24 к Правилам);

7) функциям HSS при реализации non-3GPP доступа при взаимодействии с 3GPP AAA сервером по протоколу Diameter (интерфейс SWx);

8) перечню сообщений протокола Diameter при реализации интерфейса SWx (приложение N 21 к Правилам);

9) перечню данных, хранящихся в HSS, при реализации non-3GPP доступа (приложение N 22 к Правилам).

16. Для оборудования, выполняющего функции SGSN, устанавливаются следующие требования к:

1) протоколу GTP (приложение N 7 к Правилам);

2) интерфейсам взаимодействия (приложение N 9 к Правилам);

17. Для оборудования, выполняющего функции PCRF, устанавливаются следующие требования к:

1) перечню сообщений протокола Diameter при реализации интерфейса взаимодействия PCRF с P-GW (интерфейс Gx) в случае реализации интерфейсов S5 и S8 протоколом GTP, PCRF визитной сети (далее - V-PCRF) с PCRF домашней сети (далее - H-PCRF), H-PCRF (V-PCRF) с S-GW (интерфейс Gxc) в случае реализации интерфейсов S5 и S8 протоколом PMIPv6, PCRF с функциями приложений (интерфейс Rx) (приложение N 5 к Правилам);

2) протоколу SCTP при реализации в оборудовании коммутации стандарта LTE (пункт 2 приложения N 14 к Правилам N 58-07);

3) интерфейсам взаимодействия (приложение N 9 к Правилам);

4) функциям PCRF при реализации non-3GPP к:

а) PCRF домашней сети (далее - H-PCRF):

взаимодействие с P-GW домашней сети (интерфейс Gx) должно осуществляться для обмена информацией управления качеством передачи данных QoS и правил тарификации при маршрутизации трафика через домашнюю сеть по протоколу Diameter;

взаимодействие с TWAN (интерфейс Gxa), с S-GW (интерфейс Gxc), с ePDG (интерфейсу Gxb) должно осуществляться для передачи сообщений управления качеством передачи данных QoS и тарификации по протоколу Diameter;

взаимодействие с PCRF визитной сети (далее - V-PCRF) (интерфейс S9) должно осуществляться по протоколу Diameter;

б) PCRF визитной сети:

взаимодействие с TWAN (интерфейс Gxa), с S-GW (интерфейс Gxc), с ePDG (интерфейс Gxb) должно осуществляться для передачи сообщений управления качеством передачи данных QoS и тарификации по протоколу Diameter;

взаимодействие с H-PCRF (интерфейс S9) должно осуществляться по протоколу Diameter.

18. Требования к оборудованию коммутации стандарта LTE в режиме оказания услуг связи с использованием оборудования коммутации IMS приведены в приложении N 16 к Правилам.

19. Требования к оборудованию Центра Управления и Технического Обслуживания (ЦУ и ТО) приведены в приложении N 15 к Правилам.

20. Для оборудования, выполняющего функции DA переключения (далее - DRLA), прокси-сервера (далее - DPXA), перенаправления (далее - DRDA), обеспечивающего определение местонахождения подписки пользователя, в случае наличия на сети оператора нескольких HSS, устанавливаются следующие требования к:

1) перечню сообщений протокола Diameter при реализации интерфейса взаимодействии MME с DA (интерфейс S6a) (приложение N 5 к Правилам);

2) протоколу SCTP при реализации в оборудовании коммутации стандарта LTE (пункт 2 приложения N 14 к Правилам N 58-07);

3) интерфейсам взаимодействия (приложение N 9 к Правилам).

21. Для оборудования, выполняющего функции ePDG, устанавливаются следующие требования к:

1) функциям ePDG:

а) выделение UE временного удаленного IP адреса (далее - CoA), являющегося локальным для ePDG, при реализации интерфейса S2c;

б) регистрация локального IP адреса UE;

в) обеспечение возможности транспортировки удаленного IP-адреса, выделенного в качестве IP-адреса PDN, при реализации интерфейса S2b;

г) маршрутизация пакетов данных от (к) P-GW (от (к) S-GW при выполнении S-GW функции LA в сети VPLMN к (от) UE, если реализуется интерфейс S2b протоколом GTP;

д) маршрутизация пакетов данных к UE через интерфейс SWu, связанный соединением с PDN;

е) инкапсуляция и деинкапсуляция пакетов данных IPSec, при осуществлении поддержки мобильности на базе интерфейса S2b, реализованного протоколом GTP или PMIPv6;

ж) реализация функций MAG при реализации интерфейса S2b протоколом PMIPv6;

з) формирование безопасных туннелей IPSec протоколом IKEv2 для передачи данных аутентификации и авторизации;

и) обеспечение функций LMA в случае реализации расширения протокола IKEv2;

к) генерация и распределение ключей протокола GRE, используемых для инкапсуляции данных PMIPv6, передаваемых EPC в направлении ePDG в сторону интерфейса S2b;

л) организация взаимодействия правил тарификации различных операторов;

м) реализация функций пограничного взаимодействия;

2) интерфейсам взаимодействия (приложение N 9 к Правилам);

3) протоколу PMIPv6 при реализации в оборудовании коммутации стандарта LTE (приложение N 8 к Правилам);

4) протоколу SCTP при реализации в оборудовании коммутации стандарта LTE (пункт 2 приложения N 14 к Правилам N 58-07);

5) протоколу GTP (приложение N 7 к Правилам);

6) протоколу IKEv2 (приложение N 19 к Правилам);

7) протоколу IPSec, идентификационному заголовку протокола IPSec (AH), протоколу ESP) (приложение N 20 к Правилам);

8) перечню сообщений протокола Diameter при реализации интерфейса взаимодействия ePDG и 3GPP AAA сервер/прокси (интерфейс SWm) (приложение N 21 к Правилам);

9) перечню данных, хранящихся в ePDG, при реализации non-3GPP доступа (приложение N 22 к Правилам);

10) протоколу EAP-AKA, EAP-AKA' (приложение N 23 к Правилам).

22. Для оборудования, выполняющего функции 3GPP AAA сервера, устанавливаются следующие требования к:

1) функциям 3GPP AAA сервера:

а) выполнение функции сервера для метода EAP-AKA, используемого при аутентификации UE;

б) получение от HLR/HSS информации о профилях UE для аутентификации;

в) аутентификация 3GPP пользователя с использованием данных, полученных от HLR/HSS;

г) обновление информации для доступа TWAN по запросу HLR/HSS;

д) передача информации авторизации пользователя к WLAN через 3GPP AAA прокси-сервер, если пользователь находится в визитной сети;

е) регистрация адреса в HLR/HSS при каждой аутентификации пользователя;

ж) удаление данных о подключении из HLR/HSS при отмене регистрации пользователя в 3GPP AAA сервере;

з) сохранение информации о состоянии подключения UE к WLAN;

и) формирование и передача данных для тарификации системе тарификации в HPLMN при доступе UE через UTWAN;

к) хранение данных о качестве обслуживания для TWAN;

л) взаимодействие с TWAN (интерфейс STa), с HLR/HSS (интерфейс SWx), с UTWAN (интерфейс SWa), с 3GPP AAA прокси-сервером (интерфейс SWd) по протоколу Diameter;

м) передача к P-GW информации для авторизации;

н) предоставление P-GW временного удаленного IP адреса UE, полученного от HSS при использовании статического удаленного IP адреса;

о) предоставление 3GPP AAA прокси-серверу информации о правилах обслуживания пользователя;

2) протоколу PMIPv6 при реализации в оборудовании коммутации стандарта LTE (приложение N 8 к Правилам);

3) интерфейсам взаимодействия (приложение N 9 к Правилам);

4) протоколу SCTP при реализации в оборудовании коммутации стандарта LTE (пункт 2 приложения N 14 к Правилам N 58-07);

5) протоколу IKEv2 (приложение N 19 к Правилам);

6) протоколу IPSec, идентификационному заголовку протокола IPSec (AH), протоколу ESP (приложение N 20 к Правилам);

7) перечню сообщений протокола Diameter при реализации интерфейсов STa, SWx, SWa, SWd (приложение N 21 к Правилам);

8) перечню данных, хранящихся в 3GPP AAA сервере, при реализации non-3GPP доступа (приложение N 22 к Правилам);

9) протоколу EAP-AKA, EAP-AKA' (приложение N 23 к Правилам).

23. Для оборудования, выполняющего функции 3GPP AAA прокси-сервера, устанавливаются следующие требования:

1) трансляция информации для аутентификации между WLAN и 3GPP AAA сервером;

2) предоставление информации об ограничениях, полученной из домашней сети при использовании доступа WLAN;

3) формирование и передача данных для тарификации системе тарификации VPLMN;

4) прекращение обслуживания;

5) обеспечение взаимодействия интерфейсов SWa, STa и SWd при использовании на них различных протоколов;

6) к протоколу PMIPv6 при реализации в оборудовании коммутации стандарта LTE (приложение N 8 к Правилам);

7) к интерфейсам взаимодействия (приложение N 9 к Правилам);

8) к протоколу SCTP при реализации в оборудовании коммутации стандарта LTE (пункт 2 приложения N 14 к Правилам N 58-07);

9) к протоколу IKEv2 (приложение N 19 к Правилам);

10) к протоколу IPSec, идентификационному заголовку протокола IPSec (AH), протоколу ESP (приложение N 20 к Правилам);

11) к перечню сообщений протокола Diameter при реализации интерфейсов STa, SWa, SWd (приложение N 21 к Правилам);

12) к перечню данных, хранящихся в 3GPP AAA прокси-сервере, при реализации non-3 GPP доступа (приложение N 22 к Правилам);

13) к протоколу EAP-AKA, EAP-AKA' (приложение N 23 к Правилам).

Приложение N 1
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ТРЕБОВАНИЯ К СИСТЕМЕ НУМЕРАЦИИ И ИДЕНТИФИКАЦИИ

1. Идентификация АС должна осуществляться в соответствии с требованиями приказа Министерства связи и массовых коммуникаций Российской Федерации от 25 апреля 2017 г. N 205 "Об утверждении и введении в действие российской системы и плана нумерации" (зарегистрирован Министерством юстиции Российской Федерации 13 июля 2017 г., регистрационный N 47401).

2. Оборудование коммутации стандарта LTE должно осуществлять маршрутизацию данных, используя адресацию сети Интернет в формате, определенном протоколами IP четвертой и шестой версий (далее - IPv4, IPv6).

3. Для идентификации АС в информационно-телекоммуникационной сети "Интернет" на время взаимодействия АС с информационно-телекоммуникационной сетью "Интернет" ей должен присваиваться адрес сети в формате протокола IPv4 и (или) IPv6.

4. Для аутентификации UE при доступе через TWAN должны использоваться идентификаторы:

1) доступа к сети (далее - NAI), имеющий структуру:

"1"<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org - для аутентификации EAP-AKA;

"0"<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org - для аутентификации EAP-SIM;

2) сети доступа (далее - ANID), принимающий при доступе non-3GPP следующие значения:

"WIMAX" - сеть доступа Wi-Max;

"WLAN" - сеть доступа WLAN;

"ETHERNET" - сеть фиксированного доступа с коммутацией пакетов.

Приложение N 2
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ПЕРЕЧЕНЬ
ХРАНЯЩИХСЯ В ММЕ ДАННЫХ ОБ АБОНЕНТСКИХ РАДИОСТАНЦИЯХ, ПОДДЕРЖИВАЮЩИХ СТАНДАРТ LTE И НАХОДЯЩИХСЯ В СОСТОЯНИЯХ ECM-IDLE, ECM-CONNECTED ИЛИ EMM-DEREGISTERED В ЗОНАХ СЛЕЖЕНИЯ (TA), ОБСЛУЖИВАЕМЫХ ММЕ

Таблица.

Данные	Комментарии
Международный номер АС (IMSI)	
Индикатор неподтверждения подлинности IMSI (IMSI unauthenticated-indicator)	
Международный номер АС в сети ISDN (MSISDN)	при наличии в HSS
Состояние управления мобильностью (ECM-IDLE, ECM-CONNECTED, EMM-DEREGISTERED) (MM State)	
Глобальный уникальный временный идентификатор (GUTI)	
Международный идентификатор оборудования АС и версия программного обеспечения (IMEI/IMEISV) (ME Identity)	
Список зон слежения (Tracking Area List)	
Идентификатор зоны слежения, в которой произошло последнее обновление зоны слежения (TAI of last TAU)	
Глобальный идентификатор соты в сети радиодоступа стандарта LTE (E-UTRAN Cell Global Identity)	
Время, прошедшее с момента последнего определения Глобального идентификатора соты стандарта LTE и/или LTE-Advanced (E-UTRAN Cell Identity Age)	

Идентификатор закрытой группы пользователей (CSG ID)	
Членство в закрытой группе пользователей (CSG membership)	
Режим доступа (Access mode)	
Параметры аутентификации: произвольный номер (RAND), ожидаемый ответ (XRES), ключ (KASME), символ аутентификации (AUTN) (Authentication Vector)	
Возможности радиодоступа АС (UE Radio Access Capability)	
Марка класса 2 для оборудования АС (поддержка передачи обслуживания к сети радиодоступа стандарта GSM 900/1800 или UMTS) (MS Classmark 2)	
Марка класса 3 для оборудования АС (поддержка передачи обслуживания к сети радиодоступа стандарта GSM 900/1800) (MS Classmark 3)	
Поддерживаемые кодеки (Supported Codecs)	
Сетевые возможности АС (UE Network Capability)	
Сетевые возможности АС стандарта GSM 900/1800 или UMTS (MS Network Capability)	
Параметры DRX (UE Specific DRX Parameters)	
Выбранный алгоритм безопасности слоя без доступа (Selected NAS Algorithm)	
Идентификатор установки ключа (eKSI)	
Ключ KASME (KASME)	
Ключи слоя без доступа и параметры счета (NAS Keys and COUNT)	
Идентификатор выбранного оператора сети (Selected CN operator id)	
Восстановление данных HSS (Recovery)	
Ограничение доступа (Access Restriction)	
Ограничения оператора для услуг передачи данных (ODB for PS parameters)	
Замена APN-OI (APN-OI Replacement)	
IP адрес MME для интерфейса S11 с S-GW	

(MME IP address for S11)	
Идентификатор конечной точки туннеля MME для интерфейса S11 (MME TEID for S11)	
IP адрес S-GW для интерфейсов S11/S4 (S-GW IP address for S11/S4)	
Идентификатор конечной точки туннеля S-GW для интерфейсов S11/S4 (S-GW TEID for S11/S4)	
IP адрес SGSN для интерфейса S3 (SGSN IP address for S3)	
Идентификатор конечной точки туннеля SGSN для интерфейса S3 (SGSN TEID for S3)	
IP адрес используемого узла радиодоступа eNodeB для интерфейса S1-MME (eNodeB Address in Use for S1-MME)	
Уникальный идентификатор АС для eNodeB (eNB UE S1AP ID)	
Уникальный идентификатор АС для MME (MME UE S1AP ID)	
Общая максимальная скорость передачи для АС (Подписка АС) (Subscribed-UE-AMBR)	
Общая максимальная скорость передачи (UE-AMBR)	
Характеристики для учета стоимости АС в соответствии с подпиской в сети (EPS Subscribed Charging Characteristics)	
Индекс приоритетности выбора Технологии радиодоступа/Частоты (Subscribed RFSP Index)	
Используемый Индекс приоритетности выбора Технологии радиодоступа/Частоты (RFSP Index in Use)	
Подробное описание трейса (Trace reference)	
Тип трейса (Trace Type)	
Идентификатор триггера (Trigger id)	
Идентификатор центра управления и обслуживания, куда будут передаваться отчеты по трейсам (OMC Identity)	
Параметр запроса доступности АС для MME (URRP-MME)	
Данные подписки закрытой группы пользователей (CSG Subscription Data)	

Разрешение местного IP доступа (LIPA Allowed) <*>	
Подписка на периодическое обновление зоны маршрутизации/слежения по таймеру (Subscribed Periodic RAU/TAU Timer) <*>	
Подписка на приоритетное обслуживание в домене CS (MPS CS priority) <*>	
Подписка на приоритетное обслуживание в EPS (MPS EPS priority) <*>	
Данные для каждого активного соединения сети передачи данных	
Используемая точка доступа (APN in Use)	
Ограничение точки доступа (APN Restriction)	
Подписка на APN (APN Subscribed)	
Тип сети передачи данных (IPv4, IPv6, IPv4v6) (PDN Type)	
IP адрес (адреса) сети передачи данных (IP Address(es))	
Характеристики учета стоимости абонентской станции в соответствии с подпиской в сети передачи данных EPS (EPS PDN Subscribed Charging Characteristics)	
Замещение точки доступа (APN-OI Replacement)	
Разрешения возможности распределения трафика IP (SIPTO permissions) <*>	
Разрешения LIPA (LIPA permissions) <*>	LIPA-разрешено, только LIPA, LIPA-при условии
Возможность использовать для APN AC P-GW домашней или визитной сети (VPLMN Address Allowed)	
IP адрес используемого P-GW (для плоскости управления) (P-GW Address in Use (control plane))	
Идентификатор конечной точки туннеля P-GW для интерфейса S5/S8 (для плоскости управления) (P-GW TEID for S5/S8 (control plane))	
Сообщение об изменении информации AC (MS Info Change Reporting Action)	
Сообщение об изменении информации закрытой группы пользователей (CSG Information Reporting Action)	

Профиль качества обслуживания в соответствии с подпиской в EPS (QCI и ARP) (EPS subscribed QoS profile) <*>	
Подписка Точка доступа - Общая максимальная скорость передачи (Subscribed-APN-AMBR)	
Точка доступа - Общая максимальная скорость передачи (APN-AMBR)	
Ключ GRE, выделенный P-GW для передачи пользовательских данных "вверх" (только для PMIPv6 на S5/S8) (P-GW GRE Key for uplink traffic (user plane))	
Идентификатор EPS по умолчанию (Default bearer)	
Низкий приоритет доступа (low access priority) <*>	
Данные для каждого канала соединения сети передачи данных	
Идентификатор канала передачи данных EPS (EPS Bearer ID)	
Идентификатор транзакции (TI)	
IP адрес S-GW для S1-u интерфейса (S-GW IP address for S1-u)	
Идентификатор конечной точки туннеля S-GW для интерфейсов S1-u (S-GW TEID for S1-u)	
Идентификатор конечной точки туннеля P-GW для интерфейса S5/S8 (для плоскости пользователя) (P-GW TEID for S5/S8 (user plane))	
IP адрес P-GW для интерфейса S5/S8 (для плоскости пользователя) (P-GW IP address for S5/S8 (user plane))	
Качество обслуживания в канале передачи данных EPS (QCI и ARP) (EPS bearer QoS)	
Шаблон потока трафика (только для PMIPv6 на S5/S8) (TFT)	
Данные для экстренного обслуживания АС	
Наименование точки доступа при экстренном обслуживании (Emergency Access Point Name (em APN))	
Профиль QoS при экстренном обслуживании EPS (QCI и ARP) (Emergency QoS profile)	
Точка доступа при экстренном обслуживании - Общая	

максимальная скорость передачи (Emergency APN-AMBR)	
Идентификатор P-GW при экстренном обслуживании (Emergency P-GW identity)	
Примечание: <*> "Данные" обязательны только для стандарта LTE-Advanced.	

Приложение N 3
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ПЕРЕЧЕНЬ
СООБЩЕНИЙ ПРОТОКОЛА S1-AP ПРИ ВЗАИМОДЕЙСТВИИ ОБОРУДОВАНИЯ СИСТЕМ БАЗОВЫХ СТАНЦИЙ СТАНДАРТА LTE (ENODEB) С MME

Таблица.

