Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2760

(05/2011)

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

Сети последующих поколений – Безопасность

Концепция безопасности мобильности в СПП

Рекомендация МСЭ-Т Y.2760

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие положения	Y.100–Y.199
Услуги, приложения и промежуточные программные средства	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и присваивание имен	Y.500–Y.599
Эксплуатация, управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Рабочие характеристики	Y.800–Y.899
АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ	
Общие положения	Y.1000–Y.1099
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, возможности сетей и административное управление ресурсами	Y.1200–Y.1299
Транспортирование	Y.1300–Y.1399
Взаимодействие	Y.1400–Y.1499
Качество обслуживания и сетевые показатели качества	Y.1500–Y.1599
Сигнализация	Y.1600–Y.1699
Эксплуатация, управление и техническое обслуживание	Y.1700–Y.1799
Начисление платы	Y.1800–Y.1899
IPTV по СПП	Y.1900–Y.1999
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	
Структура и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты обслуживания: возможности услуг и архитектура услуг	Y.2200–Y.2249
Аспекты обслуживания: взаимодействие услуг и СПП	Y.2250–Y.2299
Нумерация, присваивание имен и адресация	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
Будущие сети	Y.2600–Y.2699
Безопасность	**Y.2700–Y.2799**
Обобщенная мобильность	Y.2800–Y.2899
Открытая среда операторского класса	Y.2900–Y.2999
Будущие сети	Y.3000–Y.3099

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т Y.2760

Концепция безопасности в СПП

Резюме

В Рекомендации МСЭ-Т Y.2760 определяется концепция безопасности мобильности в транспортной страте сетей последующего поколения (СПП). В Рекомендации рассматриваются требования к безопасности, механизмы обеспечения безопасности и процедуры управления мобильностью и контроля мобильности в СПП.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т Y.2760	20.05.2011 г.	13-я

Ключевые слова

Безопасность мобильности, СПП.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Стр.

Рекомендация МСЭ-Т Y.2760

Концепция безопасности мобильности в СПП

1 Сфера применения

В настоящей Рекомендации описана концепция безопасности мобильности в транспортной страте сетей последующего поколения (СПП). Рассматриваются требования безопасности, определенные в [ITU-T Y.2018]. Рекомендация включает следующие вопросы: аутентификация и управление ключами; установление контекста безопасности; безопасность IP-мобильности; и безопасность управления мобильностью, контроля и транспортирования в транспортной страте. Рассматриваемые сценарии включают мобильность в рамках одной и нескольких технологий, в рамках одного и нескольких доменов.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T Q.1706] Рекомендация МСЭ-Т Q.1706/Y.2801 (2006 г.), *Требования к управлению мобильностью для СПП*.

[ITU-T X.805] Рекомендация МСЭ-Т X.805 (2003 г.), *Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами*.

[ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for next generation networks*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[ITU-T Y.2014] Recommendation ITU-T Y.2014 (2010), *Network attachment control functions in next generation networks*.

[ITU-T Y.2018] Recommendation ITU-T Y.2018 (2009), *Mobility management and control framework and architecture within the NGN transport stratum*.

[ITU-T Y.2701] Рекомендация МСЭ-Т Y.2701 (2007 г.), *Требования к безопасности для сетей последующих поколений версии 1*.

[ITU-T Y.2704] Рекомендация МСЭ-Т Y.2704 (2010 г.), *Механизмы и процедуры безопасности для сетей последующих поколений*.

[ITU-T Y-Sup.7] ITU-T Y-series Recommendation − Supplement 7 (2008), *ITU-T Y.2000-series, Supplement on NGN release 2 scope*.

[ITU-R M.1645] Recommendation ITU-R M.1645 (2003), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 передача обслуживания (handover) (пункт 6.2.2 [ITU-T Q.1706]): Возможность предоставлять услуги подвижному объекту во время движения и после него с некоторым воздействием на соглашения об уровне обслуживания.

3.1.2 горизонтальная мобильность (horizontal mobility) (пункт 6.2.3 [ITU-T Q.1706]): Мобильность на том же уровне, которая определена в [ITU-R M.1645]. Как правило, она называется мобильностью при той же технологии доступа.

3.1.3 мобильность (mobility) (пункт 3.2 [ITU-T Q.1706]): Возможность пользователя или иных подвижных единиц устанавливать связь и получать доступ к услугам вне зависимости от смены места положения или технических средств.

3.1.4 транспортная страта СПП (NGN transport stratum) (пункт 3.10 [ITU-T Y.2011]): Это та часть СПП, которая обеспечивает функции пользователя по передаче данных и функции по контролю транспортных ресурсов и управлению ими для переноса этих данных между оконечными объектами.

3.1.5 доверие (trust) (пункт 3.2.9 [ITU-T Y.2701]): Говорят, что объект X доверяет объекту Y в отношении некоторой совокупности действий, если и только если объект X исходит из того, что в связи с данными действиями объект Y будет вести себя определенным образом.

3.1.6 вертикальная мобильность (vertical mobility) (пункт 6.2.3 [ITU-T Q.1706]): Мобильность между различными уровнями, которая определена в [ITU-R M.1645]. Как правило, она называется мобильностью при разных технологиях доступа.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 мобильность в рамках нескольких технологий: См. "Вертикальная мобильность" в пункте 3.1;

3.2.2 мобильность в рамках одной технологии: См. "Горизонтальная мобильность" в пункте 3.1;

3.2.3 контекст безопасности: Набор параметров безопасности, включая идентификатор, материал ключа, алгоритм ключа и т. д.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

3G	3rd Generation	Третье поколение
ABG-FE	Access Border Gateway Functional Entity	Функциональный объект пограничного шлюза доступа
AE	Authentication Extension	Расширение аутентификации
AKA	Authentication and Key Agreement	Соглашение об аутентификации и ключе
AM-FE	Access Management Functional Entity	Функциональный объект управления доступом
AN-FE	Access Node Functional Entity	Функциональный объект узла доступа
ANI	Application to Network Interface	Интерфейс "приложение-сеть"
AR-FE	Access Relay Functional Entity	Функциональный объект коммутатора доступа
DDoS	Distributed Deny of Service	Распределенный отказ в обслуживании
EAP	Extensible Authentication Protocol	Расширяемый протокол аутентификации
EN-FE	Edge Node Functional Entity	Функциональный объект периферийного узла
FA	Foreign Agent	Внешний агент
HA	Home Agent	Местный агент

HDC-FE	Handover Decision Control Functional Entity	Функциональный объект решения о передаче обслуживания и управления передачей обслуживания
IP	Internet Protocol	Протокол Интернет
L3HEF	Layer 3 Handover Execution Function	Функция выполнения передачи обслуживания уровня 3
MIP	Mobile IP	Протокол Mobile IP
MIPv4	Mobile IP for IP version 4. See [b-IETF RFC 3220]	Протокол Mobile IP для IP версии 4. См. [b-IETF RFC 3220]
MIPv6	Mobile IP for IP version 6. See [b-IETF RFC 3775]	Протокол Mobile IP для IP версии 6. См. [b-IETF RFC 3775]
MLM-FE	Mobile Location Management Functional Entity	Функциональный объект управления на основе местоположения мобильного устройства
MMCF	Mobility Management and Control Functions	Функции управления мобильностью и контроля мобильности
MN	Mobile Node	Узел подвижной связи
MOBIKE	IKEv2 Mobility and Multihoming Protocol. See [b-IETF RFC 4555]	Протокол обеспечения мобильности и множественной адресации IKEv2. См. [b-IETF RFC 4555]
NACF	Network Attachment Control Functions	Функции контроля соединения с сетью
NGN	Next Generation Network	СПП Сети последующих поколений
NID-FE	Network Information Distribution Functional Entity	Функциональный объект распределения сетевой информации
NNI	Network to Network Interface	Интерфейс "сеть-сеть"
PKI	Public Key Infrastructure	Инфраструктура открытых ключей
PMIPv6	Proxy Mobile IPv6. See [b-IETF RFC 5213]	Протокол управления мобильностью IPv6. См. [b-IETF RFC 5213]
RAN	Radio Access Network	Сеть радиодоступа
RRP	Registration Reply	Ответ на запрос регистрации
RRQ	Registration Request	Запрос регистрации
TAA-FE	Transport Authentication and Authorization Functional Entity	Функциональный объект аутентификации и авторизации транспортирования
TLM-FE	Transport Location Management Functional Entity	Функциональный объект управления на основе местоположения при транспортировании
TLS	Transport Layer Security	Безопасность транспортного уровня
TTLS	Tunnelled Transport Layer Security	Безопасность туннелирования транспортного уровня
TUP-FE	Transport User Profile Functional Entity	Функциональный объект профиля пользователя транспортирования
UE	User Equipment	Оборудование пользователя
UNI	User to Network Interface	Интерфейс "пользователь-сеть"
WiMax	Worldwide Interoperability for Microwave Access	Технология WiMax – глобальная функциональная совместимость для микроволнового доступа
WLAN	Wireless LAN	Беспроводная локальная сеть

5 Требования к безопасности для мобильности в СПП

СПП поддерживает технологии многостанционного доступа, такие как WLAN, WiMax и 3G RAN и т. д. [ITU-T Y.2012]. Поддержка мобильности является одной из важных характеристик СПП, которая включает кочевничество и передачу обслуживания. В СПП варианта 2 передача обслуживания охватывает сценарии доступа "внутри сети" и "между сетями" [ITU-T Y-Sup.7].