Сообщение	Направление передачи
Запрос установки E-RAB (E-RAB SETUP REQUEST)	от MME к eNodeB
Ответ на запрос установки E-RAB (E-RAB SETUP RESPONSE)	от eNodeB к MME
Запрос изменения E-RAB (E-RAB MODIFY REQUEST)	от MME к eNodeB
Ответ на запрос изменения E-RAB (E-RAB MODIFY RESPONSE)	от eNodeB к MME
Команда освобождения E-RAB (E-RAB RELEASE COMMAND)	от MME к eNodeB
Ответ на команду освобождения E-RAB (E-RAB RELEASE RESPONSE)	от eNodeB к MME

Освобождение E-RAB (E-RAB RELEASE INDICATION)	от eNodeB к MME
Запрос установки инициализации контекста (INITIAL CONTEXT SETUP REQUEST)	от MME к eNodeB
Ответ на запрос установки инициализации контекста (INITIAL CONTEXT SETUP RESPONSE)	от eNodeB к MME
Ошибка установки инициализации контекста (INITIAL CONTEXT SETUP FAILURE)	от eNodeB к MME
Запрос освобождения контекста АС (UE CONTEXT RELEASE REQUEST)	от eNodeB к MME
Команда освобождения контекста АС (UE CONTEXT RELEASE COMMAND)	от MME к eNodeB
Освобождение контекста АС выполнено (UE CONTEXT RELEASE COMPLETE)	от eNodeB к MME
Запрос изменения контекста АС (UE CONTEXT MODIFICATION REQUEST)	от MME к eNodeB
Ответ на запрос изменения контекста АС (UE CONTEXT MODIFICATION RESPONSE)	от eNodeB к MME
Ошибка изменения контекста (UE CONTEXT MODIFICATION FAILURE)	от eNodeB к MME
Требуется хендовер (HANDOVER REQUIRED)	от eNodeB к MME
Команда на выполнение хендовера (HANDOVER COMMAND)	от MME к eNodeB
Хендовер не возможен (HANDOVER PREPARATION FAILURE)	от MME к eNodeB
Запрос хендовера (HANDOVER REQUEST)	от MME к eNodeB
Подтверждение запроса хендовера (HANDOVER REQUEST ACKNOWLEDGE)	от eNodeB к MME
Отсутствие ресурсов для хендовера (HANDOVER FAILURE)	от eNodeB к MME
Подтверждение хендовера (HANDOVER NOTIFY)	от eNodeB к MME
Запрос коммутации конечной точки туннеля (PATH SWITCH REQUEST)	от eNodeB к MME

Подтверждение коммутации конечной точки туннеля (PATH SWITCH REQUEST ACKNOWLEDGE)	от MME к eNodeB
Ошибка при коммутации конечной точки туннеля (PATH SWITCH REQUEST FAILURE)	от MME к eNodeB
Отмена хендовера (HANDOVER CANCEL)	от eNodeB к MME
Подтверждение отмены хендовера (HANDOVER CANCEL ACKNOWLEDGE)	от MME к eNodeB
Передача статуса eNodeB (eNB STATUS TRANSFER)	от eNodeB к MME
Передача статуса MME (MME STATUS TRANSFER)	от MME к eNodeB
Поиск (PAGING)	от MME к eNodeB
Инициализация сообщений AC INITIAL UE MESSAGE	от eNodeB к MME
Транспортировка сообщений NAS "вниз" (DOWNLINK NAS TRANSPORT)	от MME к eNodeB
Транспортировка сообщений NAS "вверх" (UPLINK NAS TRANSPORT)	от eNodeB к MME
Недоставка сообщений NAS "вниз" (NAS NON DELIVERY INDICATION)	от eNodeB к MME
Сброс (RESET)	от eNodeB к MME и от MME к eNodeB
Подтверждение сброса (RESET ACKNOWLEDGE)	от eNodeB к MME и от MME к eNodeB
Индикация ошибки (ERROR INDICATION)	от eNodeB к MME и от MME к eNodeB
Запрос установки S1 (S1 SETUP REQUEST)	от eNodeB к MME
Ответ на запрос установки S1 (SI SETUP RESPONSE)	от MME к eNodeB
Ошибка установки S1 (S1 SETUP FAILURE)	от MME к eNodeB
Обновление конфигурации eNodeB (ENB CONFIGURATION UPDATE)	от eNodeB к MME

Подтверждение обновления конфигурации eNodeB (ENB CONFIGURATION UPDATE ACKNOWLEDGE)	от MME к eNodeB
Ошибка при обновления конфигурации eNodeB (ENB CONFIGURATION UPDATE FAILURE)	от MME к eNodeB
Обновление конфигурации MME (MME CONFIGURATION UPDATE)	от MME к eNodeB
Подтверждение обновления конфигурации MME (MME CONFIGURATION UPDATE ACKNOWLEDGE)	от eNodeB к MME
Ошибка при обновления конфигурации MME (MME CONFIGURATION UPDATE FAILURE)	от eNodeB к MME
Начало перегрузки (OVERLOAD START)	от MME к eNodeB
Окончание перегрузки (OVERLOAD STOP)	от MME к eNodeB
Индикация возможностей AC (UE CAPABILITY INFO INDICATION)	от eNodeB к MME
Начало записи трейса (TRACE START)	от MME к eNodeB
Индикация ошибки записи трейса (TRACE FAILURE INDICATION)	от eNodeB к MME
Завершение трейса (DEACTIVATE TRACE)	от MME к eNodeB
Запрос информации о местоположении (LOCATION REPORTING CONTROL)	от MME к eNodeB
Ошибка при отчете о местоположении (LOCATION REPORT FAILURE INDICATION)	от eNodeB к MME
Отчет о местоположении (LOCATION REPORT)	от eNodeB к MME
Запрос начала или возобновления предупреждающих сообщений (WRITE-REPLACE WARNING REQUEST)	от MME к eNodeB
Ответ на запрос предупреждающих сообщений (WRITE-REPLACE WARNING RESPONSE)	от eNodeB к MME
Запрос удаления предупреждающих сообщений (KILL REQUEST)	от MME к eNodeB
Ответ на запрос удаления предупреждающих сообщений	от eNodeB к MME

(KILL RESPONSE)	
Передача информации eNodeB (eNB DIRECT INFORMATION TRANSFER)	от eNodeB к MME
Передача информации MME (MME DIRECT INFORMATION TRANSFER)	от MME к eNodeB
Передача конфигурации сети радиодоступа (eNB CONFIGURATION TRANSFER)	от eNodeB к MME
Передача конфигурации сети радиодоступа (MME CONFIGURATION TRANSFER)	от MME к eNodeB
Передача информации о пути в соте (CELL TRAFFIC TRACE)	от eNodeB к MME

Приложение N 4
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ПЕРЕЧЕНЬ
СООБЩЕНИЙ ПРОТОКОЛА SGSAP ПРИ РЕАЛИЗАЦИИ ИНТЕРФЕЙСА ВЗАИМОДЕЙСТВИЯ MME С СЕРВЕРОМ ЦЕНТРА МОБИЛЬНОЙ КОММУТАЦИИ MSC СЕРВЕРОМ/VLR (ИНТЕРФЕЙС SGS)

Установление входящей и исходящей радиотелефонной связи должно осуществляться к АС, имеющей регистрацию в MME сети стандарта LTE и в визитном регистре местоположения (VLR) сетей стандартов GSM 900/1800 или UMTS.

Сообщения протокола SGsAP, передаваемые между MME и MSC сервером/VLR через интерфейс SGs для установления радиотелефонной связи, приведены в таблице.

Таблица.

Сообщение	Направление передачи

Подтверждение на запрос активности АС (ALERT-ACK)	от MME к VLR
Отказ на запрос активности АС (ALERT-REJECT)	от MME к VLR
Запрос активности АС (ALERT-REQUEST)	от VLR к MME
Данные "вниз" (от VLR к АС) (DOWNLINK-UNITDATA)	от VLR к MME
Подтверждение на индикацию отключения EPS (EPS-DETACH-ACK)	от VLR к MME
Индикация отключения EPS (EPS-DETACH-INDICATION)	от MME к VLR
Подтверждение на индикацию отключения IMSI (IMSI-DETACH-ACK)	от VLR к MME
Индикация отключения IMSI (IMSI-DETACH-INDICATION)	от MME к VLR
Обновление местоположения выполнено (LOCATION-UPDATE-ACCEPT)	от VLR к MME
Обновление местоположения отклонено (LOCATION-UPDATE-REJECT)	от VLR к MME
Запрос обновления местоположения (LOCATION-UPDATE-REQUEST)	от MME к VLR
Запрос специфической абонентской информации (MM-INFORMATION-REQUEST)	от VLR к MME
Индикация статуса (STATUS)	от VLR к MME или от MME к VLR
Запрос обслуживания (SERVICE-REQUEST)	от MME к VLR
Индикация активности АС (MS-ACTIVITY-INDICATION)	от MME к VLR
АС недоступна (MS-UNREACHABLE)	от MME к VLR
Данные "вверх" (от АС к VLR) (UPLINK-UNITDATA)	от MME к VLR
Отказ в поиске (PAGING-REJECT)	от MME к VLR

Запрос поиска АС (PAGING-REQUEST)	от VLR к MME
Подтверждение выполнения сброса (RESET-ACK)	от VLR к MME или от MME к VLR
Индикация сброса (RESET-INDICATION)	от VLR к MME или от MME к VLR
Переназначение TMSI выполнено (TMSI-REALLOCATION-COMPLETE)	от MME к VLR
Запрос освобождения (RELEASE-REQUEST)	от VLR к MME

Приложение N 5
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ПЕРЕЧЕНЬ СООБЩЕНИЙ ПРОТОКОЛА DIAMETER ПРИ РЕАЛИЗАЦИИ ИНТЕРФЕЙСОВ ВЗАИМОДЕЙСТВИЯ MME С HSS (ИНТЕРФЕЙС S6A), SGSN С HSS (ИНТЕРФЕЙС S6D), MME С EIR (ИНТЕРФЕЙС S13), SGSN С EIR (ИНТЕРФЕЙС S13'), PCRF С P-GW (ИНТЕРФЕЙС GX), H-PCRF(V-PCRF) С S-GW (ИНТЕРФЕЙС GXC), V-PCRF С H-PCRF (ИНТЕРФЕЙС S9), PCRF С ФУНКЦИЯМИ ПРИЛОЖЕНИЙ (ИНТЕРФЕЙС RX)

Таблица N 1. Сообщения протокола Diameter на интерфейсах S6a/S6d между MME/SGSN и HSS, определение идентификатором приложения (далее - Auth-Application-Id), равным "16777251"

Сообщение	Код сообщения	Направление передачи
Обновление данных о местонахождении подвижного абонента. Запрос (Update-Location-Request (ULR))	316, бит R в поле команды "Флаг" установлен в "1"	от MME или SGSN к HSS

Обновление данных о местонахождении подвижного абонента. Ответ (Update-Location-Answer (ULA))	316, бит R в поле команды "Флаг" очищен	от HSS к MME или SGSN
Информация аутентификации. Запрос (Authentication-Information-Request (AIR))	318, бит R в поле команды "Флаг" установлен в "1"	от MME или SGSN к HSS
Информация аутентификации. Ответ (Authentication-Information-Answer (AIA))	318, бит R в поле команды "Флаг" очищен	от HSS к MME или SGSN
Отмена информации о местонахождении АС. Запрос (Cancel-Location-Request (CLR))	317, бит R в поле команды "Флаг" установлен в "1"	от HSS к MME или SGSN
Отмена информации о местонахождении АС. Ответ (Cancel-Location-Answer (CLA))	317, бит R в поле команды "Флаг" очищен	от MME или SGSN к HSS
Регистрация абонентских данных. Запрос (Insert-Subscriber-Data-Request (IDR))	319, бит R в поле команды "Флаг" установлен в "1"	от HSS к MME или SGSN
Регистрация абонентских данных. Ответ (Insert-Subscriber-Data-Answer (IDA))	319, бит R в поле команды "Флаг" очищен	от MME или SGSN к HSS
Удаление абонентских данных. Запрос (Delete-Subscriber-Data-Request (DSR))	320, бит R в поле команды "Флаг" установлен в "1"	от HSS к MME или SGSN
Удаление абонентских данных. Ответ (Delete-Subscriber-Data-Answer (DSA))	320, бит R в поле команды "Флаг" очищен	от MME или SGSN к HSS
Уведомление о стирании данных абонента. Запрос (Purge-UE-Request (PUR))	321, бит R в поле команды "Флаг" установлен в "1"	от MME или SGSN к HSS
Уведомление о стирании данных абонента. Ответ (Purge-UE-Answer (PUA))	321, бит R в поле команды "Флаг" очищен	от HSS к MME или SGSN
Сброс. Запрос (Reset-Request (RSR))	322, бит R в поле команды "Флаг" установлен в "1"	от HSS к MME или SGSN
Сброс. Ответ (Reset-Answer (RSA))	322, бит R в поле команды "Флаг" очищен	от MME или SGSN к HSS

Уведомление. Запрос (Notify-Request (NOR))	323, бит R в поле команды "Флаг" установлен в "1"	от MME или SGSN к HSS
Уведомление. Ответ (Notify-Answer (NOA))	323, бит R в поле команды "Флаг" очищен	от HSS к MME или SGSN

Таблица N 2. Сообщения протокола Diameter на интерфейсах S13/S13' между MME/SGSN и EIR, определенные Auth-Application-Id, равным "16777252"

Сообщение	Код сообщения	Направление передачи
Проверка международного идентификатора оборудования АС. Запрос (ME-Identity-Check-Request (ECR))	324, бит R в поле команды "Флаг" установлен в "1"	от MME или SGSN к EIR
Проверка международного идентификатора оборудования АС. Ответ (ME-Identity-Check-Answer (ECA))	324, бит R в поле команды "Флаг" очищен	от EIR к MME или SGSN

Таблица N 3. Сообщения протокола Diameter на интерфейсе Gx между PCRF и PDN GW, определенные Auth-Application-Id, равным "16777224", и на интерфейсе S9 между V-PCRF и H-PCRF, определенные Auth-Application-Id, равным "16777267"

Сообщение	Код сообщения	Направление передачи
Правила политики управления и тарификации (PCC). Запрос (CC-Request (CCR))	272, бит R в поле команды "Флаг" установлен в "1"	от PDN GW к PCRF, от V-PCRF к H-PCRF
Правила политики управления и тарификации. Ответ (CC-Answer (CCA))	272, бит R в поле команды "Флаг" очищен	от PCRF к PDN GW от H-PCRF к V-PCRF
Незапрашиваемые правила PCC. Запрос (Re-Auth-Request (RAR))	258, бит R в поле команды "Флаг" установлен в "1"	от PCRF к PDN GW от H-PCRF к V-PCRF
Незапрашиваемые правила PCC. Ответ (Re-Auth-Answer (RAA))	258, бит R в поле команды "Флаг" очищен	от PDN GW к PCRF от V-PCRF к H-PCRF

Таблица N 4. Сообщения протокола Diameter на интерфейсе Rx между PCRF и функциями приложений (далее - AF), определенные Auth-Application-Id, равным "16777236"

Сообщение	Код сообщения	Направление передачи
Информация о сессии. Запрос (AA-Request (AAR))	265, бит R в поле команды "Флаг" установлен в "1"	от AF к PCRF
Информация о сессии. Ответ (AA-Answer (AAA))	265, бит R в поле команды "Флаг" очищен	от PCRF к AF
Незапрашиваемые правила PCC. Запрос (Re-Auth-Request (RAR))	258, бит R в поле команды "Флаг" установлен в "1"	от PCRF к AF
Незапрашиваемые правила PCC. Ответ (Re-Auth-Answer (RAA))	258, бит R в поле команды "Флаг" очищен	от AF к PCRF
Окончание сессии. Запрос (Session-Termination-Request (STR))	275, бит R в поле команды "Флаг" установлен в "1"	от AF к PCRF
Окончание сессии. Ответ (Session-Termination-Answer (STA))	275, бит R в поле команды "Флаг" очищен	от PCRF к AF
Аварийное прекращение сессии. Запрос (Abort-Session-Request (ASR))	274, бит R в поле команды "Флаг" установлен в "1"	от PCRF к AF
Аварийное прекращение сессии. Ответ (Abort-Session-Answer (ASA))	274, бит R в поле команды "Флаг" очищен	от AF к PCRF

Таблица N 5. Сообщения протокола Diameter на интерфейсе Gxc между H-PCRF (V-PCRF) и S-GW, определенные Auth-Application-Id, равным "16777266"

Сообщение	Код сообщения	Направление передачи
Правила политики управления и тарификации (PCC). Запрос. (CC-Request (CCR))	272, бит R в поле команды "Флаг" установлен в "1"	от S-GW к H-PCRF (V-PCRF)
Правила политики управления и тарификации. Ответ. (CC-Answer (CCA))	272, бит R в поле команды "Флаг" очищен	от H-PCRF (V-PCRF) к S-GW
Незапрашиваемые правила PCC. Запрос. (Re-Auth-Request (RAR))	258, бит R в поле команды "Флаг" установлен в "1"	от H-PCRF (V-PCRF) к S-GW

Незапрашиваемые правила PCC. Ответ. (Re-Auth-Answer (RAA))	258, бит R в поле команды "Флаг" очищен	от S-GW к H-PCRF (V-PCRF)

Приложение N 6
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ПЕРЕЧЕНЬ
СООБЩЕНИЙ ПРОТОКОЛА NAS ПРИ РЕАЛИЗАЦИИ ИНТЕРФЕЙСА ВЗАИМОДЕЙСТВИЯ АС И MME (ИНТЕРФЕЙС S1-MME)

Таблица N 1. Сообщения протокола NAS подсистемы управления мобильностью (EMM), передаваемые между АС и MME через интерфейс S1-MME

Сообщение	Направление передачи
Подключение принято (Attach accept)	от MME к АС
Подключение выполнено (Attach complete)	от АС к MME
Подключение отклонено (Attach reject)	от MME к АС
Запрос подключения (Attach request)	от АС к MME
Неуспешная аутентификация (Authentication failure)	от АС к MME
Отклонение аутентификации (Authentication reject)	от MME к АС
Запрос аутентификации (Authentication request)	от MME к АС
Ответ аутентификации (Authentication response)	от АС к MME
Уведомление об обслуживании в CS (CS service notification)	от MME к АС
Отключение завершено (инициатор отключения АС) (Detach accept)	от MME к АС

Отключение завершено (инициатор отключения сеть) (Detach accept)	от АС к MME
Запрос отключения (инициатор отключения АС) (Detach request)	от АС к MME
Запрос отключения (инициатор отключения сеть) (Detach request)	от MME к АС
Транспортировка сообщений NAS "вниз" (доставка коротких сообщений) (Downlink NAS Transport)	от MME к АС
Информация сети об управлении мобильностью (EMM information)	от MME к АС
Состояние процесса управления мобильностью (EMM status)	от MME к АС или от АС к MME
Запрос расширенного обслуживания (Extended service request)	от АС к MME
Команда назначения глобального уникального временного идентификатора (GUTI (Globally Unique Temporary Identifier) reallocation command)	от MME к АС
Подтверждение назначения глобального уникального временного идентификатора (GUTI reallocation complete)	от АС к MME
Запрос идентичности (Identity request)	от MME к АС
Ответ на запрос идентичности (Identity response)	от АС к MME
Команда режима безопасности (Security mode command)	от MME к АС
Выполнение режима безопасности (Security mode complete)	от АС к MME
Отклонение режима безопасности (Security mode reject)	от АС к MME
Отклонение запроса обслуживания (Service reject)	от MME к АС
Запрос обслуживания (Service request)	от АС к MME
Принятие запроса обновления зоны слежения (Tracking area update accept)	от MME к АС
Выполнение обновления зоны слежения (Tracking area update complete)	от АС к MME
Отказ обновления зоны слежения	от MME к АС

(Tracking area update reject)	
Запрос обновления зоны слежения (Tracking area update request)	от АС к MME
Транспортировка сообщений NAS "вверх" (доставка коротких сообщений) (Uplink NAS Transport)	от АС к MME
Основная транспортировка сообщений NAS "вниз" (Downlink generic NAS transport)	от MME к АС
Основная транспортировка сообщений NAS "вверх" (Uplink generic NAS transport)	от АС к MME

Таблица N 2. Сообщения протокола NAS подсистемы управления сессией (ESM), передаваемые между АС и MME на интерфейсе S1-MME

Сообщение	Направление передачи
Запрос активации контекста выбранной EPS принят (Activate dedicated EPS bearer context accept)	от АС к MME
Запрос активации контекста выбранной EPS отклонен (Activate dedicated EPS bearer context reject)	от АС к MME
Запрос активации контекста выбранной EPS (Activate dedicated EPS bearer context request)	от MME к АС
Запрос активации контекста EPS по умолчанию принят (Activate default EPS bearer context accept)	от АС к MME
Запрос активации контекста EPS по умолчанию отклонен (Activate default EPS bearer context reject)	от АС к MME
Запрос активации контекста EPS по умолчанию (Activate default EPS bearer context request)	от MME к АС
Отклонение выделения ресурса (Bearer resource allocation reject)	от MME к АС
Запрос выделения ресурса (Bearer resource allocation request)	от АС к MME
Отклонение модификации ресурса (Bearer resource modification reject)	от MME к АС
Запрос модификации ресурса (Bearer resource modification request)	от АС к MME
Запрос удаления контекста выбранной EPS принят	от АС к MME

(Deactivate EPS bearer context accept)	
Запрос удаления контекста выбранной EPS (Deactivate EPS bearer context request)	от MME к АС
Запрос информации управления сессией (ESM information request)	от MME к АС
Информация управления сессией (ESM information response)	от АС к MME
Состояние процесса управления сессией (ESM status)	от MME к АС или от АС к MME
Запрос модификации контекста EPS принят (Modify EPS bearer context accept)	от АС к MME
Запрос модификации контекста EPS отклонен (Modify EPS bearer context reject)	от АС к MME
Запрос модификации контекста EPS (Modify EPS bearer context request)	от MME к АС
Отклонение возможности соединения с сетью передачи данных (PDN connectivity reject)	от MME к АС
Запрос соединения с сетью передачи данных (PDN connectivity request)	от АС к MME
Отклонение запроса разъединения с сетью передачи данных (PDN disconnect reject)	от MME к АС

Приложение N 7
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ТРЕБОВАНИЯ К ПРОТОКОЛУ GTP

1. Протокол GTP (далее - GTPv2-C) должен реализовывать в S-GW, P-GW, SGSN, MME интерфейсы взаимодействия S5/S8 (если не используется PMIPv6), Sv, S11, S4, S3, S10, S16 и

соответствовать следующим требованиям:

1.1. общий формат заголовка сообщений протокола GTPv2-C приведен на рисунке 1.

Версия	P	T	0	0	0
Тип сообщения					
Длина сообщения					
TEID					
Номер последовательности					
Резерв					

Рисунок 1.

Примечание:

в первом октете:

1) биты 6 - 8 должны определять версию протокола GTPv2-C и быть равны десятичному числу "2";

2) бит 5 (флаг P) должен определять наличие прикрепленных сообщений:

прикрепленных сообщений нет при флаге P равном "0";

другое сообщение GTPv2-C с собственным заголовком и телом присутствует в конце текущего сообщения при флаге P равном "1";

3) бит 4 (флаг T) должен определять наличие поля идентификатора конечной точки туннеля TEID в заголовке:

поле TEID не должно присутствовать при флаге T равном "0";

поле TEID должно следовать в октетах 5 - 8 за полем "Длина сообщения" и занимать четыре октета;

4) биты 3 - 1 (резервные) должен быть равен "0", а получатель не должен анализировать;

второй октет должен определять тип сообщения;

октеты 3 - 4 должны содержать поле "Длина сообщения", содержащее информацию о длине сообщения в октетах, начиная с пятого октета;

октеты 9 - 11 (в случае присутствия TEID) или 5 - 7 (в случае отсутствия TEID) должны содержать поле "Номер последовательности" GTPv2-C. Следующий октет должен использоваться как резерв;

1.2. информационные элементы сообщения GTPv2-C должны следовать за заголовком

сообщения протокола GTPv2-C;

1.3. сообщения протокола GTPv2-C приведены в таблице N 1.

Таблица N 1.

Тип сообщения	Сообщение
1	Запрос "эхо" (Echo Reques)
2	Ответ "эхо" (Echo Response)
3	Версия не поддерживается (Version Not Supported Indication)
От SGSN/MME к MSC серверу (Sv) при хэндовере	
25	Запрос отдельной непрерывности голосового вызова на радиоинтерфейсе (далее - SRVCC) при переходе от сети с коммутацией пакетов к сети с коммутацией каналов (SRVCC PS to CS Request)
26	Ответ на запрос SRVCC при переходе от сети с коммутацией пакетов к сети с коммутацией каналов (SRVCC PS to CS Response)
27	Уведомление о выполнении SRVCC при переходе от сети с коммутацией пакетов к сети с коммутацией каналов (SRVCC PS to CS Complete Notification)
28	Подтверждение выполнения SRVCC при переходе от сети с коммутацией пакетов к сети с коммутацией каналов (SRVCC PS to CS Complete Acknowledge)
29	Уведомление о завершении SRVCC при переходе от сети с коммутацией пакетов к сети с коммутацией каналов (SRVCC PS to CS Cancel Notification)
30	Подтверждение завершения SRVCC при переходе от сети с коммутацией пакетов к сети с коммутацией каналов (SRVCC PS to CS Cancel Acknowledge)
От SGSN/MME к P-GW (S4/S11, S5/S8)	
32	Запрос создания сеанса (Create Session Request)
33	Ответ на запрос создания сеанса (Create Session Response)
34	Запрос изменения носителя (Modify Bearer Request)
35	Ответ на запрос изменения канала передачи данных (Modify Bearer Response)
36	Запрос удаления сеанса (Delete Session Request)

37	Ответ на запрос удаления сеанса (Delete Session Response)
38	Запрос уведомления об изменении (Change Notification Request)
39	Ответ на запрос уведомления об изменении (Change Notification Response)
164	Уведомление о возобновлении связи (Resume Notification)
165	Подтверждение возобновления связи (Resume Acknowledge)
Сообщения без явного ответа (Messages without explicit response)	
64	Команда изменения канала передачи данных (Modify Bearer Command) (MME/SGSN к P-GW - S11/S4, S5/S8)
65	Индикация неудачного изменения канала передачи данных (Modify Bearer Failure Indication) (P-GW к MME/SGSN - S5/S8, S11/S4)
66	Команда освобождения канала передачи данных (Delete Bearer Command) (MME/SGSN к P-GW - S11/S4, S5/S8)
67	Индикация неудачного освобождения канала передачи данных (Delete Bearer Failure Indication) (P-GW к MME/SGSN - S5/S8, S11/S4))
68	Команда распределения ресурсов канала передачи данных (Bearer Resource Command) (MME/SGSN к P-GW - S11/S4, S5/S8)
69	Индикация неудачного распределения ресурсов канала передачи данных (Bearer Resource Failure Indication) (P-GW к MME/SGSN - S5/S8, S11/S4)
70	Индикация неудачного уведомления о передаче данных "вниз" (Downlink Data Notification Failure Indication) (SGSN/MME к S-GW - S4/S11)
71	Активация сеанса трассировки (Trace Session Activation) (MME/SGSN к P-GW - S11/S4, S5/S8)
72	Деактивация сеанса трассировки (Trace Session Deactivation) (MME/SGSN к P-GW - S11/S4, S5/S8)
73	Индикация остановки поиска (Stop Paging Indication) (S-GW к MME/SGSN - S11/S4)
От P-GW к SGSN/MME (S5/S8, S4/S11)	
95	Запрос активации канала передачи данных (Create Bearer Request)

96	Ответ на запрос активации канала передачи данных (Create Bearer Response)
97	Запрос обновления канала передачи данных (Update Bearer Request)
98	Ответ на запрос обновления канала передачи данных (Update Bearer Response)
99	Запрос освобождения канала передачи данных (Delete Bearer Request)
100	Ответ на запрос освобождения канала передачи данных (Delete Bearer Response)
От P-GW к MME, от MME к P-GW, от S-GW к P-GW, от SGW к MME (S5/S8, S11)	
101	Запрос удаления соединения (Delete PDN Connection Set Request)
102	Ответ на запрос удаления соединения (Delete PDN Connection Set Response)
От MME к MME, от SGSN к MME, от MME к SGSN, от SGSN к SGSN (S3/S10/S16)	
128	Запрос идентификации (Identification Request)
129	Ответ на запрос идентификации (Identification Response)
130	Запрос контекста (Context Request)
131	Ответ на запрос контекста (Context Response)
132	Подтверждение ответа на запрос контекста (Context Acknowledge)
133	Запрос передачи при перемещении АС (Forward Relocation Request)
134	Ответ на запрос передачи при перемещении АС (Forward Relocation Response)
135	Уведомление выполнения передачи при перемещении АС (Forward Relocation Complete Notification)
136	Подтверждение выполнения передачи при перемещении АС (Forward Relocation Complete Acknowledge)
137	Уведомление о передаче контекста (Forward Access Context Notification)
138	Подтверждение передачи контекста (Forward Access Context Acknowledge)
139	Запрос отмены перемещения (Relocation Cancel Request)

140	Ответ на запрос отмены перемещения (Relocation Cancel Response)
141	Конфигурация туннеля передачи (Configuration Transfer Tunnel)
152	Передача информации сети радиодоступа (RAN Information Relay)
От SGSN к MME, от MME к SGSN (S3)	
149	Уведомление об отключении (Detach Notification)
150	Подтверждение отключения (Detach Acknowledge)
151	Индикация поиска в сети с коммутацией каналов (CS Paging Indication)
153	Уведомление MME (Alert MME Notification)
154	Подтверждение на уведомление MME (Alert MME Acknowledge)
155	Уведомление активации АС (UE Activity Notification)
156	Подтверждение активации АС (UE Activity Acknowledge)
От SGSN/MME к S-GW, от SGSN к MME (S4/S11/S3), от SGSN к SGSN (S16), от S-GW к P-GW (S5/S8)	
162	Уведомление о прерывании связи (Suspend Notification)
163	Подтверждение прерывания связи (Suspend Acknowledge)
От SGSN/MME к S-GW (S4/S11)	
160	Запрос создания туннеля передачи (Create Forwarding Tunnel Request)
161	Ответ на запрос создания туннеля передачи (Create Forwarding Tunnel Response)
166	Запрос создания туннеля передачи косвенных данных (Create Indirect Data Forwarding Tunnel Request)
167	Ответ на запрос создания туннеля передачи косвенных данных (Create Indirect Data Forwarding Tunnel Response)
168	Запрос удаления туннеля передачи косвенных данных (Delete Indirect Data Forwarding Tunnel Request)
169	Ответ на запрос удаления туннеля передачи косвенных данных (Delete Indirect Data Forwarding Tunnel Response)
170	Запрос освобождения доступа к каналу передачи данных (Release Access Bearers Request)
171	Ответ на запрос освобождения доступа к каналу передачи

	данных (Release Access Bearers Response)
От S-GW к SGSN/MME (S4/S11)	
176	Уведомление о передаче данных "вниз" (Downlink Data Notification)
177	Подтверждение уведомления о передаче данных "вниз" (Downlink Data Notification Acknowledge)
179	Уведомление о рестарте P-GW (P-GW Restart Notification)
180	Подтверждение на уведомление о рестарте PGW (P-GW Restart Notification Acknowledge)
От S-GW к P-GW, от P-GW к S-GW (S5/S8)	
200	Запрос обновления соединения (Update PDN Connection Set Request)
201	Ответ на запрос удаления соединения (Update PDN Connection Set Response)
От MME к S-GW (S11)	
211	Запрос изменения канала доступа (Modify Access Bearers Request)
212	Ответ на запрос изменения канала доступа (Modify Access Bearers Response)

2. Протокол GTP (GTPv1-U) должен реализовывать в оборудовании S-GW, P-GW, SGSN интерфейсы взаимодействия S1-U, S5/S8 (если не используется PMIPv6), S4, S12 и соответствовать следующим требованиям:

2.1. формат заголовка сообщений протокола GTPv1-U приведены на рисунке 2.

Версия	PT	(*)	E	S	PN
Тип сообщения					
Длина сообщения					
TEID					
Номер последовательности					
Номер блока данных					
Дополнительный заголовок					

Рисунок 2.

Примечание:

в первом октете:

1) биты 6 - 8 должны определять версию протокола GTPv1-U и быть равны десятичному числу "1";

2) бит 5 (флаг PT) должен определять тип протокола и быть равны десятичному числу "1";

3) бит 4 (резервный) должен быть равен "0" и не должен анализироваться получателем;

4) бит 3 (флаг E) должен определять наличие поля "Дополнительный заголовок":

поле "Дополнительный заголовок" должно присутствовать при флаге E равном "1";

поле "Дополнительный заголовок" должно отсутствовать или не обрабатываться при флаге E равном "0";

5) бит 2 (флаг S) должен определять наличие поля "Номер последовательности":

поле "Номер последовательности" должно присутствовать при флаге S равном "1";

поле "Номер последовательности" должно отсутствовать или не обрабатываться при флаге S равном "0";

6) бит 1 (флаг PN) должен определять наличие поля "Номер блока данных":

поле "Номер блока данных" должно присутствовать в заголовке сообщения при флаге PN равном "1";

поле "Номер блока данных" должно отсутствовать при флаге PN равном "0";

второй октет должен определять тип сообщения;

октеты 3 - 4 должны содержать поле "Длина сообщения", указывающего длину сообщения в октетах, начиная с девятого октета;

поле TEID должно занимать четыре октета с пятого по восьмой;

октеты 9 - 10 должны содержать поле "Номер последовательности";

поля "Номер блока данных" и "Дополнительный заголовок" должны занимать по одному октету;

2.2. информационные элементы или пакеты пользовательских данных должны следовать за заголовком сообщений протокола GTPv1-U.

2.3. сообщения протокола GTPv1-U приведены в таблице N 2.

Таблица N 2.

Тип сообщения	Сообщение
1	Запрос "эхо" (Echo Request)
2	Ответ "эхо" (Echo Response)
26	Ошибочная индикация (Error Indication)
31	Уведомление о поддержке расширенных заголовков (Supported Extension Headers Notification)
254	Маркер конца обмена информацией по туннелю (End Marker)
255	Блок данных протокола GTP (G-PDU)

Приложение N 8
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ТРЕБОВАНИЯ К ПРОТОКОЛУ PMIPV6

1. Требования к протоколу PMIPv6:

1.1. формат заголовка Mobility Header и перечень поддерживаемых полей приведены в таблице N 1.

Таблица N 1.

N поля	Поля заголовка	Длина поля (бит)
1	Payload Proto	8
2	Header Len	8

3	MH Type	8
4	Резерв	8
5	Checksum	16
6	Message Data	0 - n

Примечание:

поле Payload Proto должно идентифицировать тип заголовка, следующего за заголовком Mobility Header и должно использовать значения, аналогичные используемым в заголовке "Следующий заголовок" протокола IPv6 описанное в подпункте 1.2.5 пункта 1 Приложения N 8 Правил;

поле Header Len должно указывать длину заголовка (за исключением первых 8 октетов) в единицах, равных 8 октетам, и должно быть равно "0", если сообщение не имеет параметров;

поле MH Type должно указывать тип передаваемого сообщения.

поле Резерв должно быть равно "0";

поле Checksum должно содержать контрольную сумму заголовка Mobility Header, начиная с поля Payload Proto;

поле Message Data должно быть полем переменной длины и должно содержать данные сообщения. Тип сообщения должен указываться в поле MH Type;

1.2. поле "Дополнение до границы заголовка" должно использоваться для выравнивания границы заголовка по длине, кратной 8 октетам. (свободные позиции должны заполняться нулями);

1.3. сообщения для интерфейсов S5, S8, S2a, S2b:

"Обновление регистрации прокси" (PBU - Proxy Binding Update);

"Подтверждение обновления регистрации" (PBA - Proxy Binding Acknowledgement);

"Индикация аннулирования регистрации" (BRI - Binding Revocation Indication);

"Подтверждение аннулирования регистрации" (BRA - Binding Revocation Acknowledgement);

1.4. формат заголовка Type 2 Routing Header и перечень поддерживаемых полей приведены в таблице N 2.

Таблица N 2.

N поля	Поля заголовка	Длина поля (бит)
1	Next Header	8

2	Hdr Ext Len	8
3	Routing Type	8
4	Segments Left	8
5	Резерв	32
6	Home Address	16

Примечание:

поле Next Header должно идентифицировать тип заголовка, следующего за заголовком Type 2 Routing Header и использовать значения, аналогичные используемым в заголовке "Следующий заголовок" протокола IPv6;

поле Hdr Ext Len должно указывать длину заголовка (за исключением первых 8 октетов) в единицах, равных 8 октетам и быть равно двум единицам;

поле Routing Type должно указывать тип маршрутизации и быть равно "2";

поле Segments Left должно быть равно "1";

поле Резерв быть равно "0";

поле Home Address (16 октетов) должно содержать домашний адрес узла назначения.

Приложение N 9
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ТРЕБОВАНИЯ К ИНТЕРФЕЙСАМ ВЗАИМОДЕЙСТВИЯ

1. Оборудование MME должно взаимодействовать с оборудованием UE по интерфейсу S1-MME с использованием протокола NAS, с оборудованием сети радиодоступа стандартов LTE/LTE-Advanced (далее - E-UTRAN) по интерфейсу S1-MME с использованием протокола S1-AP, с оборудованием MSC сервера/VLR по интерфейсу SGs с использованием протокола SGsAP, с оборудованием HSS/LTE по интерфейсу S6a с использованием протокола Diameter, с оборудованием SGSN по интерфейсу S3 с использованием протокола GTP уровня управления

версии 2 (далее - GTPv2-C), с оборудованием EIR по интерфейсу S13 с использованием протокола Diameter.

Взаимодействие MME с SGSN должно осуществляться по интерфейсу Gn с использованием протокола GTP, если обеспечивающий взаимодействие с MME SGSN не реализует интерфейс S3.

2. Оборудование S-GW должно взаимодействовать с оборудованием E-UTRAN по интерфейсу S1-U с использованием протокола GTP уровня пользователя версии 1 (далее - GTPv1-U), с оборудованием SGSN по интерфейсу S4, с оборудованием P-GW своей сети по интерфейсу S5, другой сети по интерфейсу S8 с использованием протоколов GTPv2-C и GTPv1-U или PMIPv6, с оборудованием MME по интерфейсу S11 с использованием протокола GTPv2-C, с оборудованием UTRAN по интерфейсу S12 с использованием протокола GTP.

3. Оборудование P-GW должно взаимодействовать с оборудованием S-GW своей сети по интерфейсу S5, другой сети по интерфейсу S8 с использованием протоколов GTPv2-C и GTPv1-U или PMIPv6, с оборудованием PCRF по интерфейсу Gx с использованием протокола Diameter. Взаимодействие SGSN с P-GW должно осуществляться по интерфейсам Gn или Gp с использованием протокола GTP, если SGSN не реализует интерфейс S4. Оборудование P-GW должно взаимодействовать с оборудованием внешней сети передачи данных по интерфейсу SGi.

4. Оборудование HSS должно взаимодействовать с оборудованием MME по интерфейсу S6a с использованием протокола Diameter.

5. Оборудование PCRF должно взаимодействовать с оборудованием P-GW по интерфейсу Gx, с оборудованием PCRF другой сети по интерфейсу S9 и с обслуживающей сетью IP по интерфейсу Rx с использованием протокола Diameter.

6. Оборудование EIR должно взаимодействовать с оборудованием MME по интерфейсу S13 с использованием протокола Diameter.

7. Оборудование SGSN должно взаимодействовать с оборудованием MME по интерфейсу S3 с использованием протокола GTPv2-C, по интерфейсу Gn с использованием протокола GTP, если обеспечивающий взаимодействие с MME SGSN не реализует интерфейс S3, с оборудованием S-GW по интерфейсу S4 с использованием протоколов GTPv2-C и GTPv1-U, с P-GW по интерфейсам Gn или Gp с использованием протокола GTP, если SGSN не реализует интерфейс S4.

8. В оборудовании коммутации стандарта LTE должны использоваться интерфейсы к сети передачи данных с использованием контроля несущей и обнаружением коллизий. Требования к параметрам согласно приложению 25 к Правилам применения оборудования проводных и оптических систем передачи абонентского доступа, утвержденным приказом Министерства информационных технологий и связи Российской Федерации от 24.08.2006 N 112 (зарегистрирован в Министерстве юстиции Российской Федерации 4 сентября 2006 г., регистрационный N 8194), с изменениями, внесенными приказами Министерства связи и массовых коммуникаций Российской Федерации от 23.04.2013 N 93 (зарегистрирован в Министерстве юстиции Российской Федерации 14 июня 2013 г., регистрационный N 28788) и от 17.03.2014 N 45 (зарегистрирован в Министерстве юстиции Российской Федерации 16 апреля 2014 г., регистрационный N 31998);

9. Для обслуживания non-3GPP доступа должны реализовываться следующие интерфейсы взаимодействия:

S2a (взаимодействие TWAN (TWAG) и S-GW либо P-GW в зависимости от архитектуры сети, обеспечение передачи данных пользователя и сигнализации, реализация протоколов управления мобильностью PMIPv6, MIPv4 (с адресацией FACoA) или GTP уровня управления и уровня пользователя);

S2b (взаимодействие ePDG и S-GW либо P-GW в зависимости от архитектуры сети, обеспечение передачи данных пользователя и сигнализации, реализация протоколов управления мобильностью PMIPv6 или GTP);

S2c (взаимодействие UE с P-GW, обеспечение передачи данных пользователя и сигнализации, поддержка протоколов управления мобильностью DSMIPv6 и IPSec). Формирование безопасных туннелей IPSec должно выполняться при помощи протокола IKEv2;

S5 (взаимодействие S-GW и P-GW, обеспечение передачи данных пользователя и сигнализации с использованием туннелей, реализация протоколов GTP либо PMIPv6);

S8 (взаимодействие S-GW в VPLMN и P-GW в HPLMN, использование пользовательского трафика через HPLMN при роуминге и в случае маршрутизации, реализация протокола GTP либо PMIPv6);

S6a (взаимодействие MME и HSS, использование для аутентификации и авторизации, реализация протокола Diameter);

S6b (взаимодействие P-GW и 3GPP AAA сервера либо 3GPP AAA прокси-сервера (при роуминге в случае маршрутизации трафика через визитную сеть) с использованием Diameter);

Gx (обеспечение передачи сообщений управления качеством передачи данных QoS и правил тарификации от PCRF к P-GW с использованием протокола Diameter);

Gxa (обеспечение передачи сообщений протокола Diameter для управления качеством передачи данных QoS от PCRF к TWAN);

Gxb (взаимодействие ePDG и VPCRF, обеспечение передачи сообщений протокола Diameter для управления качеством передачи данных QoS от VPCRF к ePDG);

Gxc (обеспечение передачи сообщений протокола Diameter для управления качеством передачи данных QoS между S-GW и PCRF);

S9 (обеспечение передачи сообщений протокола Diameter для управления качеством передачи данных QoS в условиях роуминга между HPCRF и VPCRF). По интерфейсу S9 должны передаваться данные о правилах тарификации в случае маршрутизации пользовательского трафика в PDN из визитной сети;

SGi (взаимодействие P-GW и PDN);

SWa (взаимодействие UTWAN с 3GPP AAA сервером (прокси-сервером) по протоколу Diameter для безопасной передачи информации аутентификации, авторизации и учета (тарификации);

STa (взаимодействие TWAN с 3GPP AAA сервером (прокси-сервером) по протоколу Diameter для безопасной передачи информации аутентификации, авторизации и учета (тарификации) с поддержкой протокола EAP-AKA, EAP-AKA');

SWd (взаимодействие 3GPP AAA прокси-сервера и 3GPP AAA сервера по протоколу Diameter с поддержкой протокола EAP-AKA, EAP-AKA');

SWm (взаимодействие 3GPP AAA сервера (прокси-сервера) и ePDG для передачи данных сигнализации AAA и передачи данных аутентификации и авторизации протоколов управления мобильности PMIPv6 (MAG-AAA) и MIPv6 (MIPv6 NAS-AAA) с поддержкой протокола EAP-AKA);

SWu (взаимодействие мобильного терминала и шлюза ePDG, обеспечение безопасной передачи данных в туннеле IPSec). Обмен ключами при формировании туннеля IPSec должен выполняться при помощи протокола IKEv2;

SWx (взаимодействие 3GPP AAA сервера и базы данных HSS, обеспечение обмена данными для аутентификации и авторизации UE).

Интерфейсы S5, S8, S2a, S2b должны реализовывать один и тот же протокол - либо PMIPv6, либо GTP.

Приложение N 10
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ПЕРЕЧЕНЬ
ДАННЫХ ОБ ОБСЛУЖИВАЕМЫХ В S-GW АБОНЕНТСКИХ РАДИОСТАНЦИЯХ, ПОДДЕРЖИВАЮЩИХ СТАНДАРТЫ LTE, GSM 900/1800, UMTS

Данные	LTE и/или LTE-Advanced	GSM 900/1800, UMTS
Международный номер АС (IMSI)	присутствует	присутствует
Индикатор неподтверждения подлинности IMSI (IMSI unauthenticated-indicator)	присутствует	присутствует
Международный идентификатор оборудования АС и версия программного обеспечения (IMEI/IMEISV) (ME Identity)	присутствует	присутствует

Международный номер АС в сети ISDN (MSISDN)	присутствует	присутствует
Идентификатор выбранного оператора сети (Selected CN operator id)	присутствует	присутствует
Идентификатор конечной точки туннеля MME для интерфейса S11 (MME TEID for S11)	присутствует	
IP адрес MME для интерфейса S11 (MME IP address for S11)	присутствует	
Идентификатор конечной точки туннеля S-GW для интерфейсов S11/S4 (для плоскости управления) (S-GW TEID for S11/S4 (control plane))	присутствует	присутствует
IP адрес S-GW для интерфейса S11/S4 (для плоскости управления) (S-GW IP address for S11/S4 (control plane))	присутствует	присутствует
IP адрес SGSN для интерфейса S4 (для плоскости управления) (SGSN IP address for S4 (control plane))		присутствует
Идентификатор конечной точки туннеля SGSN для интерфейса S4 (для плоскости управления) (SGSN TEID for S4 (control plane))		присутствует
Подробное описание трейса (Trace reference)	присутствует	присутствует
Тип трейса (Trace Type)	присутствует	присутствует
Идентификатор триггера (Trigger id)	присутствует	присутствует
Идентификатор центра управления и обслуживания, куда будут передаваться отчеты по трейсам (OMC Identity)	присутствует	присутствует
Последний известный идентификатор соты местонахождения АС (Last known Cell Id)	присутствует	присутствует
Время последнего обновления идентификатора соты местонахождения АС (Last known Cell Id age)	присутствует	присутствует
Данные для каждого соединения с сетью передачи данных		
Используемая точка доступа (APN in Use)	присутствует	присутствует
Характеристики учета стоимости для АС в сети передачи данных EPS (EPS PDN Charging Characteristics)	присутствует	присутствует

IP адрес используемого P-GW (для плоскости управления) (P-GW Address in Use (control plane))	присутствует	присутствует
Идентификатор конечной точки туннеля P-GW для интерфейсов S5/S8 (для плоскости управления) (только для GTP на S5/S8) (P-GW TEID for S5/S8 (control plane))	присутствует	присутствует
IP адрес используемого P-GW (для плоскости пользователя) (P-GW Address in Use (user plane))	присутствует	присутствует
Ключ GRE, выделенный P-GW для передачи пользовательских данных "вверх" (только для PMIPv6 на S5/S8) (P-GW GRE Key for uplink traffic (user plane))	присутствует	присутствует
IP адрес S-GW для интерфейса S5/S8 (для плоскости управления) (S-GW IP address for S5/S8 (control plane))	присутствует	присутствует
Идентификатор конечной точки туннеля S-GW для интерфейсов S5/S8 (для плоскости управления) (только для GTP на S5/S8) (S-GW TEID for S5/S8 (control plane))	присутствует	присутствует
IP адрес используемого S-GW (для плоскости пользователя) (S-GW Address in Use (user plane))	присутствует	присутствует
Ключ GRE, выделенный S-GW для передачи пользовательских данных "вниз" (только для PMIPv6 на S5/S8) (S-GW GRE Key for downlink traffic (user plane))	присутствует	присутствует
Канал передачи данных по умолчанию (только для PMIPv6 на S5/S8) (Default Bearer)	присутствует	присутствует
Данные о каждом канале передачи данных EPS в соединении сети передачи данных		
Идентификатор канала передачи данных EPS (EPS Bearer ID)	присутствует	присутствует
Шаблон потока трафика (TFT)	присутствует	присутствует
IP адрес используемого P-GW (для плоскости пользователя) (только для GTP на S5/S8) (P-GW Address in Use (user plane))	присутствует	присутствует
Идентификатор конечной точки туннеля P-GW для	присутствует	присутствует

интерфейса S5/S8 (для плоскости пользователя) (только для GTP на S5/S8) (P-GW TEID for S5/S8 (user plane))		
IP адрес S-GW для интерфейса S5/S8 (для плоскости пользователя) (S-GW IP address for S5/S8 ((user plane))	присутствует	присутствует
Идентификатор конечной точки туннеля S-GW для интерфейсов S5/S8 (для плоскости пользователя) (только для GTP на S5/S8) (S-GW TEID for S5/S8 (user plane))	присутствует	присутствует
IP адрес S-GW для интерфейсов S1-u, S12 и S4 (для плоскости пользователя) (S-GW IP address for S1-u, S12 and S4 (user plane))	присутствует	присутствует
Идентификатор конечной точки туннеля S-GW для интерфейсов S1-u, S12 и S4 (для плоскости пользователя) (S-GW TEID for S1-u, S12 and S4 (user plane))	присутствует	присутствует
IP адрес узла радиодоступа eNodeB для интерфейса S1-u (eNodeB Address for S1-u)	присутствует	
Идентификатор конечной точки туннеля узла радиодоступа eNodeB для интерфейса S1-u (eNodeB TEID for S1-u)	присутствует	
IP адрес контроллера сети радиодоступа UMTS для интерфейса S12 (RNC IP address for SI2)		присутствует
Идентификатор конечной точки туннеля контроллера сети радиодоступа UMTS для интерфейса S12 (RNC TEID for S12)		присутствует
IP адрес SGSN для интерфейса S4 (для плоскости пользователя) (SGSN IP address for S4 (user plane))		присутствует
Идентификатор конечной точки туннеля SGSN для интерфейса S4 (для плоскости пользователя) (SGSN TEID for S4 (user plane))		присутствует
Качество обслуживания в канале передачи данных EPS (ARP, GBR, MBR, QIC) (EPS Bearer QoS)	присутствует	присутствует
Идентификатор данных учета стоимости, генерируемых S-GW и P-GW	присутствует	присутствует

(Charging Id)		

Приложение N 11
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ТРЕБОВАНИЯ К СИСТЕМЕ УЧЕТА ДАННЫХ ДЛЯ НАЧИСЛЕНИЯ ПЛАТЫ

1. Система учета данных для начисления платы (далее - СУД) должна выполнять сбор и хранение учетных данных для последующего определения стоимости для всех видов учетного трафика.