СПП поддерживает следующие функциональные возможности:

1) Модель доверия: модель доверия безопасности СПП определяет три зоны безопасности: доверенная, доверенная, но уязвимая и недоверенная [ITU-T Y.2701]. В ней показано, что сеть доступа до получения доступа в базовую сеть должна осуществить проход через шлюз безопасности.

2) СПП поддерживает технологии многостанционного доступа.

3) СПП поддерживает несколько протоколов мобильности, такие как MIPv4, MIPv6, DSMIPv6, PMIPv6 и MOBIKE.

4) СПП поддерживает UE с большим числом радиоканалов, такое как WLAN, WiMax, 3G RAN и т. д.

5) СПП поддерживает непрерывность обслуживания при передаче обслуживания между неоднородными системами доступа.

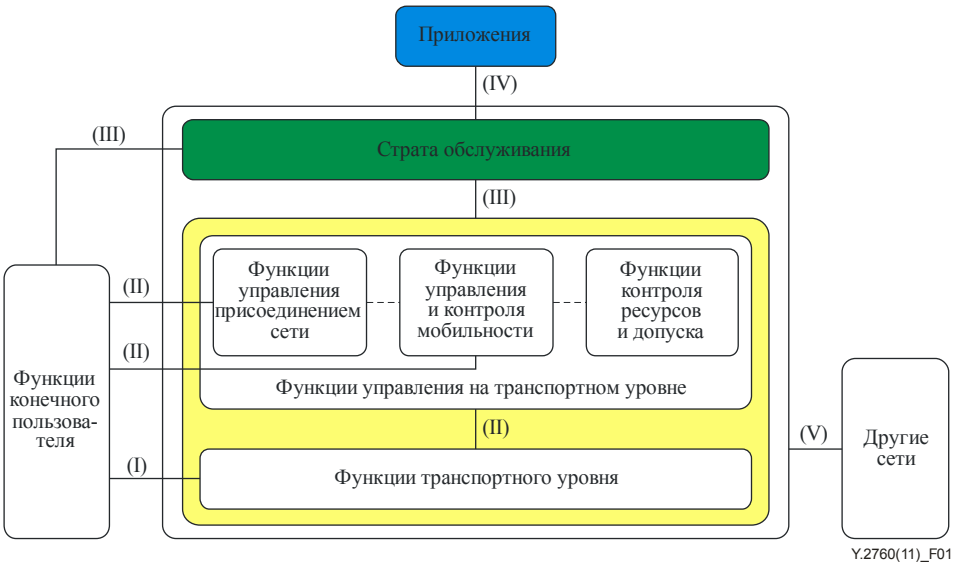

Рисунок 1 – Архитектура безопасности мобильности в СПП

Определяются пять групп свойств безопасности по:

(I) уделению особого внимания безопасности транспортирования между функциями конечного пользователя и транспортными функциями, такими как безопасность доступа, которые могут быть защищены физическими или логическими средствами между функциями конечного пользователя и объектом сети доступа в функциях транспортирования. (I) также учитывает безопасность UNI между функциями конечного пользователя и функциями транспортирования;

(II) уделению особого внимания безопасности в уровне управления между функциями конечного пользователя и функциональным объектом управления транспортированием. (II) также уделяет особое внимание безопасности в интерфейсе сообщений управления между объектом функций транспортирования и функциональным объектом управления транспортированием. (II) учитывает безопасность UNI между функциями конечного пользователя и функциями управления транспортированием;

(III) уделению особого внимания безопасности интерфейса между функциями конечного пользователя и страты обслуживания. (III) также уделяет особое внимание безопасности в интерфейсе сообщений управления между объектом функций управления транспортированием и стратой обслуживания. (III) учитывает безопасность UNI между функциями конечного пользователя и стратой обслуживания;

(IV) уделению особого внимания безопасности интерфейса между стратой обслуживания и объектом прикладного уровня. (IV) учитывает безопасность ANI между функциями конечного пользователя и функциями транспортирования;

(V) уделению особого внимания безопасности интерфейса между СПП и другими сетями, которые включают и транспортный уровень, и уровень управления. (V) учитывает безопасность NNI между СПП и другими сетями.

В отношении угроз безопасности и требований к безопасности, определенных в настоящей Рекомендации, применимы принципы, изложенные в [ITU-T X.805].

5.1 Угрозы безопасности

Следующие угрозы безопасности определены в [ITU-T Y.2018]:

T1 UE может не иметь авторизации для инициирования сигнализации мобильности с MLM-FE.

T2 В сигнализацию мобильности могут незаконно проникнуть злоумышленники.

T3 MLM-FE может играть чужую роль в целях передачи ложной информации UE.

T4 Местоположение UE может быть перехвачено злоумышленниками.

T5 Может произойти атака типа "перенаправление трафика".

T6 Атакующий объект может включить себя в трассу путем атаки "незаконный посредник".

T7 Атака типа DDoS может расходовать большой объем сетевых ресурсов.

T8 UE может не иметь авторизации для получения информации от HDC-FE или NID-FE.

T9 HDC-FE или NID-FE могут играть чужую роль для принудительной доставки ложной информации оборудованию UE.

T10 Сигнализация между UE и HDC-FE или NID-FE может быть изменена или перехвачена.

T11 Данные пользовательской плоскости могут быть перехвачены или изменены.

5.2 Требования к безопасности

Следующие требования к безопасности определены в [ITU-T Y.2018].

R1 Требуется, чтобы осуществлялась взаимная аутентификация UE и NID-FE.

R2 Требуется, чтобы обеспечивалась защита целостности и конфиденциальности сигнализации между UE и MLM-FE.

R3 Требуется, чтобы обеспечивалась защита сигнализации между UE и MLM-FE от атак типа "взлом путем замещения оригинала".

R4 Требуется, чтобы обеспечивалась секретность местоположения UE.

R5 Требуется, чтобы осуществлялась взаимная аутентификация UE и HDC-FE.

R6 Требуется, чтобы обеспечивалась защита целостности и конфиденциальности сигнализации между UE и HDC-FE.

R7 Требуется, чтобы обеспечивалась защита сигнализации между UE и HDC-FE от атак типа "взлом путем замещения оригинала".

R8 Требуется, чтобы обеспечивалась защита аутентификации и сигнализации с малым запаздыванием.

R9 Требуется, чтобы обеспечивалась оптимизация трафика, относящегося к безопасности.

R10 Требуется, чтобы средство обеспечения безопасности мобильности было независимым от среды передачи.

R11 Требуется, чтобы были доступны механизмы для защиты трафика пользовательской плоскости между UE и EN-FE, если указание об этом имеется в профиле пользователя.

В дополнение к требованиям безопасности, определенным в [ITU-T Y.2018], учитывается также следующее требование к безопасности.

R12 Требуется, чтобы поддерживалась безопасность при множественных соединениях.

6 Возможности обеспечения безопасности, поддерживаемые соответствующими функциональными объектами

В СПП с безопасностью мобильности связаны следующие функциональные объекты:

- Функциональный объект профиля пользователя транспортирования (TUP-FE).
- Функциональный объект аутентификации и авторизации транспортирования (TAA-FE).
- Функциональный объект управления на основе местоположения мобильного устройства (MLM-FE).
- Функциональный объект решения о передаче обслуживания и управления передачей обслуживания (HDC-FE).

- Функциональный объект распределения сетевой информации (NID-FE).
- Функциональный объект управления доступом (AM-FE).
- Функция выполнения передачи обслуживания уровня 3 (L3HEF).
- Функциональный объект узла доступа (AN-FE).

6.1 Функциональный объект профиля пользователя транспортирования (TUP-FE)

TUP-FE сохраняет данные аутентификации контракта, такие как материал ключа, методы аутентификации и профиль пользователя транспортирования. Подробное функциональное описание TUP-FE содержится в [ITU-T Y.2014].