2. СУД должна обеспечивать передачу учетных данных в автоматизированную систему расчетов (далее - АСР).

3. Формирование учетных данных должно начинаться с момента индикации ответа вызываемого абонента (службы) и прекращаться при отбое любого из абонентов (службы).

4. СУД должна создавать запись для обеспечения функций учета, регистрирующую следующие данные:

1) категорию и номер вызывающего абонента или адресную информацию вызывающей стороны;

2) номер вызываемого абонента (службы) или адресную информацию вызываемой стороны;

3) дату (день, месяц, год) и время начала соединения (час, минута, секунда);

4) продолжительность соединения или время окончания соединения (час, минута, секунда);

5) используемые в соединении услуги;

6) объем передаваемой/принимаемой информации с указанием качества предоставления услуги, в случае установления соединений для передачи данных;

7) индикаторы записи;

8) идентификаторы операторов;

9) идентификаторы оборудования EPC, обеспечивающего сбор данных для учета стоимости.

5. СУД должна обеспечивать хранение учетных данных.

6. Передача информации в АСР должна осуществляться с использованием стандартных сетевых протоколов и открытых интерфейсов.

7. Для бесперебойной работы СУД должны обеспечиваться дублирование и резервирование устройств. Системе управления и технического обслуживания должны посылаться сообщения об отказе или неисправности оборудования СУД при возникновении отказов или неисправности оборудования СУД, а также в процессе передачи информации в АСР, и одновременно осуществляться запись сведений о неисправностях.

8. В СУД должна быть предусмотрена система защиты от несанкционированного доступа к информации.

9. В СУД обеспечена возможность установки обслуживаемым персоналом параметров, регистрируемых в записях о соединениях, и типов записей.

10. В СУД должна обеспечиваться функция немедленного вывода на устройство технического обслуживания учетной информации для оперативной обработки данных.

Приложение N 12
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ПЕРЕЧЕНЬ
ДАННЫХ ОБ ОБСЛУЖИВАЕМЫХ В P-GW АБОНЕНТСКИХ РАДИОСТАНЦИЯХ, ПОДДЕРЖИВАЮЩИХ СТАНДАРТЫ LTE, GSM 900/1800, UMTS

Таблица.

Данные	LTE и/или LTE-Advanced	GSM 900/1800, UMTS
Международный номер АС (IMSI)	присутствует	присутствует
Индикатор неподтверждения подлинности IMSI	присутствует	присутствует

(IMSI unauthenticated-indicator)		
Международный идентификатор оборудования АС и версия программного обеспечения (IMEI/IMEISV) (ME Identity)	присутствует	присутствует
Международный номер АС в сети ISDN (MSISDN)	присутствует	присутствует
Идентификатор выбранного оператора сети (Selected CN operator id)	присутствует	присутствует
Тип технологии радиодоступа (RAT (Radio Access Technology) type)	присутствует	присутствует
Подробное описание трейса (Trace reference)	присутствует	присутствует
Тип трейса (Trace Type)	присутствует	Присутствует
Идентификатор триггера (Trigger id)	присутствует	присутствует
Идентификатор центра управления и обслуживания, куда будут передаваться отчеты по трейсам (OMC Identity)	присутствует	присутствует
Данные для каждой используемой точки доступа		
Используемая точка доступа (APN in Use)	присутствует	присутствует
Точка доступа - Общая максимальная скорость передачи (APN-AMBR)	присутствует	присутствует
Данные о соединении сети передачи данных для каждой точки доступа		
IP-адрес(а) (IP Address(es))	присутствует	присутствует
Тип сети передачи данных (PDN type)	присутствует	присутствует
IP-адрес используемого S-GW (для уровня управления) (S-GW Address in Use (control plane))	присутствует	присутствует
Идентификатор конечной точки туннеля S-GW для интерфейсов S5/S8 (для уровня управления) (только для GTP на S5/S8) (S-GW TEID for S5/S8 (control plane))	присутствует	присутствует

IP адрес используемого S-GW (для уровня пользователя) (только для PMIP на S5/S8) (S-GW Address in Use (user plane))	присутствует	присутствует
Ключ GRE, выделенный S-GW для передачи пользовательских данных "вниз" (только для PMIP на S5/S8) (S-GW GRE Key for downlink traffic (user plane))	присутствует	присутствует
IP адрес P-GW для интерфейса S5/S8 (для уровня управления) (P-GW IP address for S5/S8 (control plane))	присутствует	присутствует
Идентификатор конечной точки туннеля P-GW для интерфейсов S5/S8 (для уровня управления) (только для GTP на S5/S8) (P-GW TEID for S5/S8 (control plane))	присутствует	присутствует
IP адрес используемого P-GW (для уровня пользователя) (только для PMIP на S5/S8) (P-GW Address in Use (user plane)	присутствует	присутствует
Ключ GRE, выделенный P-GW для передачи пользовательских данных "вверх" (только для PMIP на S5/S8) (P-GW GRE Key for uplink traffic (user plane))	присутствует	присутствует
Возможность передачи сообщений об изменении информации об AC (MS Info Change Reporting support indication)		присутствует
Необходимость передачи сообщений об изменении информации об AC (MS Info Change Reporting Action)	присутствует	присутствует
Необходимость передачи сообщений об изменении информации о закрытой группе пользователей (CSG Information Reporting Action)	присутствует	присутствует
Согласованный режим управления каналом (BCM)		присутствует
Идентификатор канала передачи данных по умолчанию (Default bearer)	присутствует	присутствует
Характеристики учета стоимости абонентской станции в сети передачи данных EPS (EPS PDN Charging Characteristics)	присутствует	присутствует
Данные о каждом канале передачи данных в соединении сети передачи данных (только для GTP на S5/S8)		
Идентификатор канала передачи данных EPS	присутствует	присутствует

(EPS Bearer ID)		
Шаблон потока трафика (TFT)	присутствует	присутствует
IP адрес используемого S-GW (для уровня пользователя) (S-GW Address in Use (user plane))	присутствует	присутствует
Идентификатор конечной точки туннеля S-GW для интерфейсов S5/S8 (для уровня пользователя) (S-GW TEID for S5/S8 (user plane))	присутствует	присутствует
IP адрес используемого P-GW (для уровня пользователя) (P-GW Address in Use (user plane))	присутствует	присутствует
Идентификатор конечной точки туннеля P-GW для интерфейса S5/S8 (для уровня пользователя) (P-GW TEID for S5/S8 (user plane))	присутствует	присутствует
Качество обслуживания в канале передачи данных EPS (ARP, GBR, MBR, QCI) (EPS Bearer QoS)	присутствует	присутствует
Идентификатор данных учета стоимости, генерируемых S-GW и P-GW (Charging Id)	присутствует	присутствует

Приложение N 13
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ПЕРЕЧЕНЬ
ХРАНЯЩИХСЯ В HSS ДАННЫХ ОБ АБОНЕНТСКИХ РАДИОСТАНЦИЯХ, ПОДДЕРЖИВАЮЩИХ СТАНДАРТ LTE

Таблица.

Данные	Комментарии

Международный номер АС (IMSI)	
Международный номер АС в сети ISDN (MSISDN)	опциональный
Международный идентификатор оборудования АС и версия программного обеспечения (IMEI/IMEISV)	
Параметры аутентификации: произвольный номер (RAND), ожидаемый ответ (XRES), ключ (KASME), символ аутентификации (AUTN) (Authentication Vector)	
Идентификатор MME, обслуживающего АС в данный момент (MME Identity)	
Возможности данного MME (MME Capabilities)	
EMM и ESM контекст для АС удалены из MME (MS PS Purged from EPS)	
Ограничения обслуживающего оператора (ODB parameters)	
Ограничения доступа в соответствии с подпиской (Access Restriction)	
Характеристика для учета стоимости АС в соответствии с подпиской в сети (EPS Subscribed Charging Characteristic)	
Подробное описание трейса (Trace Reference)	
Тип трейса (Trace Type)	
Идентификатор центра управления и обслуживания, куда будут передаваться отчеты по трейсам (OMC Identity)	
Подписка АС - Общая максимальная скорость передачи (Subscribed-UE-AMBR)	
Замена точки доступа (APN-OI replacement)	
Индекс приоритетности выбора технологии радиодоступа/Частоты (RFSP Index)	
Параметр запроса доступности АС, указывающий, что подтверждение активности АС от MME зарегистрировано в HSS (URRP-MME)	
Данные подписки закрытой группы пользователей (CSG Subscription Data)	
Разрешение использования в VPLMN локального IP доступа (VPLMN LIPA Allowed) <*>	
Подписка на периодическое обновление зоны маршрутизации/слежения по таймеру (Subscribed Periodic	

RAU/TAU Timer) <*>	
Подписка на приоритетное обслуживание в домене CS (MPS CS priority) <*>	
Возможность поддержки для АС непрерывности голосового вызова на радиоинтерфейсе (UE-SRVCC-Capability)	
Подписка на приоритетное обслуживание в EPS (MPS EPS priority) <*>	
Один или несколько контекстов сети передачи данных	
Идентификатор контекста (Context Identifier)	
Адрес сети передачи данных (PDN Address)	
Тип сети передачи данных (IPv4, IPv6, IPv4v6) (PDN Type)	
Замещение точки доступа (APN-OI Replacement)	опциональный
Наименование точки доступа (Access Point Name (APN))	
Разрешения возможности распределения трафика IP для APN (SIPTO permissions) <*>	
Разрешения LIPA (LIPA permissions) <*>	LIPA - разрешено, только LIPA, LIPA - при условии
Профиль качества обслуживания в соответствии с подпиской в EPS (QCI и ARP) (EPS subscribed QoS profile)	
Подписка Точка доступа - Общая максимальная скорость передачи (Subscribed-APN-AMBR)	
Характеристики учета стоимости АС в соответствии с подпиской в сети передачи данных EPS (EPS PDN Subscribed Charging Characteristics)	
Возможность использовать для APN АС P-GW домашней или визитной сети (VPLMN Address Allowed)	
Идентификатор P-GW (P-GW identity)	
Тип выбора P-GW (статический, динамический) (P-GW Allocation Type)	
Сеть радиотелефонной связи, в которой находится динамически выбранный P-GW (PLMN of P-GW)	
Однородная поддержка голосового вызова IMS	
в зонах слежения обслуживающего MME (Homogenous Support	

of IMS Over PS Sessions for MME)	
Перечень соотношений: Наименование точки доступа - Идентификатор P-GW	
Номер соотношения APN - P-GW (APN - P-GW relation #n)	
Примечание: <*> - "данные" обязательные только для стандарта LTE-Advanced.	

Приложение N 14
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ТРЕБОВАНИЯ
К ДАННЫМ ОБ АБОНЕНТСКОЙ РАДИОСТАНЦИИ, ХРАНЯЩИМСЯ В EIR

1. В EIR должны храниться международный идентификатор оборудования АС (IMEI) или международный идентификатор оборудования и версия программного обеспечения оборудования АС (IMEISV).

2. Формат IMEI:

код типа (TAC) должен содержать 8 десятичных знаков;

серийный номер (SNR) должен содержать 6 десятичных знаков (индивидуальный серийный номер, однозначно идентифицирующий оборудование АС в пределах TAC);

резерв должен содержать 1 десятичный знак, принимающий значение равное "0" при передаче IMEI от АС.

Число десятичных знаков в IMEI должно быть равно 15.

3. Формат IMEISV:

код типа (TAC) должен содержать 8 десятичных знаков;

серийный номер (SNR) должен содержать 6 десятичных знаков (индивидуальный серийный номер, однозначно идентифицирующий оборудование АС в пределах TAC);

номер версии программного обеспечения оборудования АС (SVN), идентифицирующий номер версии программного обеспечения мобильного оборудования. Длина поля должна составлять 2 десятичных знака.

Число десятичных знаков в IMEISV должно быть равно 16.

4. Международные идентификаторы оборудования АС, содержащиеся в EIR, должны разделяться на три списка:

белый список, содержащий IMEI допущенного для работы в сети оборудования;

черный список, содержащий IMEI не допущенного для работы в сети оборудования;

серый список, содержащий IMEI не запрещенного для работы в данной сети оборудования кроме случаев, когда IMEI оборудования содержится в черном списке или не содержится в белом списке.

5. Оборудование коммутации стандарта LTE должно осуществлять проверку IMEI при каждой попытке доступа АС в EPC и останавливать любую попытку доступа при получении из регистра EIR одного из следующих ответов: "оборудование находится в черном списке" или "оборудование не содержится в белом списке".

Приложение N 15
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ТРЕБОВАНИЯ
К ЦЕНТРУ УПРАВЛЕНИЯ И ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ (ЦУ И ТО)

1. В Центр Управления и Технического Обслуживания (ЦУ и ТО) должна направляться информация о состоянии оборудования коммутации стандарта LTE. Для управления и технического обслуживания оборудования коммутации стандарта LTE должен использоваться централизованный метод.

2. ЦУ и ТО должен использоваться для управления оборудованием коммутации стандарта LTE, контроля работоспособности оборудования коммутации стандарта LTE, сбора и вывода информации о функционировании оборудования коммутации стандарта LTE обслуживающему персоналу.

3. Функции управления, эксплуатации и технического обслуживания должны выполняться автоматически в соответствии с программным обеспечением или по командам обслуживающего персонала, вводимым с терминала технического обслуживания, с использованием "меню" или графического интерфейса.

4. ЦУ и ТО должен выполнять следующие функции:

административное управление;

контроль функционирования оборудования коммутации стандарта LTE;

управление восстановлением работоспособности оборудования коммутации стандарта LTE;

управление тестированием и диагностикой.

5. Функция административного управления оборудованием коммутации стандарта LTE должна включать:

1) управление конфигурацией оборудования коммутации стандарта LTE, обеспечивающее:

ввод, изменение и удаление данных конфигурации;

активацию или деактивацию загрузки программного обеспечения (далее - ПО) в оборудование узла связи и его работоспособность;

2) управление командами системы, обеспечивающее следующие функции:

вывод всех кодов команд, реализованных в системе;

возможность изменения существующих и введение новых команд;

3) административное управление абонентскими данными, обеспечивающее следующие функции:

создание, изменение, удаление, считывание абонентских данных;

блокировка или разблокировка абонентов;

просмотр, изменение и вывод данных учета стоимости;

4) управление маршрутизацией;

5) управление защитой информации, обеспечивающее следующие функции:

защита доступа к ЦУ и ТО посредством паролей;

наличие не менее двух категорий пользователей (администратор и пользователь), имеющих различные пароли и различные права доступа к ЦУ и ТО;

6) управление системными часами реального времени, обеспечивающее контроль и возможность установки системных часов реального времени.

6. Контроль функционирования оборудования коммутации стандарта LTE должен включать

обнаружение и фиксацию аварийных сигналов с функциональных блоков, модулей, систем передачи, источников электропитания и их обработку с последующим выводом аварийных сообщений на дисплей и принтер терминала технического обслуживания или системную панель аварийных сигналов.

7. Контроль функционирования оборудования коммутации стандарта LTE должен осуществляется постоянно или периодически (по расписанию или по команде технического персонала с терминала технического обслуживания).

8. Автоматический контроль должен осуществляться распределенно (модули самостоятельно должны обнаруживать повреждения и ошибки).

9. Аварийные сообщения должны быть разделены на категории по срочности восстановления неисправностей:

1) критические аварии (неисправность, вызывающая значительное ухудшение обслуживания и требующая немедленного вмешательства);

2) главные аварии (серьезные неисправности, требующие вмешательства в течение дня);

3) незначительные аварии (неисправности, не требующие немедленного вмешательства и подлежащие устранению в период наименьшей нагрузки).

10. Управление восстановлением работоспособности должно осуществлять контроль состояния функциональных блоков и управлять перезапусками блоков с возможностью перезапуска для предотвращения влияния неисправности.

11. Обеспечение надежности должно реализовываться путем резервирования основных групповых и управляющих блоков.

12. Перезапуск ПО должен производиться с сохранением статистических и тарификационных данных и, в основном, с сохранением установленных соединений.

13. Перезагрузка ПО оборудования коммутации стандарта LTE должна производиться с сохранением данных учета стоимости соединений и статистических данных.

14. Управление тестированием и диагностикой должно осуществлять обнаружение и локализацию неисправного оборудования с помощью диагностических программ.

15. ЦУ и ТО должен обеспечивать автоматический ежемесячный статистический учет ситуаций в оборудовании коммутации стандарта LTE и программном обеспечении.

16. ЦУ и ТО должен обеспечивать возможность сбора и отображения статистических данных.

Приложение N 16
к Правилам применения оборудования
коммутации сетей подвижной

радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ТРЕБОВАНИЯ
К ОБОРУДОВАНИЮ КОММУТАЦИИ СТАНДАРТА LTE В РЕЖИМЕ ОКАЗАНИЯ УСЛУГ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ОБОРУДОВАНИЯ КОММУТАЦИИ IMS

1. Для подключения к оборудованию IMS UE должно инициировать:

процедуру подключения UE к сети радиодоступа (далее - EPS);

процедуру активации канала передачи данных в EPS;

выделение IP-адреса P-CSCF;

процедуру регистрации в IMS.

2. При оказании услуг передачи данных и телефонного соединения через оборудование коммутации IMS временно (на время взаимодействия UE с оборудованием коммутации IMS) в рамках процедур подключения UE к EPS и соединения с сетью передачи данных EPS должно обеспечиваться назначение UE IP-адреса в формате, определенном протоколами IP четвертой или шестой версий (далее - IPv4, IPv6), принадлежащем одной из сетей IMS, взаимодействующей с P-GW:

IP-адреса сети IMS домашнего оператора;

IP-адреса сети IMS визитного оператора;

IP-адреса сети взаимодействующей с IMS домашнего оператора.

Выделение UE IP-адреса P-CSCF должно осуществляться одним из следующих способов:

с помощью протокола динамической конфигурации (далее - DHCP) и сервера имен доменов (далее - DNS);

с помощью процедуры активации канала передачи данных в EPS;

UE должно выбирать P-CSCF из списка, хранящегося в идентификационном модуле абонента для работы в IMS (далее - ISIM);

UE должно выбирать P-CSCF из списка объектов управления IMS.

Первоначально активация канала передачи данных в EPS должна осуществляться в рамках процедуры подключения UE к EPS, инициируемой UE с помощью сообщения протокола NAS "Запрос подключения". В "Запросе подключения" в параметре настройки пользовательского оборудования, определяющем оборудование коммутации, через которое будет осуществляться

телефонное соединение, в третьем октете второй и третий биты должны иметь одно из трех значений:

"01" - голос только через IMS;

"10" - в первую очередь голос следует передавать через домен CS, во вторую - через IMS;

"11" - в первую очередь голос следует передавать через IMS, во вторую - через домен CS.

Третий бит при установлении соединения для передачи голоса должен быть равен "0", для передачи данных - "1".

Активация канала передачи данных EPS должна осуществляться с помощью сообщений "Запрос соединения с сетью передачи данных" протокола NAS и "Запрос активации канала передачи данных" протокола GTPv2-C. В параметре "Запроса соединения с сетью передачи данных", определяющем опции конфигурации протокола, должны быть установлены:

запрос адреса P-CSCF (если используется второй способ выделения адреса P-CSCF);

флаг сигнализации IMS.

В параметре сообщения протокола NAS "Подключение принято", определяющем поддерживаемые сетью функции, первый бит третьего октета должен быть равен "1", что указывает на поддержку IMS голоса через домен коммутации пакетов на интерфейсе S1.

Передача UE IP-адреса (в параметре "Адрес сети передачи данных") и IP-адреса P-CSCF (в параметре "Протокол параметров конфигурации") должна осуществляться в ответе на "Запрос активации канала передачи данных" протокола GTPv2-C и в одном из сообщений "Запрос активации контекста EPS по умолчанию", "Запрос активации контекста выбранной EPS" протокола NAS.

UE должен присваиваться новый IP-адрес при перемещения UE в зону обслуживания другого P-GW.