6.2 Функциональный объект аутентификации и авторизации транспортирования (TAA-FE)

TAA-FE извлекает данные аутентификации и информацию авторизации доступа из TUP-FE. TAA-FE может также функционировать в качестве прокси.

Подробное функциональное описание содержится в [ITU-T Y.2014].

6.3 Функциональный объект управления на основе местоположения мобильного устройства (MLM-FE)

MLM-FE получает информацию аутентификации, авторизации и учета от NACF, выполняет взаимную аутентификацию с UE и создает ассоциацию безопасности между UE и MLM-FE. Подробное функциональное описание содержится в [ITU-T Y.2018].

6.4 Функциональный объект решения о передаче обслуживания и управления передачей обслуживания (HDC-FE)

Требуется, чтобы HDC-FE устанавливал ассоциацию безопасности с UE, и он получает ключ защиты, используемый для ассоциации безопасности, от TAA-FE через TLM-FE. Подробное функциональное описание содержится в [ITU-T Y.2018].

6.5 Функциональный объект распределения сетевой информации (NID-FE)

Требуется, чтобы NID-FE устанавливал ассоциацию безопасности с UE в целях защиты такой информации, как информация выбора сети. NID-FE может получать информацию безопасности от TAA-FE через TLM-FE. Подробное функциональное описание содержится в [ITU-T Y.2018].

6.6 Функциональный объект управления доступом (AM-FE)

AM-FE пересылает объекту TAA-FE запросы доступа в сеть в целях аутентификации пользователя, формирования разрешения доступа или отказа в доступе и извлечения зависящих от пользователя параметров конфигурации доступа. AM-FE может повторно использовать данные регистрации/аутентификации для быстрого восстановления без повторного полного выполнения процедур регистрации/аутентификации/конфигурации. Подробное функциональное описание содержится в [ITU-T Y.2014].

6.7 Функция выполнения передачи обслуживания уровня 3 (L3HEF)

Требуется, чтобы L3HEF устанавливал ассоциацию безопасности с UE для защиты трафика между ними. Подробное функциональное описание содержится в [ITU-T Y.2018].

ПРИМЕЧАНИЕ. − Безопасность L3HEF отвечает требованию безопасности относительно защиты трафика пользовательской плоскости между UE и EN-FE.

6.8 Функциональный объект узла доступа (AN-FE)

Требуется, чтобы AN-FE устанавливал ассоциацию безопасности с UE, и он получает материал ключа от TAA-FE через AM-FE. Подробное функциональное описание содержится в [ITU-T Y.2018].

7 Управление ключами и аутентификация

7.1 Структура управления ключами

Для безопасности мобильности в СПП используется иерархический механизм выработки ключа. В СПП существуют несколько видов материала ключа, например корневой ключ, сеансовый ключ и т. д. Корневой ключ – это вид долгосрочных полномочий, сохраняемых безопасным образом (например, общий секретный ключ или пароль). Сеансовый ключ – это вид краткосрочного материала ключа, генерируемого на основе корневого ключа. UE и объект аутентификации в СПП (например, TAA-FE/TUP-FE) сохраняют общий корневой ключ.

Как правило, материал сеансового ключа генерируется на основании корневого ключа и других параметров генерирования ключа, таких как информация согласования в процессе процедуры аутентификации. Материал сеансового ключа используется для защиты трафика сигнализации и пользовательского трафика. Сеансовый ключ может быть выработан позже. Механизм выработки ключа зависит от конкретного криптографического алгоритма или протокола.

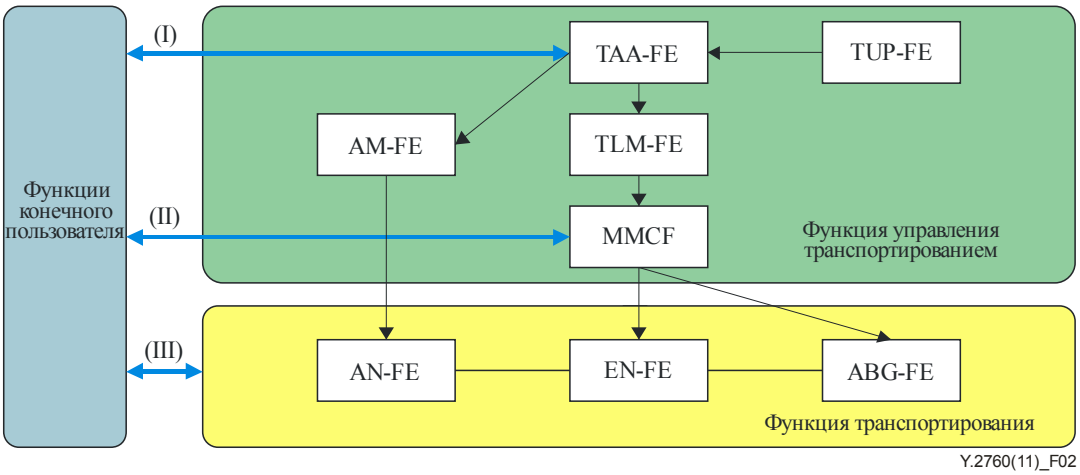

Рисунок 2 – Общая концепция безопасности мобильности на основе ключей в СПП

Ниже следует описание общей концепции безопасности мобильности на основе ключей в СПП.

(I) UE выполняет процедуру взаимной аутентификации с функциональными объектами в СПП. В рамках процедуры аутентификации TUP-FE генерирует векторы аутентификации на основе материала корневого ключа и направляет эти векторы аутентификации объекту TAA-FE. После успешного завершения процедуры взаимной аутентификации TAA-FE и UE генерируют материал сеансового ключа. Материал сеансового ключа может использоваться для генерирования материала подсеансового ключа. Материал сеансового ключа передается функциональным объектам AM-FE и MMCF. На основе принятого материала сеансового ключа оба объекта – AM-FE и MMCF – могут генерировать материал подсеансового ключа.

(II) Ассоциации безопасности в эталонных точках между UE и MMCF базируются на материале сеансового ключа, полученного от TAA-FE через TLM-FE. Материал сеансового ключа, используемый в (II), генерируется или вырабатывается в соответствии с материалом сеансового ключа в TAA-FE.

(III) Ассоциации безопасности между UE и уровнем функций транспортирования в СПП устанавливаются на основании материала общего ключа, который генерируется из материала предыдущего сеансового ключа в TAA-FE, AM-FE или MMCF. AN-FE принимает материал сеансового ключа от TAA-FE через AM-FE. Если AM-FE обладает возможностью выработки материала сеансового ключа, AN-FE может получить материал сеансового ключа непосредственно от AM-FE. Оба объекта – EN-FE и ABG-FE – принимают генерируемый материал ключа от TAA-FE через TLM-FE и MMCF. Если MMCF обладает возможностью выработки материала сеансового ключа, EN-FE и ABG-FE могут получать материал ключа напрямую от MMCF.

Процедура аутентификации базируется на протоколе типа "вызов-ответ", например AKA [b-3GPP TS 33.102].

7.2 Аутентификация

7.2.1 Общая процедура аутентификации

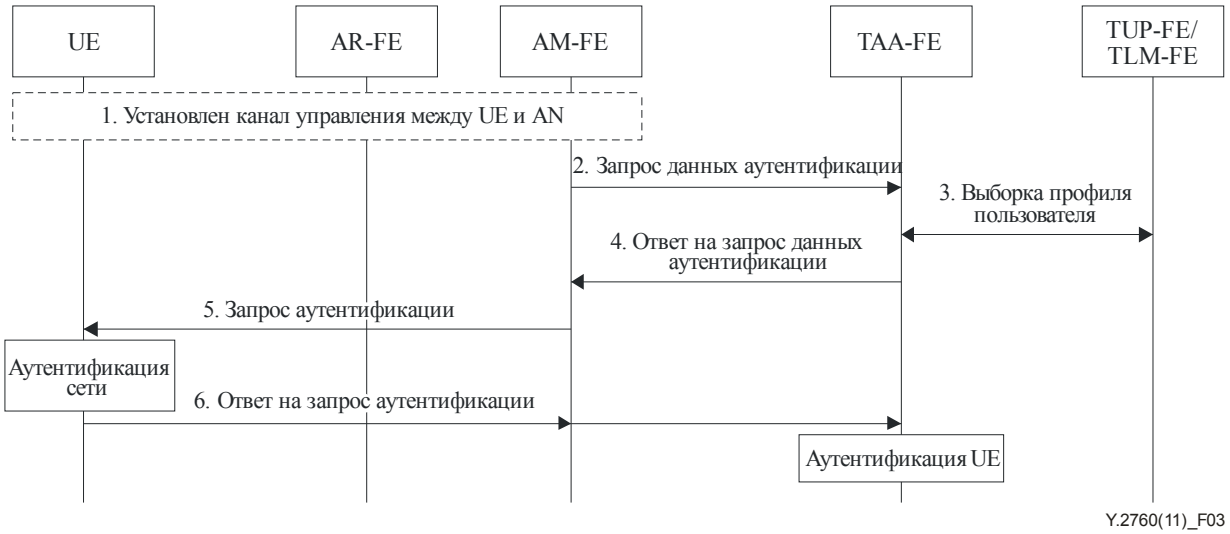

Рисунок 3 – Общая процедура аутентификации

1) Установлен канал управления между UE и функциями сети доступа (эта процедура не входит в сферу применения настоящей Рекомендации).

2) AM-FE отправляет информацию UE объекту TAA-FE для запроса данных аутентификации.

3) TAA-FE получает информацию аутентификации из запроса аутентификации, который включает идентификатор абонента и информацию сети доступа, и взаимодействует с TUP-FE/TLM-FE для получения профиля пользователя и векторов аутентификации, включая жетон аутентификации и материал сеансового ключа.

4) TAA-FE направляет ответ, содержащий данные аутентификации, включая жетон аутентификации, объекту AM-FE.

5) AM-FE направляет запрос аутентификации оборудованию UE. UE осуществляет выборку жетона аутентификации из запроса аутентификации и генерирует локальные векторы аутентификации, включая материал сеансового ключа, на основании жетона аутентификации и корневого ключа. UE выполняет аутентификацию сети путем валидации принятого жетона аутентификации.

6) UE направляет ответ на запрос аутентификации объекту AM-FE, включая жетон аутентификации, сгенерированный оборудованием UE. AM-FE пересылает информацию объекту TAA-FE. TAA-FE осуществляет выборку жетона аутентификации и проверяет валидацию принятого жетона аутентификации в целях аутентификации UE.

7.2.2 Общая процедура быстрой повторной аутентификации

Быстрая повторная аутентификация используется для уменьшения задержки передачи обслуживания. TUP-FE/TLM-FE не участвует в процедуре быстрой повторной аутентификации, что ускоряет процедуру аутентификации и снижает нагрузку на TUP-FE/TLM-FE. Рекомендуется, чтобы и UE, и объекты аутентификации в СПП поддерживали общую быструю повторную аутентификацию.

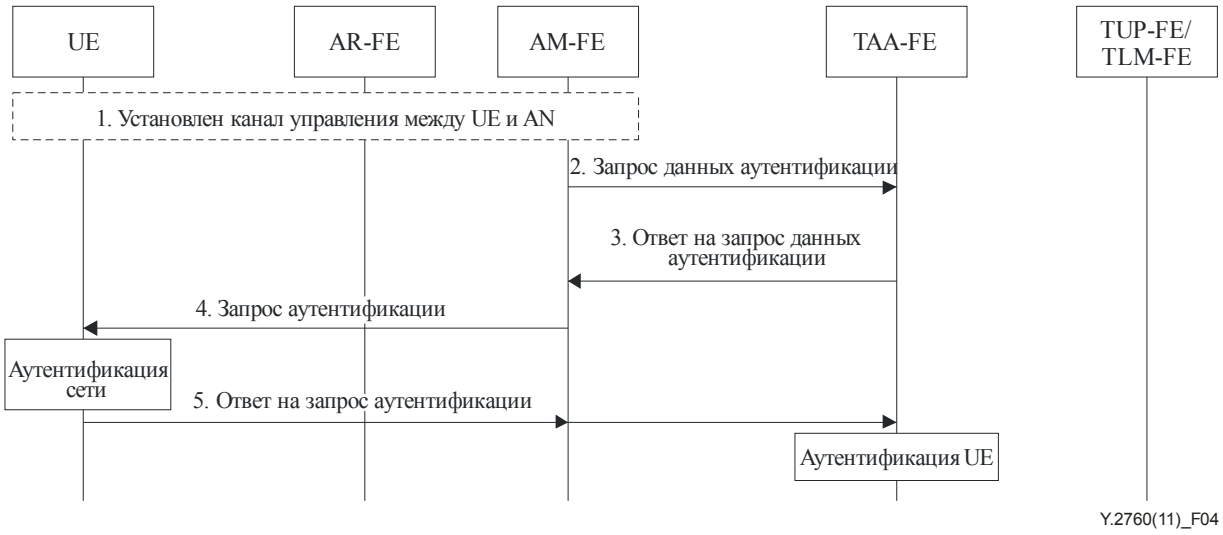

Рисунок 4 – Общая процедура быстрой повторной аутентификации

При исходном положении о том, что UE и TAA-FE обладают возможностью выполнения быстрой повторной аутентификации, выполняются следующие шаги.

1) Установлен канал управления между UE и функциями сети доступа (эта процедура не входит в сферу применения настоящей Рекомендации).

2) AM-FE отправляет информацию UE объекту TAA-FE для запроса данных аутентификации.

3) TAA-FE направляет ответ, содержащий данные аутентификации, включая жетон аутентификации, объекту AM-FE.

4) AM-FE направляет запрос аутентификации оборудованию UE. UE осуществляет выборку жетона аутентификации из запроса аутентификации и генерирует локальные векторы аутентификации, включая материал сеансового ключа, на основании жетона аутентификации и корневого ключа. UE выполняет аутентификацию сети путем валидации принятого жетона аутентификации.

5) UE направляет ответ на запрос аутентификации объекту AM-FE, включая жетон аутентификации, сгенерированный оборудованием UE. AM-FE пересылает информацию объекту TAA-FE. TAA-FE осуществляет выборку жетона аутентификации и проверяет валидацию принятого жетона аутентификации в целях аутентификации UE.

Если UE повторно использует материал сеансового ключа, информация быстрой повторной аутентификации используется только для взаимной аутентификации. Если UE не использует повторно сеансовый ключ, UE и объект аутентификации (например, TAA-FE/TUP-FE) генерируют новый сеансовый ключ на основании материала сеансового ключа и информации быстрой повторной аутентификации.

7.2.2.1 Оптимизированная быстрая повторная аутентификация

Для выполнения оптимизированной быстрой повторной аутентификации UE, который предварительно был аутентифицирован СПП, генерирует информацию аутентификации. Эта процедура отличается от общей повторной аутентификации, в которой UE первым выполняет аутенитификацию СПП, и далее СПП генерирует жетон аутентификации.

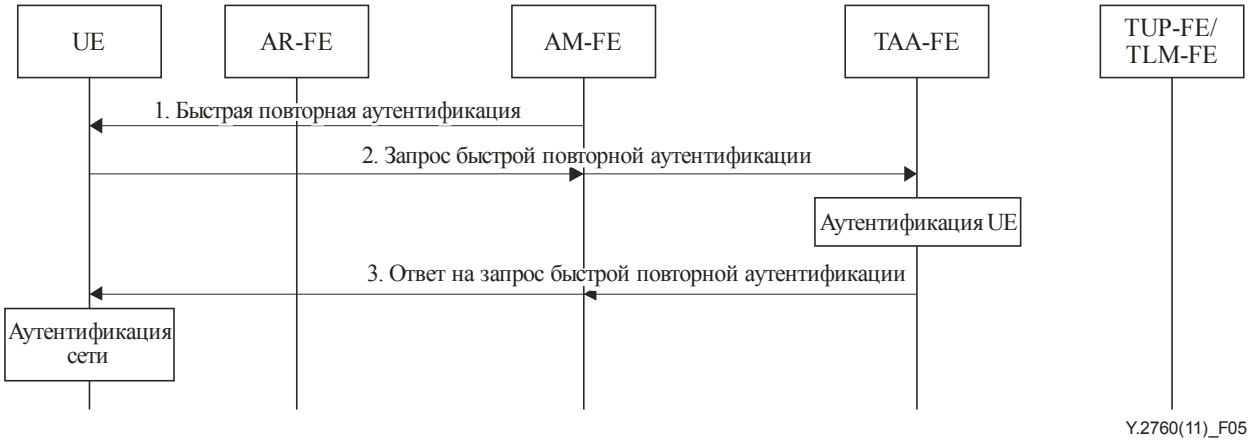

Рисунок 5 – Процедура оптимизированной быстрой повторной аутентификации

1) Установлен канал управления между UE и функциями сети доступа (эта процедура не входит в сферу применения настоящей Рекомендации). AM-FE отправляет индикацию оптимизированной повторной аутентификации оборудованию UE, которая показывает, что TAA-FE поддерживает оптимизированную быструю повторную аутентификацию.