UE должно осуществлять процедуру регистрации или перерегистрации в IMS после назначения или изменения IP-адреса UE или IP-адреса P-CSCF.

Освобождение динамического IP-адреса UE должно осуществляться при разрыве соединения с оборудованием коммутации IMS с помощью сообщения "Запрос разъединения с сетью передачи данных" протокола NAS или при окончании времени регистрации.

Приложение N 17
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства

цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ТРЕБОВАНИЯ К ПРОТОКОЛУ MIPV4

1. Требования к дополнениям и расширениям протоколов, необходимых для поддержки мобильности пользователя в сети, использующей IPv4:

1.1. Требования к дополнительным сообщениям "Запрос регистрации" (Registration Request), "Результат регистрации" (Registration Reply), поддерживающие управление мобильностью пользователя и отправляемые с порта UDP/TCP 434:

а) формат сообщения "Запрос регистрации" приведен на рисунке 1.

Тип	S	B	D	M	G	r	T	X	Длительность регистрации
Домашний адрес									
Адрес домашнего агента									
CoA									
Идентификация									
Расширения									

Рисунок 1

Примечание:

поле "Тип" (1 байт) должно быть равно "1";

поле "S" (1 бит) должно быть равно "1", если мобильный узел запрашивает сохранение нескольких предыдущих адресов привязки;

поле "B" (1 бит) должно быть равно "1", если мобильный узел запрашивает у домашнего агента доставку широковещательных дейтаграмм;

поле "D" (1 бит) должно быть равно "1", если мобильный узел декапсулирует дейтаграммы, направленные по адресу CoA;

поле "M" (1 бит) должно быть равно "1", если мобильный узел запрашивает у домашнего агента режим минимальной инкапсуляции данных;

поле "G" (1 бит) должно быть равно "1", если мобильный узел запрашивает у домашнего агента режим инкапсуляции GRE;

поля "r" и "X" (по 1 биту) должно быть равны "0" и должны игнорироваться при приеме;

поле "T" (1 бит) должно указывать на запрос обратного туннелирования;

поле "Длительность регистрации" (2 байта) должно указывать длительность регистрации в секундах (при значении "0" - запрос отмены регистрации, при значении "0xffff" - бесконечность);

поле "Домашний адрес" (4 байта) должно указывать IP-адрес мобильного узла в домашней сети;

поле "Адрес домашнего агента" (4 байта) должно указывать IP-адрес домашнего агента;

поле "CoA" (4 байта) должно указывать временный IP-адрес мобильного узла в визитной сети;

поле "Идентификация" должно содержать сгенерированное мобильным узлом 64-битовое число, используемое для сопоставления запроса регистрации и ответа;

б) формат сообщения "Результат регистрации" приведен на рисунке 2.

Тип	Код	Длительность регистрации
Домашний адрес		
Адрес домашнего агента		
Идентификация		
Расширения		

Рисунок 2

Примечание:

поле "Тип" (1 байт) должно быть равно "3";

поле "Код" (1 байт) должно указывать результат регистрации;

поле "Длительность регистрации" (2 байта) должно указывать длительность регистрации в секундах (при значении "0" - отмена регистрации, при значении "0xffff" - бесконечность);

поле "Домашний адрес" (4 байта) должно указывать IP-адрес мобильного узла в домашней сети;

поле "Адрес домашнего агента" (4 байта) должно указывать IP-адрес домашнего агента;

поле "Идентификатор" должно содержать сгенерированное мобильным узлом 64-битовое число, используемое для сопоставления запроса регистрации и ответа;

в) в сообщениях "Запрос регистрации", "Результат регистрации" должно присутствовать одно из следующих расширений: "Аутентификация в домашней сети (Mobile-Home Authentication), тип расширения - 32", "Аутентификация в визитной сети (Mobile-Foreign Authentication), тип расширения - 33", "Аутентификация между домашней и визитной сетями (Foreign-Home

Authentication), тип расширения - 34".

Формат расширений для сообщений "Запрос регистрации", "Результат регистрации" приведен на рисунке 3.

Тип расширения	Длина	SPI
SPI		Аутентификатор

Рисунок 3.

Примечание:

поле "Длина" должно указывать длину аутентификатора плюс 4 байта.

поле "SPI" (Security Parameter Index) должно указывать идентификатор параметров защиты, используемый для вычисления аутентификатора. Алгоритм аутентификации, используемый по умолчанию, должен быть HMAC-MD5.

поле "Аутентификатор" должна быть переменной длины. Аутентификатор должен вычисляться для каждого сообщения регистрации, а также должны использоваться поля поступивших с порта 434 UDP сообщений регистрации, все присутствующие в сообщениях регистрации расширения, поля "Тип", "Длина" и "SPI" расширения.

1.2. требования к сообщениям протокола ICMPv4 "Объявление маршрутизатора" (Router Advertisement), "Запрос доступности маршрутизатора" (Router Solicitation), поддерживающим управление мобильностью пользователя:

а) значения расширений, используемых для сообщений протокола ICMPv4 "Объявление маршрутизатора" (Router Advertisement), "Запрос доступности маршрутизатора" (Router Solicitation):

"0" - один байт заполнения, последнее расширение сообщения ICMP должно использоваться для дополнения длины сообщения до четного количества байт;

"16" - "Объявление мобильного агента" (Mobility Agent Advertisement);

"19" - длина префикса;

б) формат расширения "Объявление мобильного агента" приведен на рисунке 4.

Тип расширения	Длина	Порядковый номер							
Длительность регистрации		R	B	H	F	M	G	r	T	Резерв
Адрес(а) CoA									

Рисунок 4.

Примечание:

поле "Тип расширения" (1 байт) должно быть равно "16";

поле "Порядковый номер" (2 байта) должно содержать номер сообщения с расширением Agent Advertisement;

поле "Длительность регистрации" (2 байта) должно содержать информацию о длительности регистрации в секундах (при значении "0" - запрос отмены регистрации, при значении "0xffff" - бесконечность);

поле "R" (1 бит) должно содержать информацию, что требуется регистрация в визитном агенте (FA) при наличии у мобильного узла адреса CoA;

поле "B" (1 бит) должно содержать информацию, что FA не осуществляет регистрацию мобильных узлов;

поле "H" (1 бит) (домашний агент, HA) должно содержать информацию, что агент предлагает услугу домашнего агента;

поле "F" (1 бит) (визитный агент) должно содержать информацию, что агент предлагает услугу визитного агента;

поле "M" (1 бит) (минимальная инкапсуляция) должно содержать информацию, что агент реализует прием дейтаграмм, использующих минимальную инкапсуляцию;

поле "G" (1 бит) (GRE инкапсуляция) должно содержать информацию, что агент реализует прием дейтаграмм, которые используют GRE инкапсуляцию;

поле "r" (1 бит) должно быть резервным и равно "0";

поле "T" (1 бит) должно содержать информацию, что FA поддерживает обратную инкапсуляцию;

поле "Резерв" (8 бит) должно быть равно "0";

поле "Адрес(а) CoA" должно содержать один или более адресов CoA при установлении бита F (количество адресов, присутствующих в поле, должно определяться указателем длины);

в) формат расширения "Длина префикса" (19) приведен на рисунке 5.

Тип расширения	Длина	Длина префикса

Рисунок 5.

Примечание:

поле "Тип расширения" (1 байт) должно быть равно "19";

поле "Длина префикса" (8 бит) должно определять число начальных битов, определяющих номер сети в адресе маршрутизатора, указанного в сообщении ICMP Router Advertisement (для каждого адреса должна указываться своя длина префикса).

Расширение "Длина префикса" может следовать за расширением "Объявление мобильного агента" и должно указывать количество бит префикса сети, применяемого к каждому адресу маршрутизатора, указанному в сообщении ICMP Router Advertisement.

Приложение N 18
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ТРЕБОВАНИЯ К ПРОТОКОЛАМ MIPV6, DSMIPV6

1. Требования к дополнительному заголовку протокола мобильности IPv6 Mobility Header (MH), обеспечивающему мобильность пользователя:

1.1. заголовок "Mobility Header" должен обозначаться в поле "Next Header" (Следующий заголовок) значением "135" и включать поля, приведенные в таблице N 1.

Таблица N 1.

Поля заголовка		
N поля	Название	Длина поля (бит)
1	Payload Proto	8
2	Header Len	8
3	MH Type	8
4	Резерв	8
5	Checksum	16
6	Message Data	0-n

Примечание:

поле "Payload Proto" должно идентифицировать тип заголовка, следующего сразу за Mobility Header, использовать значения, соответствующие заголовку "Следующий заголовок" протокола IPv6.

поле "Header Len" должно указывать длину заголовка (за исключением первых 8 октетов) в единицах, равных 8 октетам. Значение Header Len должно устанавливаться равным "0", если сообщение не имеет параметров.

поле "MH Type" должно указывать тип передаваемого сообщения.

поле "Резерв" должно устанавливаться равным "0".

поле "Checksum" должно содержать контрольную сумму заголовка "Mobility Header", начиная с поля "Payload Proto".

поле "Message Data" должно быть полем переменной длины и должно содержать данные сообщения. Тип сообщения должен указываться в поле "MH Type".

поле "Дополнение до границы заголовка" должно использоваться для выравнивания границы заголовка по длине, кратной 8 октетам. Свободные позиции должны заполняться нулями.

1.2. сообщения, передаваемые при использовании заголовка "Mobility Header":

а) "Запрос обновления привязки UE" (сообщение BRR (Binding Refresh Request) должно включать следующие поля (поле "MH Type" для сообщения BRR должно быть равно "0"):

"Резерв" (16 бит) (должно быть резервным, равно "0" и должно игнорироваться получателем);

"Опции мобильности" (Mobility Options) (должно быть переменной длины (длина полного заголовка мобильности должна быть кратна 8 октетам) и должно содержать одну или несколько опций мобильности, закодированных в формате TLV, или не должно содержать таких опций, а получатель должен игнорировать и пропускать любые опции);

б) "Инициирование проверки домашнего адреса" (сообщение HoTI (Home Test Init) должно включать следующие поля (поле "MH Type" для сообщения HoTI должно быть равно "1"):

"Резерв" (16 бит) (должно быть резервным, равно "0" и должно игнорироваться получателем);

"Идентифицирующая цепочка домашнего адреса" (Home Init Cookie) (должно быть 64-битовым полем, содержащим значение вновь сгенерированного случайного числа, которое возвращается в UE в сообщении Home Test);

"Опции мобильности" (Mobility Options) (должно быть полем переменной длины (длина полного заголовка мобильности должна быть кратна 8 октетам), содержать одну или несколько опций мобильности, закодированных в формате TLV, или не должно содержать таких опций, а получатель должен игнорировать и пропускать любые опции).

Мобильный узел должен использовать сообщение "Home Test Init" для инициализации процедуры обратной маршрутизации и запроса маркера "Home keygen token" от узла-корреспондента, туннелируемое через домашнего агента, когда мобильный узел находится в визитной сети;

в) "Инициирование проверки временного адреса" (сообщение Care-of Test Init) должно включать следующие поля (поле "MH Type" для сообщения "Care-of Test Init" должно быть равно

"2"):

"Идентифицирующая цепочка временного адреса" (Care-of Init Cookie) (должно быть 64-битовым полем, содержащим значение вновь сгенерированного случайного числа, которое возвращается в UE в сообщении "Care-of Test");

"Опции мобильности" (Mobility Options) (должно быть полем переменной длины (длина полного заголовка мобильности должна быть кратна 8 октетам), содержать одну или несколько опций мобильности, закодированных в формате TLV, или не должно содержать таких опций, а получатель должен игнорировать и пропускать любые опции).

Мобильный узел должен использовать сообщение "Care-of Test Init" (CoTI) для инициализации процедуры обратной маршрутизации и запроса маркера "Care-of Keygen Token" от узла-корреспондента;

г) "Проверка домашнего адреса" (сообщение Home Test), используемое для осуществления возврата UE идентифицирующей цепочки, посылаемой узлу-корреспонденту в сообщении "Home Test Init" должно включать следующие поля (поле "MH Type" для сообщения "Home Test" должно быть равно "3"):

"Одноразовый индекс домашнего номера" (Home Nonce Index) (должно быть 16-битовым полем и возвращаться узлу-корреспонденту мобильным узлом в сообщении "Binding Update");

"Идентифицирующая цепочка домашнего адреса" (Home Init Cookie) (должно быть 64-битовым полем и приниматься в сообщении "Home Test Init");

"Маркер Home Keygen Token" (должно содержать 64 бита маркера, используемого в процедуре обратной маршрутизации);

"Опции мобильности" (Mobility Options) (должно быть полем переменной длины (длина полного заголовка мобильности должна быть кратна 8 октетам), содержать одну или несколько опций мобильности, закодированных в формате TLV, или не должно содержать таких опций, а получатель должен игнорировать и пропускать любые опции);

д) "Care-of Test", используемое для возврата UE идентифицирующей цепочки, посылаемой узлу-корреспонденту в сообщении "Care-of Test Init" должно включать следующие поля (поле "MH Type" для сообщения "Care-of Test" должно быть равно "4"):

"Одноразовый индекс временного номера" (Care-of Nonce Index) (должно быть 16-битовым полем, возвращаемым обратно узлу-корреспонденту мобильным узлом в сообщении "Binding Update");

"Идентифицирующая цепочка временного адреса" (Care-of Init Cookie) (должно быть 64-битовым полем, содержащим принятое в сообщении "Care-of Test Init" значение);

"Маркер Care-of Keygen Token" (должно содержать 64 бита маркера, используемого в процедуре обратной маршрутизации);

"Опции мобильности" (Mobility Options) (должно быть полем переменной длины (длина полного заголовка мобильности должна быть кратна 8 октетам), содержать одну или несколько опций мобильности, закодированных в формате TLV, или не должно содержать таких опций, а получатель должен игнорировать и пропускать любые опции);

е) "Информирование об обновлении привязки" (сообщение BU (Binding Update) должно использоваться мобильным узлом для уведомления других узлов о своем новом временном адресе и включать следующие поля (поле "MH Type" для сообщения "Binding Update" должно быть равно "5"):

"Порядковый номер" (Sequence) (должно быть 16-битовым полем, используемым для нумерации сообщений "Binding Update" для сопоставления сообщения "Binding Acknowledgement" с сообщением "Binding Update");

бит "Подтверждение" (A) (Acknowledge) (должен устанавливаться посылающим мобильным узлом и содержать информацию об ожидании сообщения "Подтверждение привязки");

бит "Регистрация в домашнем агенте" (H) (Home Registration) (должен устанавливаться посылающим мобильным узлом, чтобы принимающий узел домашней сети служил ему домашним агентом);

бит "Соответствие линка и локального адреса" (L) (Link-Local Address Compatibility) (должен устанавливаться при одинаковом идентификаторе интерфейса домашнего адреса, переданного мобильным узлом, и линка);

бит "Возможность мобильного управления ключами" (Key Management Mobility Capability) (K) (должен быть равен "0", когда используемый для установления контекстов безопасности между мобильным узлом и домашним агентом протокол IPsec не переносит информацию о перемещении, должен использоваться только в сообщениях "Binding Update", посылаемых домашнему агенту, и должен быть равен "0" в других сообщениях "Binding Update", а узлы-корреспонденты должны игнорировать указанный бит);

"Зарезервировано" (Reserved) (12 бит) (должно быть равно "0" и должно игнорироваться получателем);

"Время жизни" (Lifetime) (16 бит) (должно указывать на количество единиц времени, оставшихся до того момента, когда привязка UE считается просроченной (при значении "0" указывает на необходимость удаления информации о привязке мобильного узла при этом указанный временный адрес должен устанавливаться равным домашнему адресу). За единицу времени должны быть приняты 4 секунды);

"Опции мобильности" (Mobility Options) (должно быть полем переменной длины (длина полного заголовка мобильности должна быть кратна 8 октетам), содержать одну или несколько опций мобильности, закодированных в формате TLV, или не должно содержать таких опций, получатель должен игнорировать и пропускать любые опции).

В сообщении "Binding Update" должны быть допустимы следующие опции мобильности:

опция "Данные авторизации привязки" (Binding Authorization Data) (должна быть обязательной в сообщениях "Binding Update", посылаемых узлу-корреспонденту);

опция "Индексы одноразовых номеров" (Nonce Indices);

опция "Альтернативный (запасной) временный адрес" (Alternate Care-of Address).

Поле заголовка "Mobility Header Header Len" должно быть равно "1" при отсутствии опций в сообщении, а также следует использовать 4 октета заполнения.

ж) "Подтверждение приема сообщения об обновлении привязки" (сообщение BA (Binding Acknowledgement) (поле "MH Type" для сообщения BA должно быть равно "6");

з) "Сообщение об ошибке, связанной с мобильностью" (сообщение BE (Binding Error) (поле "MH Type" для сообщения BE должно быть равно "7");

1.3. дополнительный заголовок протокола IPv6 "Type 2 Routing Header", обеспечивающий дополнительные данные для маршрутизации:

а) поля заголовка "Type 2 Routing Header" приведены в таблице N 2.

Таблица N 2.

Поля заголовка		
N поля	Название	Длина поля (бит)
1	Next Header	8
2	Hdr Ext Len	8
3	Routing Type	8
4	Segments Left	8
5	Резерв	32
6	Home Address	16

Примечание:

поле "Next Header" должно идентифицировать тип заголовка, следующего за заголовком "Type 2 Routing Header" и использовать для идентификации заголовков те же значения, что и в заголовке "Следующий заголовок" протокола IPv6;

поле "Hdr Ext Len" должно содержать информацию о длине заголовка (за исключением первых 8 октетов) в единицах, равных 8 октетам и быть равно "2";

поле "Routing Type" должно содержать информацию о типе маршрутизации и быть равно "2";

поле "Segments Left" должно быть равно "1";

поле "Резерв" должно быть равно "0";

поле "Home Address" должно быть полем длиной 16 октетов и содержать домашний адрес узла назначения.

1.4. дополнительные сообщения ICMP IPv6:

Протоколом Mobile IPv6 вводится четыре новых типа сообщений для протокола ICMP.

Для определения адреса домашнего агента должны использоваться новые сообщения ICMP:

"Запрос определения адреса домашнего агента" (Home Agent Address Discovery Request) (должно использоваться мобильным терминалом для инициации механизма динамического определения адреса домашнего агента);

"Ответ определения адреса домашнего агента" (Home Agent Address Discovery Reply) (должно использоваться домашним агентом для ответа мобильному узлу, использующему механизм динамического определения адреса домашнего агента).

Для перенумерования сетей и конфигурирования адресов на мобильном узле должны использоваться новые сообщения ICMP:

"Запрос мобильного префикса" (Mobile Prefix Solicitation);

"Объявление мобильного префикса" (Mobile Prefix Advertisement).

а) формат сообщения "Запрос определения адреса домашнего агента" (Home Agent Address Discovery Request) приведен на рисунке 1.

Тип	Код	Контрольная сумма
Идентификатор		Резерв

Рисунок 1

Примечания:

поле "Тип" (1 байт) должно быть равно "144";

поле "Код" (1 байт) должно быть равно "0";

поле "Идентификатор" (2 байта) должно содержать сгенерированное мобильным узлом 64-битовое число, используемое для сопоставления запроса и ответа;

поле "Резерв" должно быть равно "0" и должно игнорироваться получателем;

б) формат сообщения "Ответ определения адреса домашнего агента" (Home Agent Address Discovery Reply) приведен на рисунке 2.

Тип	Код	Контрольная сумма
Идентификатор		Резерв
Адрес домашнего агента		

Рисунок 2

Примечание:

поле "Тип" (1 байт) должно быть равно "145";

поле "Код" (1 байт) должно быть равно "0";

поле "Идентификатор" (2 байта) должно содержать число из сообщения "Home Agent Address Discovery Request";

поле "Резерв" должно быть равно "0" и должно игнорироваться получателем;

поле "Адреса домашнего агента" должно содержать список адресов домашних агентов мобильного узла в домашней сети;

в) формат сообщения "Запрос мобильного префикса" (Mobile Prefix Solicitation) приведен на рисунке 3.

Тип	Код	Контрольная сумма
Идентификатор		Резерв

Рисунок 3

Примечание:

поле "Тип" (1 байт) должно быть равно "146";

поле "Код" (1 байт) должно быть равно "0";

поле "Идентификатор" (2 байта) должно содержать сгенерированное мобильным узлом 64-битовое число, используемое для сопоставления запроса и ответа;

поле "Резерв" должно должно быть равно "0" и должно игнорироваться получателем.

Поля пакета протокола IPv6 должны заполняться следующим образом: в поле "Адрес источника" (Source Address) должен указываться временный адрес мобильного узла, а в поле "Адрес места назначения" (Destination Address) - адрес домашнего агента мобильного узла;

г) формат сообщения "Объявление мобильного префикса" (Mobile Prefix Advertisement) приведен на рисунке 4.

Тип	Код	Контрольная сумма		
Идентификатор		M	O	Резерв
Опции				

Рисунок 4

Примечание:

поле "Тип" (1 байт) должно быть равно "147";

поле "Код" (1 байт) должно быть равно "0";

поле "Идентификатор" (2 байта) должно содержать сгенерированное мобильным узлом 64-

битовое число, используемое для сопоставления запроса и ответа;

поле "M" (1 бит) (флаг управляемого конфигурирования адресов) должно указывать на доступность адреса через DHCPv6 при значении поля "M" равном "1";

поле "O" (1 бит) (флаг другой конфигурации) должно указывать на существование другой информации о конфигурации, доступной через DHCPv6, при значении поля "O" равном "1";

поле "Резерв" должно быть равно "0" и должно игнорироваться получателем;

поле "Опции" (сообщение должно содержать одну или несколько опций "Prefix Information") должно передавать префикс, который мобильный узел использует для конфигурирования своего домашнего адреса (домашних адресов).

Поля пакета протокола IPv6 должны заполняться следующим образом: в поле "Адрес источника" (Source Address) должен указываться адрес домашнего агента, а в поле "Адрес места назначения" (Destination Address) - значение поля "Source Address" из сообщения "Запрос мобильного префикса".

2. Требования к формату сообщений протокола обнаружения соседних узлов (далее - NDP):

2.1. формат сообщения "Объявление маршрутизатора" (Router Advertisement) приведен на рисунке 5.