2) UE генерирует вектор аутентификации и отправляет запрос оптимизированной повторной аутентификации объекту TAA-FE через AM-FE. Запрос оптимизированной повторной аутентификации включает жетон аутентификации и информацию повторной аутентификации. TAA-FE генерирует локальный вектор аутентификации и новый материал сеансового ключа на основании информации повторной аутентификации и материала сеансового ключа. TAA-FE выполняет аутентификацию UE путем валидации принятого жетона аутентификации.

3) TAA-FE отправляет ответ на запрос повторной аутентификации, включая жетон аутентификации, оборудованию UE через AM-FE. UE выполняет аутентификацию сети с помощью собственного вектора аутентификации. После успешного завершения аутентификации UE может генерировать материал подсеансового ключа.

7.2.3 Внутридоменная аутентификация

7.2.3.1 Аутентификация при одиночном сетевом соединении

Одиночное сетевое соединение означает, что UE может определить разные сети, но осуществить одновременный доступ только к одной сети. Предварительная авторизация означает, что UE выполняет взаимную аутентификацию с целевой сетью через обслуживающую сеть до того, как UE осуществит передачу обслуживания в целевую сеть. Если UE базируется на одиночном сетевом соединении, UE использует предварительную аутентификацию для сохранения непрерывности обслуживания и малой задержки. Процедура предварительной аутентификации аналогична общей процедуре аутентификации. При необходимости в процедуре предварительной аутентификации участвуют AM-FE обслуживающей сети и AM-FE целевой сети.

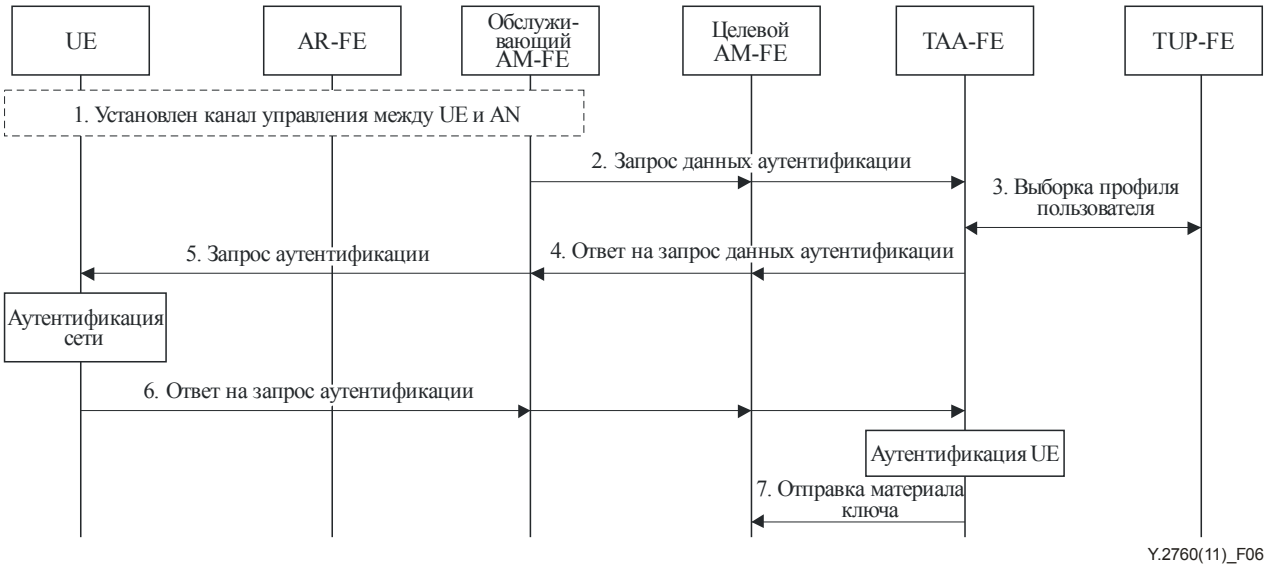

Рисунок 6 – Процедура предварительной аутентификации на основе одиночного сетевого соединения

1) Установлен канал управления между UE и функциями сети доступа (эта процедура не входит в сферу применения настоящей Рекомендации).

2) AM-FE отправляет запрос данных аутентификации, который включает информацию об абоненте, объекту TAA-FE. Запрос данных аутентификации пересылается AM-FE обслуживающей сети и AM-FE целевой сети.

3) TAA-FE осуществляет выборку профиля пользователя, взаимодействуя с TUP-FE.

4) TAA-FE отправляет ответ на запрос данных аутентификации, включая жетон аутентификации, объекту AM-FE целевой сети и объекту AM-FE обслуживающей сети.

5) AM-FE обслуживающей сети отправляет запрос аутентификации оборудованию UE. UE осуществляет выборку жетона аутентификации и выполняет аутентификацию сети с помощью собственной информации аутентификации. После успешного завершения аутентификации UE генерирует материал сеансового ключа.

6) UE отправляет ответ на запрос аутентификации объекту AM-FE обслуживающей сети. Обслуживающий AM-FE пересылает эту информацию, включая жетон аутентификации, целевым AM-FE и TAA-FE. TAA-FE извлекает жетон и выполняет аутентификацию UE. После успешного завершения аутентификации TAA-FE генерирует материал сеансового ключа, который при необходимости может использоваться для выработки материала подсеансового ключа.

7) TAA-FE отправляет материал ключа целевого AM-FE, который будет использоваться после выполнения UE передачи обслуживания в целевую сеть для защиты связи между UE и целевой сетью.

7.2.4 Междоменная аутентификация

Разные административные домены означают разных поставщиков СПП. Ниже описана процедура аутентификации для выполнения оборудованием UE передачи обслуживания между разными административными доменами.

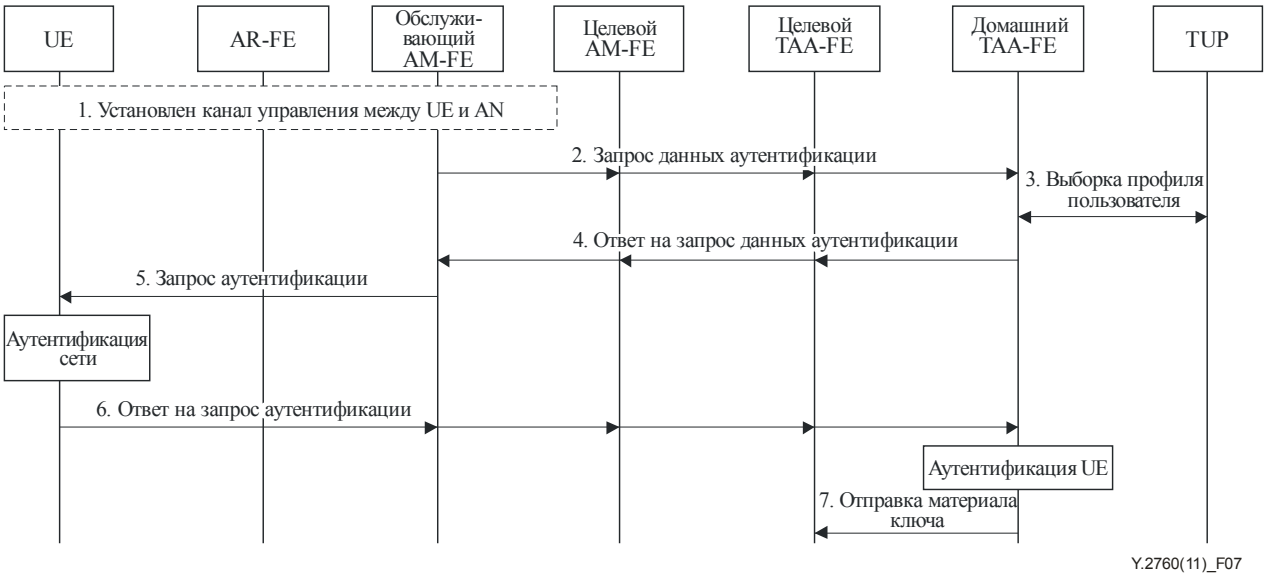

Рисунок 7 – Процедура аутентификации между разными доменами

1) Установлен канал управления между UE и функциями сети доступа (эта процедура не входит в сферу применения настоящей Рекомендации).

2) AM-FE обслуживающей сети отправляет запрос данных аутентификации, который включает информацию об абоненте, объекту TAA-FE домашней сети. Запрос данных аутентификации пересылается объектом AM-FE целевой сети и объектом TAA-FE целевой сети. TAA-FE домашней сети выполняет выборку профиля пользователя, взаимодействуя с TUP-FE.

3) TAA-FE осуществляет выборку профиля пользователя, взаимодействуя с TUP-FE.

4) TAA-FE домашней сети отправляет ответ на запрос данных аутентификации, включая жетон аутентификации, объекту AM-FE обслуживающей сети. Ответ на запрос данных аутентификации пересылается объектом TAA-FE целевой сети объекту AM-FE целевой сети.

5) AM-FE обслуживающей сети отправляет запрос аутентификации оборудованию UE. UE осуществляет выборку жетона аутентификации и выполняет аутентификацию сети с помощью собственной информации аутентификации. После успешного завершения аутентификации UE генерирует материал сеансового ключа.

6) UE отправляет ответ на запрос аутентификации, включая жетон аутентификации, объекту TAA-FE домашней сети. TAA-FE домашней сети извлекает жетон и выполняет аутентификацию UE. После успешного завершения аутентификации TAA-FE домашней сети генерирует материал сеансового ключа, который при необходимости может использоваться для выработки материала подсеансового ключа.

7) После успешного завершения аутентификации TAA-FE домашней сети отправляет объекту TAA-FE целевой сети материал ключа, который используется после выполнения UE передачи обслуживания из обслуживающей сети в целевую сеть для защиты связи между UE и целевой сетью.

7.2.5 Механизм отображения материала ключа в процессе аутентификации

Когда UE переходит из обслуживающей сети в целевую сеть, взаимная аутентификация и генерирование материала сеансового ключа выполнены. СПП поддерживает разные механизмы выработки ключа, и для координации материала ключа, используемого для разных механизмов выработки ключа, применяется отображение материала ключа.

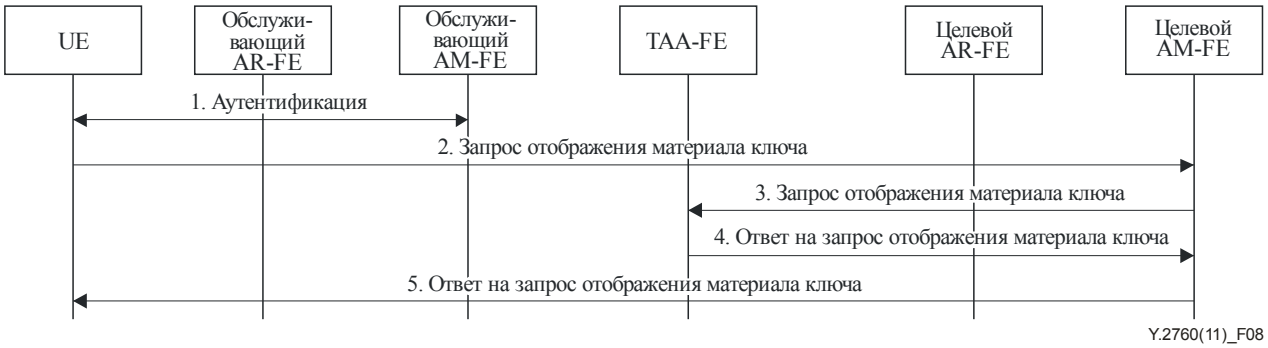

Рисунок 8 – Процедура отображения материала ключа

1) Установлено соединение между UE и TAA-FE, завершена процедура аутентификации и выполнено генерирование сеансового ключа.

2) UE определяет целевую сеть и подготавливает передачу обслуживания в целевую сеть. UE отправляет запрос отображения материала ключа объекту AM-FE целевой сети. Запрос отображения материала ключа включает информацию отображения, такую как текущий механизм выработки ключа и поддерживаемый механизм выработки ключа.

3) AM-FE целевой сети отправляет запрос отображения материала ключа объекту TAA-FE.

4) TAA-FE принимает запрос отображения материала ключа и выполняет отображение материала ключа в обслуживающей сети в материал ключа в целевой сети и отправляет ответ на запрос отображения материала ключа объекту AM-FE целевой сети.

5) AM-FE целевой сети отправляет запрос отображения оборудованию UE. UE выполняет отображение материала ключа в обслуживающей сети в материал ключа целевой сети в целевой сети. Материал целевого ключа в целевой сети является общим для UE и TAA-FE и используется для защиты трафика между UE целевой сетью.

7.2.6 Аутентификация при доступе к нескольким сетям

Аутентификация при доступе к нескольким сетям означает, что UE обладает возможностью осуществлять связь одновременно с несколькими сетями доступа. Если UE обладает возможностью доступа к нескольким сетям, UE соединяется с целевой сетью и выполняет процедуру взаимной аутентификации до отсоединения от обслуживающей сети. Взаимная аутентификация – это общая аутентификация, представленная на рисунке 3. После успешного завершения взаимной аутентификации UE и TAA-FE генерируют материал общего сеансового ключа, и TAA-FE отправляет материал сеансового ключа объекту AM-FE целевой сети. Когда UE перемещается в целевую сеть, трафик между UE и целевой сетью защищается материалом сеансового ключа или материалом его подключа.

7.2.7 Аутентификация при множественном соединении

Множественное соединение означает, что UE осуществляет одновременно подсоединение к нескольким сетям. Разные типы сетевых соединений могут обеспечиваться в случае разных интерфейсов с пользователями, например, большая ширина полосы, малое время задержек и высокий уровень безопасности. Случай множественных соединений с разными административными доменами не входит в сферу применения настоящей Рекомендации.

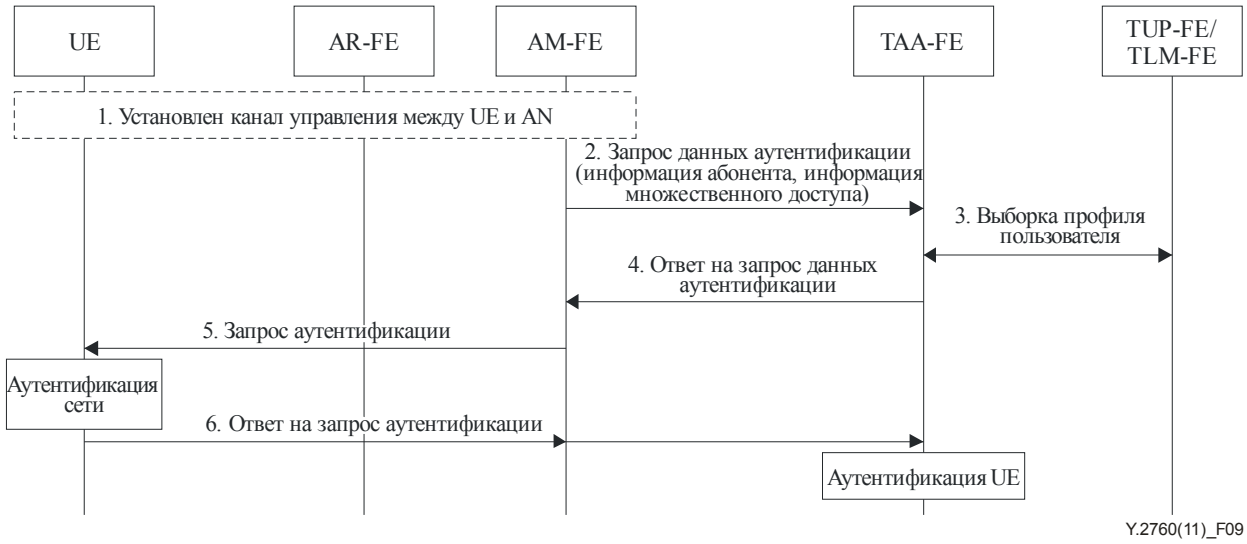

Рисунок 9 – Аутентификация при множественном соединении

1) Установлен канал управления между UE и функциями сети доступа (данная процедура не входит в сферу применения настоящей Рекомендации). UE получает информацию от сети доступа и индикацию о поддержке аутентификации при множественном доступе.

2) AM-FE отправляет запрос данных аутентификации объекту TAA-FE. Запрос данных аутентификации включает информацию UE, такую как информация об абоненте (например, идентификатор абонента пользователя); информацию множественного доступа (например, индикация множественного доступа и идентификатор интерфейса множественного доступа).

3) TAA-FE получает информацию аутентификации и взаимодействует с TUP-FE/TLM-FE для получения профиля пользователя и вектора аутентификации. Вектор аутентификации генерируется в TUP-FE/TLM-FE. Жетон аутентификации включается в вектор аутентификации.

4) TAA-FE отправляет запрос данных аутентификации, включая жетон аутентификации, объекту AM-FE.

5) AM-FE отправляет запрос аутентификации оборудованию UE. UE генерирует локальные жетоны аутентификации на основании информации аутентификации, содержащейся в сообщении запроса аутентификации. UE выполняет аутентификацию сети путем проверки валидации принятого жетона аутентификации в соответствии с локальными жетонами аутентификации. После успешного завершения аутентификации UE генерирует сеансовый ключ на основании информации аутентификации. Если установлена индикация множественного доступа, UE генерирует множественные материалы сеансовых ключей на основании информации о множественном доступе.