Тип	Код				Контрольная сумма
Текущий предел шагов	M	O	H	Резерв	Время жизни маршрутизатора
Время достижимости					
Время повторной передачи					
Опции					

Рисунок 5

Примечание:

поле "Тип" (1 байт) должно быть равно "134";

поле "Код" (1 байт) должно быть равно "0";

поле "Текущий предел шагов" должно содержать значение по умолчанию и его следует поместить в поле числа шагов IP-заголовка для исходящих пакетов;

поле "M" (1 бит) (флаг управляемого конфигурирования адресов) должно содержать информацию о доступности адреса через DHCPv6 при значении поля "M" равном "1";

поле "O" (1 бит) (флаг другой конфигурации) должно содержать информацию о существовании другой информации о конфигурации, доступной через DHCPv6, при значении поля "O" равном "1";

поле "H" (1 бит) (флаг домашнего агента) содержать информацию о функционировании маршрутизатора в качестве домашнего агента при значении поля "H" равном "1";

поле "Резерв" должно быть равно "0" и должно игнорироваться получателем;

поле "Время жизни маршрутизатора" должно содержать информацию о времени функционирования устройства в качестве маршрутизатора, измеряемое в секундах;

поле "Время достижимости" (4 байта) должно содержать информацию о времени доступности соседнего маршрутизатора после получения подтверждения доступности, измеряемое в миллисекундах;

поле "Время повторной передачи" (4 байта) должно содержать информацию о времени между повторно пересылаемыми сообщениями запросов, измеряемое в миллисекундах.

3. Требования к протоколу DSMIPv6:

3.1. на мобильном терминале должно устанавливаться программное обеспечение (далее - ПО) клиента DSMIPv6, на P-GW - ПО домашнего агента DSMIPv6 для функционирования протокола DSMIPv6 на интерфейсе S2c;

3.2. расширения для сообщений протокола MIPv6:

а) Для сообщения "Binding Update", передаваемого от UE к домашнему агенту или точке привязки мобильности (Mobility Anchor Point (далее - MAP):

опция "IPv4 Home Address Option" (должна указывать домашний адрес мобильного узла формата IPv4);

опция "IPv4 Care-of Address Option" (должна указывать временный адрес мобильного узла формата IPv4 при нахождении его в сети, поддерживающей только протокол IPv4);

флаг (F) (должен указывать при его установке на необходимость инкапсуляции с помощью протокола UDP);

б) для сообщения "Binding Acknowledgement", передаваемого от домашнего агента или MAP к UE:

опция "IPv4 Acknowledgement Option" (должна указывать на осуществление обновления адреса привязки для мобильного узла адресом формата IPv4 и адрес мобильного узла формата IPv4);

опция "NAT Detection Option" (должна указывать UE на наличие трансляции сетевого адреса (Network Address Translation, далее - NAT) при помощи домашнего агента, включать счетчик повторной передачи обновления и флага "F", указывающего при его установке на необходимость инкапсуляции с помощью протокола UDP.

Приложение N 19

к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ТРЕБОВАНИЯ К ПРОТОКОЛУ IKEV2

1. Протокол обмена ключами в Интернет (Internet Key Exchange) версия 2 (далее - IKEv2) должен пользоваться услугами протокола UDP через порты 500 и 4500. В дейтаграмме UDP должна осуществляться передача одного сообщения IKEv2. Адреса IP и номера портов UDP в заголовках должны сохраняться и использоваться для передачи ответных пакетов. Сообщение IKEv2 должно начинаться непосредственно после заголовка UDP при передаче через порт UDP 500, а при передаче через порт UDP 4500 перед сообщением IKEv2 должны помещаться четыре октета с нулевыми значениями. Эти октеты не являются частью сообщения IKEv2 и не должны учитываться в размерах и контрольных суммах IKEv2.

2. Требования к заголовкам протокола IKEv2:

2.1. сообщение протокола IKEv2 должно начинаться с заголовка. После заголовка должен следовать один или несколько элементов данных IKEv2, идентифицируемых значением поля "Next Payload" предыдущего элемента данных. Элементы данных должны обрабатываться в порядке их следования в сообщении IKEv2 путем вызова соответствующей процедуры, определяемой значением поля "Next Payload" в заголовке IKEv2, затем значением поля "Next Payload" в первом элементе данных IKEv2 и далее, пока в поле "Next Payload" не будет обнаружено нулевое значение, указывающее на отсутствие следующего элемента данных. Элемент данных типа Encrypted при приеме должен быть дешифрован, а результат расшифровки необходимо разбирать как дополнительные элементы данных. Элемент Encrypted должен быть последним элементом в пакете. В зашифрованные элементы недопустимо включать другие элементы типа Encrypted;

2.2. формат заголовка IKEv2 приведен на рисунке 1.

<table>
<tr><td colspan="6">Initiator's SPI</td></tr>
<tr><td colspan="6">Responder's SPI</td></tr>
<tr><td>Next Payload</td><td>MjVer</td><td>MnVer</td><td>ExchType</td><td>Flags</td><td>Message ID</td></tr>
<tr><td colspan="5">Length</td><td></td></tr>
</table>

Рисунок 1.

Примечание:

поле "Initiator's SPI" (8 октетов) должно содержать значение, выбранное инициатором для уникальной идентификации параметров безопасности (Security Parameter Index, далее - SPI) IKEv2 и не должно быть равно "0";

поле "Responder's SPI" (8 октетов) должно содержать значение, выбранное ответчиком для уникальной идентификации защищенной связи IKE и должно быть равно "0" в первом сообщении начального обмена IKEv2 (включая повторы этого сообщения, содержащие cookie), для всех остальных сообщений не должно быть равно "0";

поле "Next Payload" (1 октет) должно содержать информацию о типе элемента данных, расположенного сразу после заголовка.

Формат и значения типа элемента данных:

"Mj Ver" (4 бита) должен задавать старшую часть номера версии используемого протокола IKE. Реализации на основе IKEv2 должны устанавливать значение Major Version равное "2". Основанные на этой версии протокола IKE реализации должны отвергать или игнорировать пакеты со значением этого поля, превышающим "2";

"Mn Ver" (4 бита) должен задавать младшую часть номера версии IKE. Реализации на основе IKEv2 должны устанавливать значение Minor Version равное "0" и игнорировать младшую часть номера в принимаемых сообщениях;

"Exchange Type" (1 октет) должен указывать тип используемого обмена, ограничивающий набор элементов данных в каждом сообщении и порядок сообщений в обмене.

Типы обмена приведены в таблице N 1.

Таблица N 1.

Тип обмена	Значение
IKE_SA_INIT	34
IKE_AUTH	35
CREATE_CHILD_SA	36
INFORMATIONAL	37
Резерв IANA	38 - 239
Резерв для частного использования	240 - 255

Примечание:

"Flags" (1 октет) должен указывать на наличие специфических опций в сообщении при установлении соответствующего бита флага в "1";

"Message ID" (4 октета) должен содержать идентификатор сообщения и использоваться для управления повторной передачей потерянных пакетов и связывания запросов с откликами;

"Length" (4 октета) должен содержать размер всего сообщения (заголовок и элементы данных) в октетах;

2.3. структура базового заголовка элемента данных (payload) IKEv2 приведена на рисунке 2.

Идентификатор следующего элемента	C	Резерв	Размер текущего элемента
Элементы данных			

Рисунок 2

Примечание:

поле "Идентификатор следующего элемента" (Next Payload) (1 октет) должно указывать тип следующего элемента данных в сообщении, должно быть равно "0", если текущий элемент является последним, и не должно использоваться для элемента типа Encrypted (всегда должен быть последним в сообщении). Указанный элемент должен содержать структуры данных в формате дополнительных элементов. В заголовке элемента Encrypted поле "Next Payload" должно устанавливаться в соответствии с типом первого вложенного элемента (вместо "0").

Значения идентификаторов следующих элементов сообщения приведены в таблице N 2.

Таблица N 2.

Идентификатор следующего элемента	Обозначения	Значение
Отсутствует следующий элемент		0
Резерв		1 - 32
Контекст безопасности	SA	33
Обмен ключами	KE	34
Идентификатор инициатора	IDi	35
Идентификатор отвечающего	IDr	36
Сертификат	CERT	37
Запрос сертификата	CERTREQ	38
Идентификация	AUTH	39
Случайное число	Ni, Nr	40
Уведомление	N	41
Удаление	D	42

Идентификатор реализации	V	43
Селектор трафика - Инициатор	TSi	44
Селектор трафика - Ответчик	TSr	45
Кодирование	E	46
Конфигурация	CP	47
Расширяемая идентификация	EAP	48
Резерв IANA		49 - 127
Для частного применения		128 - 255

Примечание:

поле "C" (1 бит) должно быть равно "0" для обеспечения заявленной отправителем возможности по пропуску получателем элемента данных, когда получатель не идентифицирует код в поле "Next Payload" предыдущего элемента. Получатель должен игнорировать этот флаг при идентификации типа элемента. Флаг "C" должен относиться к текущему элементу данных;

поле "Резерв" (7 битов) должно быть равно "0" при передаче и игнорироваться на приеме;

поле "Размер текущего элемента" (Payload Length) (2 октета) должно содержать размер текущего элемента данных в октетах с учетом базового заголовка;

2.4. структура элемента данных "Предложения" (SA) приведена на рисунке 3.

<table>
<tr><td>0 или 2</td><td>Резерв</td><td colspan="2">Длина предложения</td></tr>
<tr><td>Номер предложения</td><td>Идентификатор протокола</td><td>Значение SPI</td><td>Число преобразований</td></tr>
<tr><td colspan="4">SPI передающей стороны</td></tr>
<tr><td colspan="4">Структура преобразования</td></tr>
</table>

Рисунок 3

Данные контекста безопасности (Security Association Payload, далее - SA) должны использоваться для согласования атрибутов защищенной связи. Элемент SA может включать несколько предложений, упорядоченных в порядке снижения приоритета. Каждое предложение может включать несколько протоколов IPsec (IKEv2, ESP, AH), каждый протокол может включать множество преобразований, а каждое преобразование может включать несколько атрибутов.

Примечание:

первый октет должен содержать информацию о том, является ли предложение последним в субструктуре предложений элемента SA (предложение должно быть последним при значении

первого октета равном "0" и не должно являться последним при значении равном "2");

поле "Длина предложения" (2 октета) должно указывать размер предложения, включая все входящие в него преобразования и атрибуты;

поле "Номер предложения" (1 октет) должно указывать номер предложения. Первое предложение в элементе SA должно иметь номер "1", а номера последующих предложений должны совпадать с номером предшественника (И - пересечение двух предложений) или быть на 1 больше (ИЛИ - объединение двух предложений). Все номера предложений в элементе SA должны совпадать при приеме и соответствовать номеру переданного предложения, которое было принято;

поле "Идентификатор протокола" (1 октет) должно задавать идентификатор протокола IPsec для текущего согласования;

поле "Значение SPI" (1 октет) должно использоваться для начального согласования IKE_SA и должно быть равно "0". Значение SPI следует получать из внешнего заголовка и при последующих согласованиях поле "Значение SPI" должно показывать размер SPI (в октетах) для соответствующего протокола (8 для IKEv2, 4 для ESP и AH);

поле "Число преобразований" (1 октет) должно содержать информацию о числе преобразований в предложении;

поле "SPI передающей стороны" должно быть переменного размера;

поле "Структура преобразования" должно быть переменного размера.

Формат поля "Структура преобразования" приведен на рисунке 4.

0 или 3	Резерв	Длина преобразования
Тип преобразования	Резерв	Идентификатор преобразования
Атрибуты преобразования		

Рисунок 4

Примечание:

первый октет должен должен содержать информацию о том, является ли преобразование последним в предложении. Преобразование должно быть последним при значении первого октета равном "0" и не должно являться последним при значении равном "3";

поле "Резерв" (1 октет) должно быть равно "0" при передаче и игнорироваться на приеме;

поле "Длина преобразования" (2 октета) должно содержать информацию о размере поля "Структура преобразования" (в октетах) с учетом заголовка и атрибутов;

поле "Тип преобразования" (1 октет) должно содержать тип преобразования, задаваемого этим элементом. Преобразование не должно включаться в предложение, если оно является необязательным и инициатор предлагает его пропустить. Инициатор должен включать

субструктуру преобразования с идентификатором Transform ID равном "0" в качестве одной из опций при передаче вопроса об использовании необязательного преобразования ответчику.

Типы преобразований приведены в таблице N 3.

Таблица N 3.

Название преобразования	Тип преобразования	Используемый протокол
Резерв	0	
Encryption Algorithm (ENCR) - алгоритм шифрования	1	IKE и ESP
Pseudo-random Function (PRF) - псевдослучайная функция	2	IKE
Integrity Algorithm (INTEG) - алгоритм защиты целостности	3	IKE, AH, опционально в ESP
Diffie-Hellman Group (D-H) - группа Diffie-Hellman	4	IKE, опционально в AH и ESP
Extended Sequence Numbers (ESN) - расширенные порядковые номера	5	AH и ESP
Резерв IANA	6 - 240	
Частное применение	241 - 255	

Примечание:

поле "Идентификатор преобразования" (2 октета) должно содержать идентификатор конкретного преобразования указанного типа.

Число и тип преобразований в элементах данных SA должны зависеть от типа протокола в самой SA.

Обязательные и опциональные типы преобразований приведены в таблице N 4.

Таблица N 4.

Протокол	Обязательные типы	Опциональные типы
IKE	ENCR, PRF, INTEG, D-H	
ESP	ENCR, ESN	INTEG, D-H
AH	INTEG, ESN	D-H

Примечание:

поле "Атрибуты преобразования" должно содержать атрибуты, представляющие собой пары "тип-значение" для каждого преобразования элемента данных SA, приведенные в таблице N 5.

Таблица N 5.

Тип атрибута	Значение атрибута	Формат атрибута
Резерв	0 - 13	
Размер ключа шифрования переменного размера (Key Length) (в битах)	14	тип/значение
Резерв	15 - 17	
Резерв IANA	18 - 16383	
Для частного применения	16384 - 32767	

Примечание:

Значение атрибута должно иметь фиксированную (2 октета) или переменную длину. Для представления атрибута переменной длины должен использоваться формат "тип-размер-значение".

Формат поля "Атрибута преобразования" приведен на рисунке 5.

Тип атрибута	Длина атрибута (значение)
Значение атрибута	

Рисунок 5

Примечание:

поле "Тип атрибута" (2 октета) должно содержать идентификатор атрибута. Для атрибута должен использоваться полный формат атрибута (тип/размер/значение) при установлении старшего бита поля "Тип атрибута" - флага формата атрибута (AF), равного "0" или сокращенный формат атрибута (тип/значение) при AF равном "1";

поле "Длина атрибута (значение)" (2 октета) должно содержать информацию о размере атрибута, содержащийся в поле "Значение атрибута" (переменная длина), при AF равном "0" или содержать значение атрибута при AF равном "1";

2.5. формат элемента данных Обмен ключами (Key Exchange, далее - KE) приведен на рисунке 6.

Номер группы DH	Резерв

Данные обмена ключами

Рисунок 6

Элемент данных KE должен использоваться для обмена открытыми номерами протокола Дúффи-Хéллмана (Diffie-Hellman, далее - DH) при обмене ключами DH.

Элемент данных KE должен создаваться путем копирования открытого значения DH в поле "Данные обмена ключами". Размер открытого значения DH должен быть равен размеру первичного модуля, для которого выполняется возведение в степень, дополненного при необходимости нулями в начале.

Поле "Номер группы DH" (2 байта) должно идентифицировать группу DH, в которой было рассчитано значение поля "Данные обмена ключами". Сообщение должно игнорироваться с возвратом элемента "Уведомление типа INVALID_KE_PAYLOAD" при выборе предложения, использующего другую группу DH;

2.6. формат элементов Идентификатор инициатора (IDi) и Идентификатор отвечающего (IDr) приведен на рисунке 7.

Тип идентификации	Резерв
Данные идентификатора	

Рисунок 7

Примечание:

поле "Тип идентификации" (1 байт) должен задавать тип используемых идентификаторов;

поле "Данные идентификатора" (переменной длины) должно содержать идентификатор, тип которого указан в предыдущем поле;

2.7. формат элемента данных Сертификат приведен на рисунке 8.

Тип сертификата	Данные сертификата

Рисунок 8

Примечание:

поле "Тип сертификата" (1 октет) должно содержать информацию о способе кодирования сертификата;

поле "Данные сертификата" должно иметь переменный размер.

Элемент данных Сертификат должен обеспечивать способ передачи сертификатов или другой, связанной с идентификацией информации через IKE. Элемент данных Сертификат следует включать в обмен, если сертификат доступен отправителю до указания партнером возможности

получения идентификационной информации иным путем с использованием элемента Уведомление типа HTTP_CERT_LOOKUP_SUPPORTED. Требования к

Значения поля "Тип сертификата" приведены в таблице N 6.

Таблица N 6.

Способ кодирования сертификата	Значение Формат атрибута
Резерв	0
Сертификат X.509 с PKCS (Public Key CryptographyStandard - криптографический стандарт открытого ключа)) N 7	1
Сертификат PGP (Pretty Good Privacy)	2
Подписанный ключ DNS (Domain Name System)	3
Сертификат X.509 - подпись	4
Маркер Kerberos	6
Список отозванных сертификатов CRL (Certificate Revocation List)	7
ARL	8
Сертификат простой инфраструктуры открытых ключей SPKI (Simple Public Key Infrastructure) I	9
Сертификат X.509 - атрибут	10
Неразобранный ключ криптографического алгоритма с открытым ключом RSA	11
Хеш и URL сертификата X.509	12
Хеш и URL связки (bundle) X.509	13
Резерв IANA	14 - 200
Для частного применения	201 - 255

2.8. формат элемента данных Запрос сертификата приведен на рисунке 9.

Тип сертификата	Удостоверяющий центр

Рисунок 9

Примечание:

поле "Тип сертификата" (1 октет) должно содержать информацию о способе кодирования сертификата;

поле "Удостоверяющий центр" должно иметь переменный размер.

2.9. элемент данных Идентификация должен содержать данные, используемые для идентификации.

Формат элемента данных Идентификация приведен на рисунке 10.

Метод идентификации	Резерв
Идентификационные данные	

Рисунок 10

Примечание:

поле "Метод идентификации" (1 октет) должно содержать информацию о используемом методе идентификации и принимать значения:

RSA цифровая подпись (1) (должно рассчитываться с использованием приватного ключа RSA и хэш-значения PKCS N 1 с заполнением);

Shared Key Message Integrity Code (2) (должно рассчитываться с использованием разделяемого ключа, связанного с объектом из элемента Тип идентификации и согласованной функции prf);

DSS (Digital Signature Standard) цифровая подпись (3) (должно рассчитываться с использованием закрытого ключа DSS и хэш-значения алгоритма криптографического хеширования SHA-1 (Secure Hash Algorithm);

Значение 0 и 4 - 200 должны быть зарезервированы IANA, 201 - 255 должны быть выделены для частных приложений;

поле "Идентификационные данные" должно иметь переменный размер;

2.10. элемент данных Случайное число должно иметь одно поле переменного размера, содержащее созданное передающей стороной случайное значение, размер элемента должен находиться в диапазоне (16 - 256) октетов включительно, повторное использование значения Случайного числа не допускается;

3. элемент данных Уведомление должен использоваться для передачи служебной информации.

Формат элемента данных Уведомление приведен на рисунке 11.

Идентификатор протокола	Размер SPI	Тип уведомления

SPI
Данные уведомления

Рисунок 11

Примечание:

поле "Идентификатор протокола" (1 октет) должно показывать тип SA, если уведомление относится к существующей SA, должно быть равно "1" для уведомлений IKE_SA, "2" для протокола AH или "3" для протокола ESP для уведомлений, касающихся IPsec, и "0" при передаче и игнорироваться на приеме для уведомлений, не относящихся к существующим SA. Все остальные значения должны быть зарезервированы IANA для использования в будущем.

поле "Размер SPI" (Security Parameter Index) (1 октет) должно указывать размер SPI в октетах;

поле "Тип уведомления" (2 октета) должен задавать тип уведомления;

поле "SPI" должно иметь переменный размер и содержать идентификатор параметров защиты;

поле "Данные уведомления" должно иметь переменный размер и содержать дополнительную информацию к типу уведомления;

3.1. формат элемента данных Удаление приведен на рисунке 12.

Элемент данных Удаление должен содержать определяемый протоколом идентификатор защищенной связи.

Идентификатор протокола	Размер SPI	Количество SPI
Индекс параметров безопасности (SPI)		

Рисунок 12

Примечание:

поле "Идентификатор протокола" (1 октет) должно быть равно "1" для IKE_SA, з "2" - для AH, "3" - для ESP;

поле "Размер SPI" (1 октет) должно содержать размер SPI указанного протокола (в октетах);

поле "Количество SPI" (2 октета) должно содержать количество SPI в элементе данных Удаление;

поле "Индекс параметров безопасности" (SPI) должно иметь переменный размер и идентифицировать удаляемое защищенное соединение;

3.2. элемент данных Идентификатор реализации должен иметь одно поле переменного

размера, содержащее уникальный идентификатор производителя;

3.3. элементы данных Селектор трафика - Инициатор, Селектор трафика - Ответчик.

Формат элемента Селектор трафика приведен на рисунке 13.

Количество селекторов трафика	Резерв
Селектор(ы) трафика	

Рисунок 13

Примечание:

поле "Количество селекторов трафика" должно иметь размер 1 октет;

поле "Резерв" (3 октета) должно быть равно "0" при передаче и игнорироваться на приеме;

поле "Селектор трафика" должно иметь переменный размер и содержать один или несколько отдельных указателей типа трафика;

3.4. элемент данных Кодирование (Encrypted - далее E), должен содержать другие элементы в зашифрованном виде. При наличии в сообщении элемента Кодирование он должен быть последним в сообщении.

Формат элемента данных Кодирование приведен на рисунке 14.

Initialization Vector	
Данные IKE	
Padding (0 - 255) октетов	Pad Length
Integrity Checksum Data	

Рисунок 14

Примечание:

поле "Initialization Vecto" должно содержать случайное значение, совпадающее с размером блока используемого алгоритма шифрования. Получатели должны воспринимать любые значения этого поля, а отправителям следует генерировать псевдослучайное значение независимо для каждого сообщения или использовать для выбора значений шифрованный блок предыдущего сообщения;

поле "Данные IKE" должно быть переменной длины, содержать шифрованные элементы IKE и шифроваться с использованием согласованного алгоритма;

поле "Padding" может содержать любое значение, выбранное отправителем, должно иметь размер, который делает суммарный размер шифрованных элементов, поля "Padding" и поля "Pad Length" кратным размеру блока шифрования "Initialization Vecto" и шифроваться с

использованием согласованного алгоритма;

поле "Pad Length" (1 октет) должно содержать информацию о размере поля Padding и шифроваться с использованием согласованного алгоритма. Отправителю следует устанавливать в поле "Pad Length" минимальное значение, которое делает размер полей шифрованных элементов "Padding" и "Pad Length" кратными размеру блока шифрования. Получатель должен принимать любые значения, обеспечивающие требуемое выравнивание. Это поле шифруется с использованием согласованного алгоритма;

поле "Integrity Checksum Data" должно содержать криптографическую контрольную сумму всего сообщения, начиная с фиксированного заголовка IKE и заканчивая полем "Pad Length". Контрольная сумма должна рассчитываться для зашифрованного сообщения. Размер поля должен определяться согласованным алгоритмом защиты целостности;

3.5. элемент данных Конфигурация (CP) должен использоваться для обмена конфигурационными параметрами между партнерами IKE.