6) UE отправляет сообщение ответа на запрос аутентификации объекту AM-FE. AM-FE пересылает эту информацию, в том числе жетон аутентификации, сгенерированный UE, объекту TAA-FE. TAA-FE осуществляет выборку жетона аутентификации в сообщении ответа на запрос аутентификации и выполняет аутентификацию UE на основании вектора аутентификации в TAA-FE. После успешного завершения аутентификации TAA-FE генерирует материал сеансового ключа в соответствии с жетоном аутентификации. Если установлена индикация множественного доступа, TAA-FE генерирует множественные материалы сеансовых ключей на основании информации о множественном доступе.

8 Установление контекста безопасности

8.1 Передача контекста безопасности между AM-FE обслуживающей сети и AM-FE целевой сети

Следует обеспечивать защиту трафика передачи контекста безопасности между AM-FE обслуживающей сети и AM-FE целевой сети. Безопасность между обслуживающим AM-FE

и целевым AM-FE достигается путем установления ассоциации безопасности. Если два AM-FE находятся в пределах той же зоны, ассоциация безопасности не требуется. Если два AM-FE находятся в разных зонах, например в доменах разных операторов, ассоциация безопасности создается механизмом безопасности, а также на основании политики операторов и соглашения между ними.

8.2 Передача контекста безопасности между AR-FE обслуживающей сети и AR-FE целевой сети

Если UE выполняет передачу обслуживания между AR-FE обслуживающей сети и AR-FE целевой сети, трафик передачи контекста безопасности между целевым AR-FE и обслуживающим AR-FE должен быть защищен. Безопасность передачи контекста безопасности между обслуживающим AR-FE и целевым AR-FE достигается путем установления ассоциации безопасности.

8.3 Передача контекста безопасности между UE и HDC-FE

8.3.1 Передача контекста безопасности по инициативе хост-узла

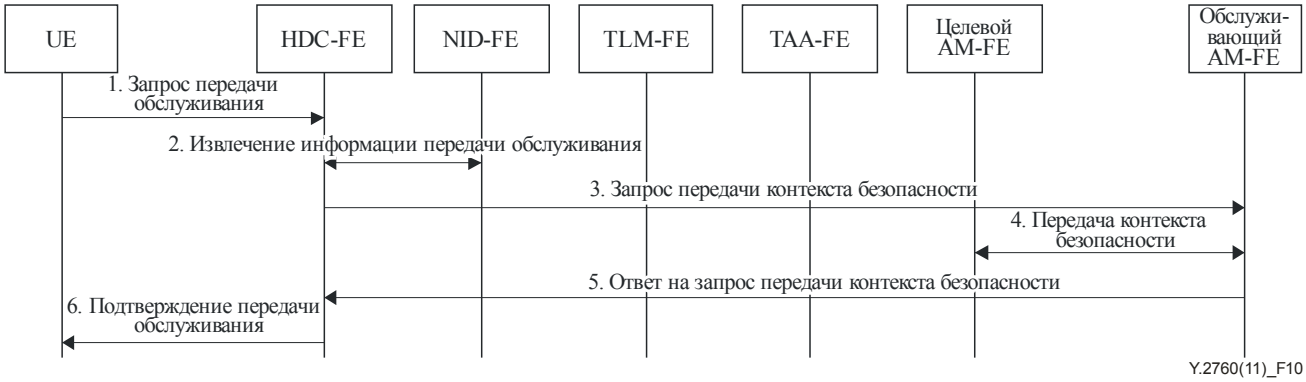

Рисунок 10 – Процедура передачи контекста безопасности по инициативе хост-узла

Если UE принимает решение осуществить передачу обслуживания от обслуживающей сети в целевую сеть, UE отправляет запрос передачи обслуживания объекту HDC-FE, который запускает передачу контекста безопасности. После завершения передачи контекста безопасности AM-FE целевой сети использует контекст безопасности для защиты трафика между UE и целевой сетью. Выполняются следующие шаги:

1) UE отправляет запрос передачи обслуживания объекту HDC-FE.
2) HDC-FE принимает запрос передачи обслуживания, взаимодействует с NID-FE для получения информации, относящейся к передаче обслуживания.
3) HDC-FE пересылает запрос передачи обслуживания, включая информацию, относящуюся к передаче обслуживания, объекту AM-FE обслуживающей сети.
4) Обслуживающий AM-FE взаимодействует с целевым AM-FE в целях передачи контекста безопасности.
5) По завершении передачи контекста безопасности обслуживающий AM-FE отправляет ответ на запрос передачи контекста безопасности объекту HDC-FE.
6) HDC-FE принимает ответ на запрос передачи контекста безопасности. Если передача контекста безопасности завершается успешно, HDC-FE отправляет подтверждение передачи обслуживания оборудованию UE.

8.3.2 Передача контекста безопасности по инициативе сети

Если HDC-FE принимает решение о приведении в действие UE для выполнения передачи обслуживания от обслуживающей сети в целевую сеть, HDC-FE отправляет сообщение начальной загрузки передачи обслуживания для запуска передачи контекста безопасности. После завершения передачи контекста безопасности AM-FE целевой сети использует контекст безопасности для защиты трафика между UE и целевой сетью.

Рисунок 11 – Процедура передачи контекста безопасности по инициативе сети

1) HDC-FE выполняет подготовку к процедуре передачи обслуживания и отправляет стартовое сообщение начальной загрузки передачи обслуживания объекту AM-FE обслуживающей сети для запуска передачи контекста безопасности.

2) AM-FE обслуживающей сети взаимодействует с AM-FE целевой сети в целях передачи контекста безопасности.

3) По завершении передачи контекста безопасности AM-FE обслуживающей сети отправляет объекту HDC-FE сообщение о завершении начальной загрузки передачи обслуживания.

4) По получении HDC-FE сообщения о завершении начальной загрузки передачи обслуживания он начинает процедуру передачи обслуживания путем отправки запроса передачи обслуживания оборудованию UE.

5) По завершении передачи обслуживания UE отправляет сообщение подтверждения передачи обслуживания.

9 Безопасность IP-мобильности

9.1 Безопасность мобильности на базе хост-узла

Требуется, чтобы защищался трафик управления мобильностью на безе хост-узла между UE и MLM-FE (C). Требуется создание ассоциации безопасности (SA) между UE и MLM-FE(C). SA между UE и MLM-FE (P) является необязательной.

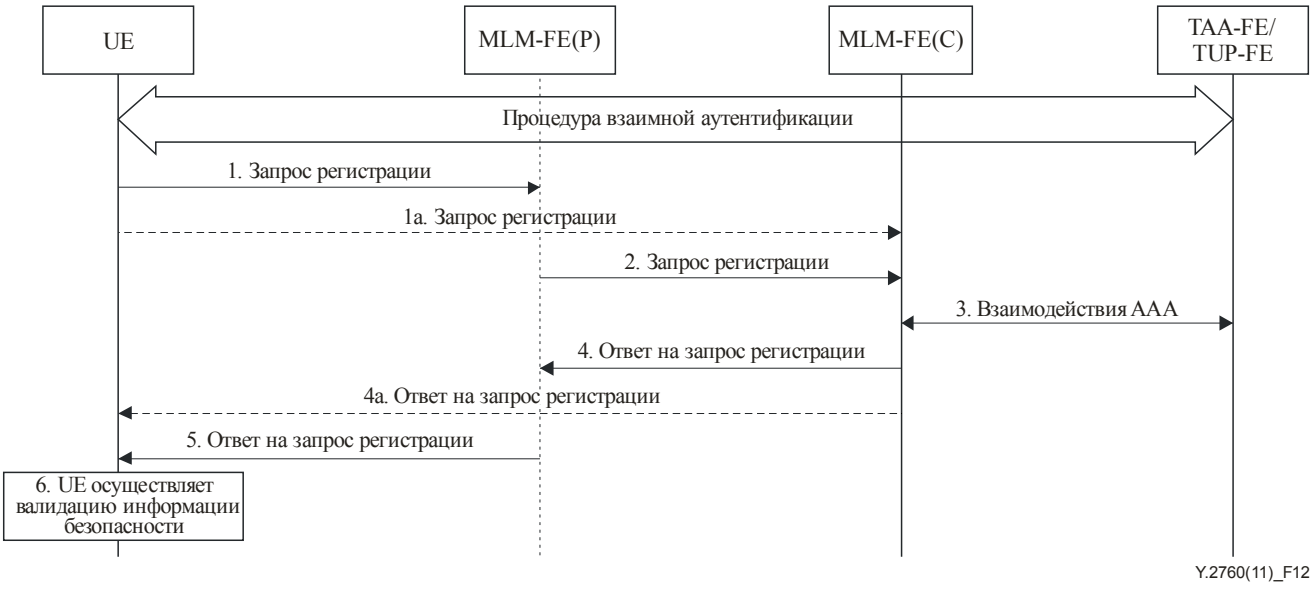

Рисунок 12 – Процедура безопасности мобильности на базе хост-узла

При исходном положении о том, что UE и TAA-FE завершили общую процедуру аутентификации, выполняются следующие шаги.