Требования к формату элемента данных Конфигурация приведены на рисунке 15.

Тип обмена	Резерв
Атрибуты конфигурации	

Рисунок 15

Элемент данных Конфигурация должен включать базовый заголовок IKE и следующие поля:

поле "Тип обмена" (1 октет) должно содержать информацию о типе обмена данными Конфигурации (REQUEST-1, REPLY-2, SET-3, ACK-4);

поле "Резерв" (3 октета) должно быть равно "0" при передаче и игнорироваться на приеме;

поле "Атрибуты конфигурации" должно иметь переменный размер и содержать атрибуты конфигурации в формате "тип-размер-значение".

Элемент данных Конфигурация может содержать несколько атрибутов или не содержит атрибуты;

3.6. элемент данных Расширяемая идентификация (EAP) должен позволять выполнять идентификацию IKE_SA с использованием протокола EAP. Формат элемента данных EAP приведен на рисунке 16.

Код	Идентификатор	Длина
Тип	Данные	

Рисунок 16

Примечание:

поле "Код" (1 октет) должно показывать тип сообщение и должно быть равно "1" при запросе (Request), "2" при отклике (Response), "3" при успешном завершении (Success) или "4" при отказе (Failure);

поле "Идентификатор" (1 октет) должно использоваться в протоколе PPP, чтобы отличить повторное использование сообщений от повторной передачи. В откликах поле "Идентификатор" должно быть равно значению идентификатора в соответствующем запросе, а в остальных сообщениях может принимать любое значение;

поле "Длина" (2 октета) должно содержать информацию о размере сообщения EAP и быть в 4 раза меньше значения поля "Размер текущего элемента (Payload Lenqth) базового заголовка";

поле "Тип" (1 октет) должно быть только в сообщениях с кодом Request (1) или Response (2). Для других кодов размер сообщения EAP должно составлять четыре октета, а поля "Тип" и "Данные" должны отсутствовать. В запросах (1) поле "Тип" должно указывать запрашиваемые данные, а в откликах (2) поле "Тип" должно быть пустым или соответствовать типу запрошенных данных.

Значения поля "Тип":

1 - тождественность;

2 - уведомление;

3 - только отклики;

4 - MD5 - вызов;

5 - однократный пароль;

6 - маркерная карта базового типа.

Поле "Данные" должно быть переменного размера и зависеть от типа запроса и связанного с ним отклика.

Приложение N 20
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ТРЕБОВАНИЯ К ПРОТОКОЛУ IPSEC

1. Требования к идентификационному заголовку АН:

1.1. идентификационный заголовок протокола IPSec (АН) должен использоваться для обеспечения целостности дейтаграмм IP и идентификации источника данных без организации специальных соединений и защиты против повторного использования пакетов. АН может использоваться в комбинации с ESP или путем вложения. Услуги по защите могут обеспечиваться между парой взаимодействующих элементов сети IP.

1.2. формат заголовка идентификации АН приведены на рисунке 1.

Следующий заголовок	Длина заголовка	Резерв
Идентификатор параметров защиты (SPI)		
Порядковый номер		
Аутентификационные данные (Значение контрольной суммы (ICV)) (перемен.)		

Рисунок 1

Примечание:

поле "Следующий заголовок" (1 октет) должно показывать тип информации, расположенной после идентификационного заголовка АН. Значения этого поля должны выбираться из списка номеров протоколов, предоставленного Администрацией адресного пространства Интернет IANA;

поле "Длина заголовка" (1 октет) должно содержать информацию о размере заголовка АН в 32-битовых словах (4-байтовых блоках) минус 2;

поле "Резерв" (2 октета) должно быть резервным, равно "0" и игнорируется получателем. Значение этого поля должно учитываться при вычислении ICV, но игнорироваться получателем;

поле "Идентификатор параметров защиты" (SPI) должно быть произвольным 32-битовым значением, используемым получателем для идентификации SA, с которой связан входящий пакет. Для индивидуальных SA значение SPI может идентифицировать SA или использоваться в комбинации с типом протокола IPsec (в данном случае АН). Поле SPI должно быть обязательным и механизм отображения входящего трафика на индивидуальные SA должен поддерживаться всеми реализациями АН;

поле "Порядковый номер" (4 октета) должно содержать значение счетчика пакетов, увеличиваемое на "1" для каждого переданного пакета (счетчик пакетов для SA). Это поле должно быть обязательным и присутствовать даже в случае, когда получатель не пользуется услугами по предотвращению повторного использования пакетов для конкретной SA. Отправитель должен передавать указанное поле, но получатель не обязан принимать его во внимание. Счетчики на стороне отправителя и получателя должны инициализироваться при значении поля "Порядковый номер" равном "0" при создании SA (первый пакет, переданный с использованием данной SA, будет иметь порядковый номер - "1"). Если предотвращение повторного использования пакетов включено (используется по умолчанию), передаваемые порядковые номера никогда не должны повторяться. Расширенный порядковый номер должен позволять использовать для SA 64-битовые порядковые номера. В заголовке АН каждого пакета должны передаваться только младшие 32

бита расширенного порядкового номера, а старшие 32 бита должны учитываться как часть порядкового номера отправителем и получателем и включаться в расчет ICV, но не должны передаваться;

поле "Аутентификационные данные" должно содержать значение контрольной суммы ICV для данного пакета. Размер поля должен быть кратным 32 битам как для IPv4, так и для IPv6. Указанное поле может включать заполнение для обеспечения кратности размера заголовка AH в целом 32 (IPv4) или 64 (IPv6) битам. Заполнение должны поддерживать все реализации и размер заполнения должен быть минимально достаточным для выравнивания заголовков в соответствии с требованиями IPv4/IPv6;

1.3. местонахождение заголовка AH:

AH должно обеспечивать работу в двух режимах: транспортном и туннельном:

а) в транспортном режиме AH должен помещаться между заголовком протокола IP и заголовком протокола транспортного уровня или перед другими заголовками IPsec при наличии. Требования к местонахождению заголовка AH в транспортном режиме приведены на рисунке 2.

Заголовок исходного IP пакета	Заголовок AH	Заголовок TCP (UDP)	Данные

Рисунок 2

При использовании IPv4 AH должен размещаться после заголовка IP (после всех опций заголовка IP), но перед заголовком протокола следующего уровня. При использовании IPv6 заголовок AH должен размещаться после заголовков IP и расширения. В расширенном заголовке необходимо обеспечить расположение опций получателя перед заголовком AH, после него или по обе стороны;

б) в туннельном режиме заголовок AH должен защищать исходный IP пакет целиком (включая его заголовок).

Требования к местонахождению заголовка AH в туннельном режиме приведены на рисунке 3;

Заголовок внешнего IP пакета	Заголовок AH	Заголовок исходного IP пакета	Заголовок TCP (UDP)	Данные

Рисунок 3

2. Требования к протоколу ESP:

2.1. протокол ESP (IP Encapsulating Security Payload) должен использоваться для обеспечения целостности и конфиденциальности данных путем их шифрования. В зависимости от пользовательских требований к безопасности этот механизм следует применять для шифрования пакетов транспортного уровня (например, TCP, UDP, ICMP, IGMP) или дейтаграмм IP полностью.

В протоколе ESP должно быть обеспечено одновременное или раздельное использование функций аутентификации и криптографической защиты вместе;

2.2. Должна обеспечиваться возможность содержания ESP в любом месте между заголовком IP и конечным протоколом транспортного уровня. Для протокола ESP должен использоваться идентификатор IANA 50. Заголовок, расположенный непосредственно перед заголовком ESP, должен всегда содержать значение равное "50" в поле "Следующий заголовок" для IPv6 или "Протокол" для IPv4. ESP должен состоять из нешифрованного заголовка, за которым должны следовать зашифрованные данные. Шифруемые данные должны включать в себя защищенные поля заголовка ESP и защищаемые пользовательские данные: дейтаграмму IP или пакет протокола вышележащего уровня.

Формат заголовка ESP приведен на рисунке 4.

<table>
<tr><td colspan="3">Идентификатор параметров защиты (SPI)</td></tr>
<tr><td colspan="3">Порядковый номер</td></tr>
<tr><td colspan="3">Данные (перемен.)</td></tr>
<tr><td colspan="2">Данные (перемен.)</td><td>Заполнитель</td></tr>
<tr><td>Заполнитель</td><td>Длина заполнителя</td><td>Следующий заголовок</td></tr>
<tr><td colspan="3">Аутентификационные данные (перемен.)</td></tr>
</table>

Рисунок 4

2.3. местонахождение заголовка ESP:

Должна обеспепечиваться возможность работы ESP в транспортном и туннельном режимах.

а) в транспортном режиме зашифрованные данные должны транспортироваться между хостами, заголовок исходного IP-пакета должен оставаться внешним, а Заголовок ESP должен помещаться в передаваемый пакет между заголовками протоколов третьего и четвертого уровней.

Шифроваться должны только данные исходного IP-пакета и заключительная часть ESP заголовка. В этом режиме ESP не должен шифровать заголовок IP-пакета, поля "SPI" и "Порядковый номер".

б) Функции туннельного режима должны реализовываться в шлюзах безопасности.

В туннельном режиме в качестве внешнего заголовка должен создаваться новый заголовок IP, ESP заголовок должен помещаться перед заголовком исходного IP-пакета, а весь исходный IP-пакет и заключительная часть заголовка ESP должны шифроваться. Заголовок внешнего IP-пакета не должен защищаться протоколом ESP.

Приложение N 21
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ПЕРЕЧЕНЬ
СООБЩЕНИЙ ПРОТОКОЛА DIAMETER ПРИ РЕАЛИЗАЦИИ ИНТЕРФЕЙСОВ S6B, SWX, SWM, STA, SWD, SWA

Таблица N 1. Сообщения протокола Diameter на интерфейсе S6b, определенные идентификатором приложения (далее - Auth-Application-Id), равным "16777272"

Сообщение	Код сообщения	Направление передачи
Diameter-EAP-Request (DER)	268, бит R в поле команды "Флаг" установлен в "1"	от P-GW к 3GPP AAA серверу
Diameter-EAP-Answer (DEA)	268, бит R в поле команды "Флаг" очищен	от 3GPP AAA сервера к P-GW
Информация о сессии. Запрос (AA-Request (AAR))	265, бит R в поле команды "Флаг" установлен в "1"	от P-GW к 3GPP AAA серверу
Информация о сессии. Ответ (AA-Answer (AAA))	265, бит R в поле команды "Флаг" очищен	от 3GPP AAA сервера к P-GW
Окончание сессии. Запрос (Session-Termination-Request (STR))	275, бит R в поле команды "Флаг" установлен в "1"	от P-GW к 3GPP AAA серверу или от 3GPP AAA сервера к P-GW
Окончание сессии. Ответ (Session-Termination-Answer (STA))	275, бит R в поле команды "Флаг" очищен	от 3GPP AAA сервера к P-GW или от P-GW к 3GPP AAA серверу
Аварийное прекращение сессии. Запрос (Abort-Session-Request (ASR))	274, бит R в поле команды "Флаг" установлен в "1"	от 3GPP AAA сервера к P-GW

Аварийное прекращение сессии. Ответ (Abort-Session-Answer (ASA))	274, бит R в поле команды "Флаг" очищен	от P-GW к 3GPP AAA серверу
Обновление данных авторизации. Запрос (Re-Auth-Request (RAR))	258, бит R в поле команды "Флаг" установлен в "1"	от 3GPP AAA сервера/прокси к P-GW
Обновление данных авторизации. Ответ (Re-Auth-Answer (RAA))	258, бит R в поле команды "Флаг" очищен	от P-GW к 3GPP AAA серверу/прокси

Таблица N 2. Сообщения протокола Diameter на интерфейсе SWx, определенные Auth-Application-Id, равным "16777265"

Сообщение	Код сообщения	Направление передачи
Аутентификация при мультимедийной сессии. Запрос. (Multimedia-Authentication-Request (MAR))	303, бит R в поле команды "Флаг" установлен в "1"	от 3GPP AAA сервера к HSS
Аутентификация при мультимедийной сессии. Ответ (Multimedia-Authentication-Answer (MAA))	303, бит R в поле команды "Флаг" очищен	от HSS к 3GPP AAA серверу
Обновление профилей. Запрос. (Push-Profile-Request (PPR))	305, бит R в поле команды "Флаг" установлен в "1"	от HSS к 3GPP AAA серверу
Обновление профилей. Ответ. (Push-Profile-Answer (PPA))	305, бит R в поле команды "Флаг" очищен	от 3GPP AAA сервера к HSS
Регистрация сервера сервера. Запрос. (Server-Assignment-Request (SAR))	301, бит R в поле команды "Флаг" установлен в "1"	от 3GPP AAA сервера к HSS
Регистрация сервера. Ответ. (Server-Assignment-Answer (SAA))	301, бит R в поле команды "Флаг" очищен	от HSS к 3GPP AAA серверу
Окончание регистрации. Запрос. (Registration-Termination-Request (RTR)	304, бит R в поле команды "Флаг" установлен в "1"	от HSS к 3GPP AAA серверу или от 3GPP AAA сервера к HSS
Окончание регистрации. Ответ (Registration-Termination-Answer (RTA))	304, бит R в поле команды "Флаг" очищен	от 3GPP AAA сервера к HSS или от HSS к 3GPP AAA серверу

Таблица N 3. Сообщения протокола Diameter на интерфейсе SWm, определенные Auth-Application-Id, равным "16777264"

Сообщение	Код сообщения	Направление передачи
Diameter-EAP-Request (DER)	268, бит R в поле команды "Флаг" установлен в "1"	от ePDG к 3GPP AAA серверу/прокси
Diameter-EAP-Answer (DEA)	268, бит R в поле команды "Флаг" очищен	от 3GPP AAA сервера/прокси к ePDG
Информация о сессии. Запрос (AA-Request (AAR))	265, бит R в поле команды "Флаг" установлен в "1"	от ePDG к 3GPP AAA серверу/прокси
Информация о сессии. Ответ (AA-Answer (AAA))	265, бит R в поле команды "Флаг" очищен	от 3GPP AAA сервера/прокси к ePDG
Окончание сессии. Запрос (Session-Termination-Request (STR))	275, бит R в поле команды "Флаг" установлен в "1"	от ePDG к 3GPP AAA серверу/прокси
Окончание сессии. Ответ (Session-Termination-Answer (STA))	275, бит R в поле команды "Флаг" очищен	от 3GPP AAA сервера/прокси к ePDG
Аварийное прекращение сессии. Запрос (Abort-Session-Request (ASR))	274, бит R в поле команды "Флаг" установлен в "1"	от 3GPP AAA сервера/прокси к ePDG
Аварийное прекращение сессии. Ответ (Abort-Session-Answer (ASA))	274, бит R в поле команды "Флаг" очищен	от ePDG к 3GPP AAA серверу/прокси
Обновление данных авторизации. Запрос (Re-Auth-Request (RAR))	258, бит R в поле команды "Флаг" установлен в "1"	от 3GPP AAA сервера/прокси к ePDG
Обновление данных авторизации. Ответ (Re-Auth-Answer (RAA))	258, бит R в поле команды "Флаг" очищен	от ePDG к 3GPP AAA серверу/прокси

Таблица N 4. Сообщения протокола Diameter на интерфейсе STa, определенные Auth-Application-Id, равным "16777250"

Сообщение	Код сообщения	Направление передачи
Diameter-EAP-Request (DER)	268, бит R в поле команды "Флаг" установлен в "1"	от TWAN к 3GPP AAA серверу

Diameter-EAP-Answer (DEA)	268, бит R в поле команды "Флаг" очищен	от 3GPP AAA сервера к TWAN
Аварийное прекращение сессии. Запрос (Abort-Session-Request (ASR))	274, бит R в поле команды "Флаг" установлен в "1"	от 3GPP AAA сервера/прокси к TWAN
Аварийное прекращение сессии. Ответ (Abort-Session-Answer (ASA))	274, бит R в поле команды "Флаг" очищен	от TWAN к 3GPP AAA серверу/прокси
Окончание сессии. Запрос (Session-Termination-Request (STR))	275, бит R в поле команды "Флаг" установлен в "1"	от TWAN к 3GPP AAA серверу/прокси
Окончание сессии. Ответ (Session-Termination-Answer (STA))	275, бит R в поле команды "Флаг" очищен	от 3GPP AAA сервера/прокси к TWAN
Обновление данных авторизации. Запрос (Re-Auth-Request (RAR))	258, бит R в поле команды "Флаг" установлен в "1"	от 3GPP AAA сервера/прокси к TWAN
Обновление данных авторизации. Ответ (Re-Auth-Answer (RAA))	258, бит R в поле команды "Флаг" очищен	от TWAN к 3GPP AAA серверу/прокси
Информация о сессии. Запрос (AA-Request (AAR))	265, бит R в поле команды "Флаг" установлен в "1"	от TWAN к 3GPP AAA серверу/прокси
Информация о сессии. Ответ (AA-Answer (AAA))	265, бит R в поле команды "Флаг" очищен	от 3GPP AAA сервера/прокси к TWAN

Таблица N 5. Сообщения протокола Diameter на интерфейсе SWa, определенные Auth-Application-Id, равным "16777250"

Сообщение	Код сообщения	Направление передачи
Diameter-EAP-Request (DER)	268, бит R в поле команды "Флаг" установлен в "1"	от UTWAN к 3GPP AAA серверу
Diameter-EAP-Answer (DEA)	268, бит R в поле команды "Флаг" очищен	от 3GPP AAA сервера к UTWAN
Аварийное прекращение сессии. Запрос (Abort-Session-Request (ASR))	274, бит R в поле команды "Флаг"	от 3GPP AAA сервера/прокси к

	установлен в "1"	UTWAN
Аварийное прекращение сессии. Ответ (Abort-Session-Answer (ASA))	274, бит R в поле команды "Флаг" очищен	от UTWAN к 3GPP AAA серверу/прокси
Окончание сессии. Запрос (Session-Termination-Request (STR))	275, бит R в поле команды "Флаг" установлен в "1"	от UTWAN к 3GPP AAA серверу/прокси
Окончание сессии. Ответ (Session-Termination-Answer (STA))	275, бит R в поле команды "Флаг" очищен	от 3GPP AAA сервера/прокси к UTWAN
Обновление данных авторизации. Запрос (Re-Auth-Request (RAR))	258, бит R в поле команды "Флаг" установлен в "1"	от 3GPP AAA сервера/прокси к UTWAN
Обновление данных авторизации. Ответ (Re-Auth-Answer (RAA))	258, бит R в поле команды "Флаг" очищен	от UTWAN к 3GPP AAA серверу/прокси
Информация о сессии. Запрос (AA-Request (AAR))	265, бит R в поле команды "Флаг" установлен в "1"	от UTWAN к 3GPP AAA серверу/прокси
Информация о сессии. Ответ (AA-Answer (AAA))	265, бит R в поле команды "Флаг" очищен	от 3GPP AAA сервера/прокси к UTWAN
Обновление данных авторизации. Ответ (Re-Auth-Answer (RAA))	258, бит R в поле команды "Флаг" очищен	от UTWAN к 3GPP AAA серверу/прокси

На интерфейсе SWd должны транслироваться сообщения протокола Diameter с интерфейсов S6b, SWm, STa, приведенные в таблицах N N 1, 3, 4 соответственно.

Приложение N 22
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации

от 25.06.2018 N 319

ПЕРЕЧЕНЬ
ДАННЫХ, ХРАНЯЩИХСЯ В HSS, MME, S-GW, P-GW, EPDG, 3GPP AAA СЕРВЕРЕ, 3GPP AAA ПРОКСИ-СЕРВЕРЕ, ПРИ РЕАЛИЗАЦИИ NON-3GPP ДОСТУПА

Таблица.

Параметр	HSS	MME	S-GW	P-GW	ePDG	3GPP AAA сервер	3GPP AAA прокси-сервер	Тип пар.
Международный идентификатор MS (IMSI)	О	У	У	У	У			П
Международный номер MS в сети ISDN (MSISDN)	У	У	У	У	У	У		П
Параметры для аутентификации в сети UMTS (RAND, XRES, CK, IK, AUTN)	О					О		В
Параметры для аутентификации в сети LTE (RAND, XRES, KASME, AUTN)	О					О		В
Режим доступа к сети (Network Access Mode)	У					У		В
Подробное описание трейса 2 (Trace Reference 2)	У			У		У		П
Уровень глубины трейса (Trace depth)	У			У		У		П
Список сетевых элементов, в которых проводится сбор трейсов (List of NE types to trace)	У					У		П
Параметры, указываемые в трейсах (Triggering events)	У			У		У		П
Перечень интерфейсов сетевых элементов для которых формируются трейсы (List of interfaces to trace)	У			У		У		П

IP-адреса для которых формируются трейсы (IP address of Trace Collection Entity)	У			У		У		П
Профили имен точек доступа (APN-Configuration-Profile)	О			У	У	У		В
Указанная в подписке общая максимальная скорость передачи для точки доступа (Subscribed APN-AMBR)	О			У	У	У		П
Используемая максимальная скорость передачи для точки доступа (Used APN-AMBR)				У				В
Адрес сети передачи данных (PDN Address)	У		У	У	У	У		П/В
Разрешенный адрес визитной сети радиотелефонной связи (VPLMN Address Allowed)	О	У			У	У		П
Идентификатор PDN GW (PDN GW identity)	О	У			У	У		П
Используемая точка доступа (APN in Use)				У	У			В
Идентификатор EPS (EPS Bearer ID)				У	У			В
Качество обслуживания EPS (EPS Bearer QoS)				У	У			В
Характеристики учета стоимости соединения EPS PDN (EPS PDN Connection Charging Characteristics)	У			У	У	У		П
Тип технологии радиодоступа (RAT type)	У		У	У	У	У		В
Постоянный идентификатор пользователя (Permanent user identity)	О		О	О	О	О		П
Возможности мобильности при доступе не 3GPP (Mobility Capabilities)				О	У	У		В

IP-адрес шлюза MAG (MAG IP address)						У		В
Идентификатор визитной сети (Visited Network Identifier)	У			У	У	У		В
Данные для аутентификации EAP (EAP payload)						У		В
Данные об используемом протоколе мобильности (MIP Subscriber profile)	О			О				П
Ключ GRE для восходящего направления интерфейса S5 (Uplink S5 GRE Key)		У	У	У				В
Ключ GRE для нисходящего направления интерфейса S5 (Downlink S5 GRE Key)			У	У				В
Ключ GRE для восходящего направления интерфейса S8 (Uplink S8 GRE Key)		У	У	У				В
Ключ GRE для нисходящего направления интерфейса S8 (Downlink S8 GRE Key)			У	У				В
Ключи GRE интерфейса S2a (S2a GRE Keys)			У	У	У			В
Ключи GRE интерфейса S2b (S2b GRE Keys)			У	У	У			В
Идентификатор мобильного узла (Mobile Node Identifier)			У	У				В
Адрес маршрутизатора по умолчанию формата IPv4 (IPv4 Default Router Address)			У	У				В
Локальный адрес линка (Link-local address)			У	У				В
Данные пользователя не 3GPP (Non 3GPP User Data)	У				У	У		В
Идентификатор 3GPP AAA Сервера (3GPP AAA Server Identity)	У			У	У			В

Выбор режима поддержки мобильности (Selected IP mobility mode)				У	У	У		В
Идентификатор сервера Diameter для HSS (Diameter Server Identity of HSS)		У				У		В
Неаутентифицированный IMSI (Unauthenticated IMSI)			У	У				В
Идентификатор соединения PDN (PDN Connection ID)			У	У	У			В
Идентификатор конечной точки туннеля ePDG F для S2b (плоскость управления) (ePDG F-TEID for S2b (control plane))				У	У			В
Идентификатор конечной точки туннеля ePDG F для S2b (плоскость пользователя) ePDG F-TEID for S2b (user plane)				У	У			В
Идентификатор конечной точки туннеля PGW F для S2b (плоскость управления) (PGW F-TEID for S2b (control plane))				У	У			В
Идентификатор конечной точки туннеля PGW F для S2b (плоскость пользователя) (PGW F-TEID for S2b (user plane))				У	У			В
Параметры тарификации пользователя (Subscribed Charging Characteristics)	О				У	У		П
Мастер ключ сессии (Master session Key)				У	У	У		В
Примечание: В - временные данные, О - обязательные данные, У - данные по условию, П - постоянные данные.								

Приложение N 23
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ТРЕБОВАНИЯ К ПРОТОКОЛАМ EAP-AKA, EAP-AKA'

1. Протокол EAP-AKA должен быть расширяемым протоколом аутентификации для аутентификации и согласования ключей пользователей UMTS при помощи универсального модуля идентификации абонента (USIM).

Протокол EAP-AKA' должен применяться для доступа к оборудованию коммутации стандартов GSM 900/1800, UMTS, LTE с использованием TWAN или UTWAN доступа.

Протоколы EAP-AKA и EAP-AKA' должны пользоваться услугами протоколов канального уровня.

2. Требования к протоколу EAP-AKA:

2.1. формат пакетов EAP приведены на рисунке 1.

Код	Идентификатор	Длина
Данные		

Рисунок 1

Примечание:

поле "Код" (1 октет) должен содержать информацию о типе пакета EAP и принимать значения:

1 - запрос (Request);

2 - ответ (Response);

3 - подтверждение (Success);

4 - отказ (Failure).

Пакеты EAP с другими значениями кода должны отбрасываться обеими сторонами без уведомления;

поле "Идентификатор" (1 октет) должно обеспечивать соответствие запросов и ответов на

них;

поле "Длина" (2 октета) должно содержать размер (в октетах) пакета EAP с учетом полей "Код", "Идентификатор", "Длина" и "Данные". Октеты, выходящие за пределы указанного размера, следует считать заполнением канального уровня, на приеме такие данные следует игнорировать. Сообщения со значением поля "Длина", превышающем размер полученного пакета, должны отбрасываться без уведомления;

поле "Данные" должно иметь размер 0 или более октетов. Формат поля должен зависеть от типа пакета (значения поля "Код");

2.2. формат пакетов EAP Request и Response, используемых для аутентификации и согласования ключей с помощью USIM (далее - AKA), приведен на рисунке 2.

Код	Идентификатор	Длина
Тип (23)	Подтип	Резерв
Тип атрибута	Длина атрибута	Значение (2 и более байтов)

Рисунок 2

Примечание:

для пакетов Request и Response поле "Данные" должно начинаться с поля "Тип" (1 октет) и содержать тип запрашиваемой информации. Пакеты Request должны передаваться, пока не будет получен корректный отклик, не завершится отсчет числа попыток или нижележащий уровень не сообщит об отказе. Поле "Идентификатор" должно сохранять значение для повторных запросов, чтобы их можно было отличить от новых запросов. Содержимое поля "Данные" должно зависеть от "Типа" запроса. Пакеты Response должны передаваться в ответ на корректный запрос;

поле "Тип" для пакетов EAP-AKA должно быть равно "23";

поле "Данные" должно включать поле "Подтип" (1 октет) и поле "Резерв" (2 октета). Поле "Подтип" должно указывать тип запроса/ответа для EAP-AKA;

поле "Атрибуты" следует в поле "Данные" за полем "Резерв" и должно использовать формат: тип-длина-значение;

2.3. содержание пакетов EAP-Request/AKA-Identity (подтип-5) (запрос идентификационной информации).

Идентификационной информацией для пользователя сети стандартов GSM900/1800, UMTS, LTE и информационно-телекоммуникационной сети "Интернет" должны быть IMSI (TMSI) и NAI (имя пользователя@оператор).

Запрос должен содержать один из трех атрибутов, указывающих тип запрашиваемого идентификатора:

AT_PERMANENT_ID_REQ;

AT_FULLAUTH_ID_REQ;

AT_ANY_ID_REQ;

2.4. содержание пакетов EAP-Response/AKA-Identity (ответ, содержащий запрашиваемую идентификационную информацию).

Ответ должен содержать атрибут AT_IDENTITY;

2.5. пакет EAP-Request/AKA-Challenge (подтип-1) должен содержать данные для полной аутентификации пользователя и включать атрибуты AT_RAND, AT_MAC и AT_AUTN;

2.6. пакет EAP-Response/AKA-Challenge должен содержать отклик пользователя и включать атрибуты AT_MAC и AT_RES;

2.7. пакет EAP-Response/AKA-Authentication-Reject (подтип-2) должен передаваться, если пользователь не принимает параметр аутентификации сети AUTN;

2.8. пакет EAP-Response/AKA-Synchronization-Failure (подтип-4) должен передаваться при ошибке в порядковом номере AUTN и включает атрибут AT_AUTS;

2.9. пакет EAP-Request/AKA-Reauthentication (подтип-13) должен передаваться при запросе сервером повторной быстрой аутентификации пользователя после получения EAP-Response/Identity или EAP-Response/AKA-Identity и включать атрибут AT_MAC;

2.10. пакет EAP-Response/AKA-Reauthentication должен передаваться в ответ на запрос AKA-Reauthentication и включать атрибуты AT_MAC, AT_IV и AT_ENCR_DATA;

2.11. пакет EAP-Response/AKA-Client-Error (подтип-14) должен передаваться при обнаружении пользователем ошибки в пакете EAP/AKA, и содержать атрибут AT_CLIENT_ERROR_CODE;

2.12. пакет EAP-Request/AKA-Notification (подтип-12) должен включать атрибут AT_NOTIFICATION AT_MAC и передаваться для передачи пользователю уведомления от идентифицирующей стороны;

2.13. пакет EAP-Response/AKA-Notification должен передаваться в ответ на EAP-Request/AKA-Notification и включать атрибуты AT_ENCR_DATA и AT_IV;

2.14. генерация ключа должна осуществляться с использованием функции SHA-1.

3. Требования к протоколу EAP-AKA' должны соответствовать требованиям к EAP-AKA за исключением:

для пакетов EAP-AKA' значение поля "Тип" должно устанавливаться равным "50";

должны использоваться новые атрибуты AT_KDF, AT_KDF_INPUT;

генерация ключа должна осуществляться с использованием функции SHA-256.

Приложение N 24
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

ТРЕБОВАНИЯ К ПРОТОКОЛУ ВЗАИМОДЕЙСТВИЯ СЕРВЕРА АБОНЕНТСКИХ ДАННЫХ HSS И/ИЛИ ЦЕНТРА АУТЕНТИФИКАЦИИ AUC С ОТДЕЛЬНЫМ АППАРАТНЫМ МОДУЛЕМ БЕЗОПАСНОСТИ HSM, ВЫПОЛНЯЮЩИМ КРИПТОГРАФИЧЕСКИЕ ФУНКЦИИ АУТЕНТИФИКАЦИИ АБОНЕНТОВ

1. Для взаимодействия сервера абонентских данных и/или центра аутентификации HSS/AuC и HSM, выполняющим криптографические функции аутентификации абонентов, должны использоваться следующие сообщения:

1.1. запрос со стороны HSS/AuC аутентификационной информации (Authentication Crypto Request - ACR).

Содержание информационных элементов, используемых в данном сообщении, приведено в таблице N 1;

Таблица N 1.

Информационный элемент	Содержание информационного элемента
Code	Информационный элемент Code должен содержать код сообщения HSM. Длина должна быть 48 бит.
K	Информационный элемент K должен содержать ключ K, который хранится в сервере абонентских данных HSS/AuC. Длина должна быть 128 бит.
AMF	Информационный элемент AMF (Authentication management field), предусмотренный п. 6.3 ETSI TS 133 102. Длина должна быть 16 бит.
SQN	Информационный элемент SQN (sequence number), предусмотренный п. 6.3 ETSI TS 133 102. Длина должна быть 48 бит.
AIR-Filler	Информационный элемент должен обеспечивать превышение длиной запроса длины соответствующего

	ему ответа. Длина должна быть 448 бит.

1.2. ответ HSM с аутентификационной информацией (Authentication Crypto Answer - ACA).

Содержание информационных элементов, используемых в данном сообщении, приведено в таблице N 2;

Таблица N 2.

Информационный элемент	Содержание информационного элемента
Code	Информационный элемент Code должен содержать код сообщения HSM. Длина должна быть 48 бит.
Authentication Vector	Информационный элемент Authentication Vector (AV), предусмотренный п. 6.3 ETSI TS 133 102. Длина должна быть 576 бит.

1.3. запрос со стороны HSS/AuC аутентификационной информации при ресинхронизации (Resynchronization Crypto Request - RCR).

Содержание информационных элементов, используемых в данном сообщении, приведено в таблице N 3;

Таблица N 3.

Информационный элемент	Содержание информационного элемента
Code	Информационный элемент Code должен содержать код сообщения HSM. Длина должна быть 48 бит.
K	Информационный элемент K должен содержать ключ абонента K, предусмотренный п. 6.3 ETSI TS 133 102. Длина должна быть 128 бит.
RAND	Информационный элемент RAND должен содержать RAND, предусмотренный п. 6.3 ETSI TS 133 102. Длина должна быть 128 бит.
Conc (SQN_{MS})	Информационный элемент Conc(SQN_{MS}) должен содержать Conc(SQNMS), предусмотренный п. 6.3 ETSI TS 133 102. Длина должна быть 48 бит.

1.4. ответ HSM с аутентификационной информацией при ресинхронизации (Resynchronization Crypto Answer - RCA).

Содержание информационных элементов, используемых в данном сообщении, приведено в

таблице N 4;

Таблица N 4.

Информационный элемент	Содержание информационного элемента
Code	Информационный элемент Code должен содержать код сообщения HSM. Длина должна быть 48 бит.
XMACS	Информационный элемент должен содержать криптографически защищенную имитовставку XMACS, предусмотренную п. 6.3 ETSI TS 133 102. Длина должна быть 64 бит.
SQN_{MS}	Информационный элемент должен содержать SQN_{MS}, предусмотренный п. 6.3 ETSI TS 133 102. Длина должна быть 48 бит.

2. HSS/AuC при реализации протокола взаимодействии с HSM должен обеспечить:

2.1. отправку запроса в HSM для генерации данных аутентификации;

2.2. установку для каждого отправленного запроса уникального адреса отправителя сообщения согласно протоколу взаимодействия 4 уровня (транспортного протокола передачи дейтаграмм пользователя - UDP);

2.3. ожидание для каждого отправленного запроса ответа от HSM в течение установленного при настройке времени.

3. HSM при реализации протокола взаимодействии с HSS/AuC должен обеспечить:

3.1. принятие от HSS/AuC корректного запроса для генерации данных аутентификации, обработку запроса и передачу ответа в HSS/AuC;

3.2. совпадение указанного в ответе адреса получателя сообщения с адресом, указанным в запросе отправителя сообщения, согласно протоколу взаимодействия 4 уровня;

3.3. отказ в ответе при поступлении от HSS/AuC некорректных запросов;

3.4. оповещение системы об отказе в ответе путем отключения интерфейса на физическом уровне взаимодействия.

4. Реализация протокола взаимодействия 4 уровня должна осуществляться с учетом следующих требований:

4.1. для адресации запросов и ответов согласно протоколу взаимодействия 4 уровня должны использоваться UDP-порты из диапазона 49152 - 65535;

4.2. адреса получателя ответов и отправителя ответов согласно протоколу взаимодействия 4 уровня должны устанавливаться одинаковыми в конфигурациях HSS/AuC и HSM соответственно;

4.3. информация, передаваемая в сообщениях согласно протоколу взаимодействия 4 уровня, должна быть защищена от несанкционированного доступа к ней.

5. Значения кодов информационных сообщений при взаимодействии HSS/AuC с HSM должны соответствовать значениям, приведенным в таблице N 5.

Таблица N 5.

	Информационное сообщение	Сокращение	Значение кода/Code
1.1	Authentication Crypto Request без использования AK	ACR	0
1.2	Authentication Crypto Request с использованием AK	ACR	1
2.	Authentication Crypto Answer	ACA	2
3.1	Resynchronization Crypto Request без использования AK	RCR	4
3.2	Resynchronization Crypto Request с использованием AK	RCR	5
4.	Resynchronization Crypto Answer	RCA	6

Приложение N 25
к Правилам применения оборудования
коммутации сетей подвижной
радиотелефонной связи. Часть VII.
Правила применения оборудования
коммутации стандарта LTE,
утвержденным приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 25.06.2018 N 319

Справочно

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

1. 3GPP - 3rd Generation Partnership Project (консорциум, разрабатывающий спецификации для сетей радиотелефонной связи).

2. AAA - Authentication, Authorization и Accounting (аутентификация, проверка полномочий,

учет).

3. AH - Authentication Header (аутентификационный заголовок для протокола IP).

4. ANID - Access Network Identity (идентификатор сети доступа).

5. APN - Access Point Name (идентификатора точки доступа к PDN).

6. ARP - Allocation and Retention Priority (назначение и сохранение приоритета).

7. AUTN - Authentication Token (символ аутентификации).

8. CoA - Care-of Address (адрес, назначаемый в момент регистрации пользователя в сети).

9. CN - Core Network (базовая сеть).

10. DA - Diameter Agent (оборудование, реализующее функцию агента протокола Diameter).

11. DHCP - Dynamic Host Configuration Protocol (протокол динамической настройки узла).

12. DSMIP - Dual-Stack Mobile IPv6 (двухстековый протокол IPv6 по обеспечению мобильности).

13. DPXA - Diameter Proxy Agents (функция прокси протокола Diameter).

14. DRDA - Diameter Redirect Agents (функция перенаправления протокола Diameter).

15. DRLA - Diameter Relay Agents (функция переключения протокола Diameter).

16. EAP-AKA - Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (расширяемый протокол Аутентификации для аутентификации и согласования ключей пользователей UMTS).

17. EIR - Equipment Identity Register (регистр идентификации оборудования).

18. eNodeB - Evolved NodeB (базовые станции стандарта LTE и LTE-Advanced).

19. ECM - EPS Connection Management (управление соединением в EPS).

20. ECM-CONNECTED - EPS Connection Management-CONNECTED (состояние процесса управления соединением для "абонентская радиостанция - соединение").

21. ECM-IDLE - EPS Connection Management-IDLE (исходное состояние процесса управления соединением для АС в EPS).

22. EMM - EPS Mobility Management (управление мобильностью в EPS).

23. EMM-DEREGISTERED - EPS Mobility Management-DEREGISTERED (состояние процесса управления мобильностью для АС в EPS - не зарегистрирована).

24. EPC - Evolved Packet Core (базовая сеть стандартов LTE и LTE-Advanced).

25. ePDG - Evolved Packet Data Gateway (оборудование, реализующее функции доступа к

оборудованию коммутации стандарта LTE из сети Интернет при использовании доступа UTWAN).

26. EPS - Evolved Packet System (сеть радиодоступа и базовая сеть стандартов LTE и LTE-Advanced).

27. ESP - Encapsulating Security Payload (протокол защиты (шифрования) данных).

28. E-UTRAN - Evolved UTRAN (сеть радиодоступа стандартов LTE и LTE-Advanced).

29. FA - Foreign Agent (агент визитной сети).

30. FACoA - Foreign Agent Care-of Address (адрес агента визитной сети).

31. GBR - Guaranteed Bit Rate (гарантированная скорость передачи данных).

32. GRE - Generic Routing Encapsulation (общая инкапсуляция маршрутов).

33. GSM - Global System for Mobility (глобальная система мобильной связи).

34. GTP - GPRS Tunnelling Protocol (протокол туннелирования GPRS).

35. HA - Home Agent (агент домашней сети сети).

36. HBM - Host Based Mobility (управление мобильностью на базе хостов).

37. HLR - Home Location Register (домашний регистр местонахождения).

38. HMAC - hash-based message authentication code (код аутентификации сообщений, использующий хеш-функции).

39. HPLMN - Home Public Land Mobile Network (сеть Оператора мобильной связи, в которой абонент подписан на оказание услуг мобильной связи).

40. HSS - Home Subscriber Server (сервер абонентских данных).

41. HSM - Hardware Security Module (аппаратный модуль безопасности).

42. ICMP - Internet Control Message Protocol (протокол управляющих сообщений в Интернет).

43. IKEv2 - Internet Key Exchange version 2 (Протокол обмена ключами в Интернет версия 2).

44. IMEI - International Mobile Equipment Identity (международный идентификатор оборудования абонентской радиостанции).

45. IMEISV - International Mobile Equipment Identity and Software Version (международный идентификатор оборудования и номер версии программного обеспечения оборудования абонентской радиостанции).

46. IMSI - International Mobile Subscriber Identity (международный номер абонентской станции).

47. IP - Internet Protocol (протокол Интернет).

48. IPSec - Internet Protocol Security (протокол Интернет с поддержкой функций безопасности)

49. KDF - key derivation function (функция формирования ключа).

50. LIPA - Local IP Access (местный IP-доступ).

51. LMA - Local Mobility Anchor (локальный узел управления мобильностью).

52. LTE - Long-Term Evolution (эволюция на длительный период).

53. LTE-Advanced - (развитие стандарта LTE).

54. MAG - Mobile Access Gateway (шлюз мобильного доступа).

55. MBR - Maximum Bit Rate (максимальная скорость передачи).

56. MCM - Multi-connection mode (режим нескольких соединений).

57. MD5 - Message Digest 5 (128-битный алгоритм хеширования).

58. MIPv4 - Mobile IP version 4 (расширение функциональности протокола IPv4 по обеспечению мобильности).

59. MME - Mobility Management Entity (модуль управления мобильностью).

60. MSISDN - Mobile Subscriber ISDN Number (международный номер АС в сети ISDN).

61. NAI - Network Access Identifier (идентификатор доступа к сети).

62. NAS protocol - Non-Access-Stratum protocol (протокол слоя без доступа).

63. NBM - Network Based Mobility (управление мобильностью на базе сети).

64. NDP - Neighbor Discovery Protocol (протокол обнаружения соседей).

65. Non-3GPP - сеть радиодоступа, отличная от стандартов GSM 900/1800, UMTS, LTE, использующая передачу данных в диапазоне от 30 МГц до 66 ГГц

66. P-GW - Packet Data Networks Gateway (шлюз взаимодействия с сетями, использующими технологию с коммутацией пакетов).

67. PCRF - The Policy and Charging Rules Function (функция правил политики)

68. PDN - Packet Data Network (сеть передачи данных).

69. PMIPv6 - Proxy Mobile IP version 6 (расширение функциональности протокола IPv6 по обеспечению сетевой мобильности).

70. PPP - Point-to-Point Protocol (протокол канала связи с непосредственным соединением).

71. PRF - PSEUDO_RANDOM_FUNCTION (псевдослучайная функция).

72. QCI - QoS Class Identifier (идентификатор класса качества обслуживания).

73. QoS - Quality of Service (качество обслуживания).

74. RADIUS - Remote Authentication in Dial-In User Service (протокол для аутентификации, авторизации удаленных пользователей).

75. S1-AP - S1 Application Protocol (прикладной протокол для интерфейса S1).

76. SCM - Single-connection mode (режим одного соединения).

77. SCTP - Stream Control Transmission Protocol (протокол передачи с управлением потоками).

78. SGSN - Serving GPRS Support Node (обслуживающий узел поддержки GPRS).

79. SGsAP - SGs Application Part (прикладной протокол для интерфейса SGs).

80. S-GW - Serving Gateway (обслуживающий шлюз).

81. SHA - Secure Hash Algorithm (алгоритм криптографического хеширования).

82. SIPTO - Selected IP Traffic Offload (возможность распределения трафика IP).

83. SRVCC - Single Radio Voice Call Continuity (отдельная непрерывность голосового вызова на радиоинтерфейсе).

84. TCP - Transmission Control Protocol (протокол управления передачей).

85. TEID - Tunnel Endpoint Identifier (идентификатор конечной точки туннеля).

86. TLV - Tag-length-value ("тип-длина-значение", метод записи данных в телекоммуникационных протоколах).

87. TMAG - Trusted Mobile Access Gateway (шлюз мобильного доступа).

88. TMSI - Temporary Mobile Subscriber Identity (временный идентификатор мобильного абонента).

89. TSCM - Transparent single-connection mode (режим одного прозрачного соединения).

90. TWAG - TWAN Access Gateway (шлюз сети TWAN).

91. TWAN - trusted WLAN (доверенный беспроводный доступ).

92. UDP - User Datagram Protocol (протокол передачи дейтаграмм пользователя).

93. UE - User Equipment (радиотелефонная станция стандартов GSM900/1800/UMTS/LTE, поддерживающая стандарт беспроводной передачи данных в диапазоне от 30 МГц до 66 ГГц).

94. UMTS - Universal Mobile Telecommunications System (универсальная система мобильной связи).

95. USIM - Universal Subscriber Identity Module (универсальный модуль идентификации

абонента; карта мобильного пользователя для работы в сети UMTS).

96. UTRAN - Universal Terrestrial Radio Access Network (сеть радиодоступа стандарта UMTS).

97. UTWAN - Untrusted WLAN (ненадежный беспроводный доступ).

98. VPLMN - Visited Public Land Mobile Network (гостевая сеть мобильной связи, в которой в настоящий момент обслуживается абонент).

99. WLAN - Wireless Local Area Network (локальная сеть, построенная на основе беспроводных технологий).

WLAN AN - WLAN Access Network (сеть беспроводного абонентского доступа).