1) UE отправляет запрос регистрации объекту MLM-FE(P). Запрос регистрации включает информацию безопасности между UE и MLM-FE(C) и информацию безопасности между UE и MLM-FE(P).

   1a) Если MLM-FE(P) не существует, UE отправляет запрос регистрации напрямую объекту MLM-FE(C).

2) MLM-FE(P) осуществляет валидацию информации безопасности между UE и MLM-FE(P) и пересылает запрос регистрации объекту MLM-FE(C). До пересылки сообщения запроса регистрации MLM-FE(P) может добавить к нему информацию безопасности между MLM-FE(P) и MLM-FE(C).

3) MLM-FE(C) взаимодействует с TAA-FE/TUP-FE для получения информации аутентификации и информации авторизации.

4) MLM-FE(C) осуществляет валидацию информации безопасности между UE и MLM-FE(C) в запросе регистрации. MLM-FE(C) отправляет ответ на запрос регистрации и информацию безопасности объекту MLM-FE(P). Ответ на запрос регистрации может содержать информацию безопасности между UE и MLM-FE(C) и информацию безопасности между MLM-FE(P) и MLM-FE(C).

   4a) Если MLM-FE (P) не существует, MLM-FE(C) отправляет ответ на запрос регистрации напрямую UE. Ответ на запрос регистрации может включать информацию безопасности между UE и MLM-FE(C).

5) MLM-FE(P) осуществляет валидацию информации безопасности между MLM-FE(P) и MLM-FE(C) и отправляет ответ на запрос регистрации объекту UE. До пересылки сообщения ответа на запрос регистрации MLM-FE(P) может добавить к нему информацию безопасности между UE и MLM-FE(P).

6) MLM-FE(C) осуществляет валидацию информации безопасности между UE и MLM-FE(C) и создает SA между UE и MLM-FE(C). Если MLM-FE(P) существует, UE осуществляет валидацию информации безопасности между UE и MLM-FE(P) и создает SA между UE и MLM-FE(P).

9.2 Безопасность мобильности на базе сети

Защита трафика управления мобильностью на базе сети между двумя сетевыми объектами в доверенной зоне или доверенной, но уязвимой зоне, является необязательной и зависит от политики конкретного оператора. Механизмы безопасности для трафика управления мобильностью на основе сети базируются на механизме безопасности, представленном в [ITU-T Y.2704].

10 Безопасность между UE и HDC-FE

Поток информации между UE и HDC-FE используется для передачи информации, необходимой для принятия решения о передаче обслуживания. UE и HDC-FE должны установить ассоциацию безопасности для защиты информационного потока между UE и HDC-FE.

10.1 Установление ассоциации безопасности между UE и HDC-FE по инициативе хост-узла

Процедура установления ассоциации безопасности между UE и HDC-FE по инициативе хост-узла означает, что UE запускает процедуру создания ассоциации безопасности между UE и HDC-FE, которая отражена на рисунке 13. Существует два предварительных условиях для установления ассоциации безопасности между UE и HDC-FE. Во-первых, UE и TAA-FE имеют материал ключа, предварительно установленного общим. Материал ключа, предварительно установленного общим, может быть создан после процедуры взаимной аутентификации. Во-вторых, UE знает информацию HDC-FE, такую как адрес, с помощью которой UE отправляет запрос ассоциации безопасности объекту HDC-FE. Способ получения UE информации HDC-FE не входит в сферу применения настоящей Рекомендации. Для ретрансляции информации материала ключа к/от TAA-FE используется TLM-FE, который на следующем рисунке не показан.

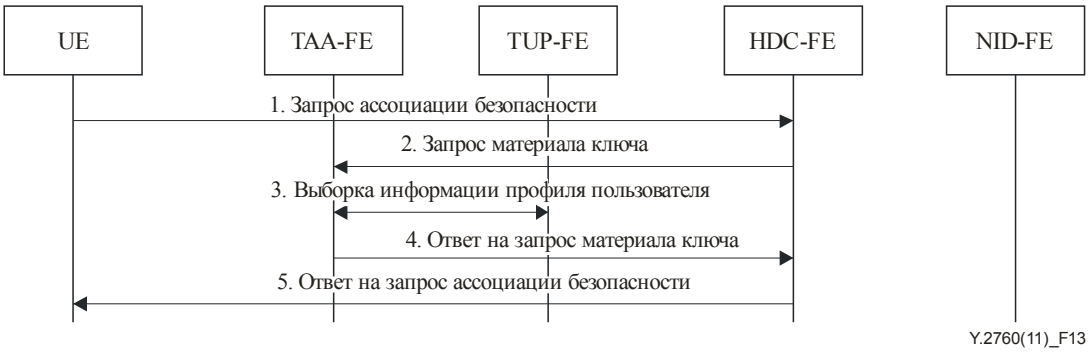

Рисунок 13 – Процедура установления ассоциации безопасности по инициации хост-узла

1) UE генерирует материал общего ключа для создания ассоциации с HDC-FE в соответствии с информацией аутентификацией, UE отправляет запрос ассоциации безопасности, включая информацию аутентификации и информацию UE, объекту HDC-FE.
2) HDC-FE отправляет запрос материала ключа объекту TAA-FE, включая информацию HDC-FE, информацию аутентификации и информацию UE.
3) TAA-FE осуществляет выборку информации профилей пользователей, взаимодействуя с TUP-FE, и проверяет, имеет ли HDC-FE разрешение на создание ассоциации безопасности с UE.
4) Если HDC-FE имеет разрешение на создание ассоциации безопасности с UE, TAA-FE генерирует материал ключа для HDC-FE в соответствии с информацией аутентификации, информацией HDC-FE и информацией UE. TAA-FE отправляет ответ, содержащий материал ключа, а также такую информацию, как материал ключа для HDC-FE, срок действия ключа, объекту HDC-FE.
5) HDC-FE отправляет ответ на запрос ассоциации безопасности для сообщения о том, что ассоциация безопасности между UE и HDC-FE установлена.

10.2 Установление ассоциации безопасности между UE и HDC-FE по инициативе сети

Процедура установления ассоциации безопасности по инициативе сети означает, что сторона сети запускает процедуру создания ассоциации безопасности между UE и HDC-FE, которая отражена на рисунке 14. Существует два предварительных условиях для установления ассоциации безопасности между UE и HDC-FE. Во-первых, UE и TAA-FE имеют материал ключа, предварительно установленного общим. Материал ключа, предварительно установленного общим, может быть создан после процедуры взаимной аутентификации. Во-вторых, HDC-FE знает информацию UE, такую как информация об абоненте или информация о местоположении, с помощью которой HDC-FE отправляет информацию ассоциации безопасности оборудованию UE. Способ получения UE информации для HDC-FE не входит в сферу применения настоящей Рекомендации.

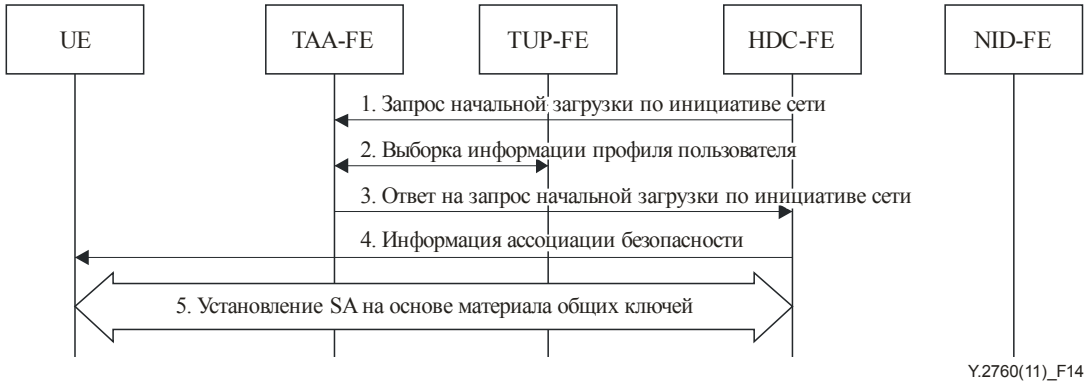

Рисунок 14 – Процедура установления ассоциации безопасности по инициативе сети

1) HDC-FE отправляет запрос начальной загрузки по инициативе сети, включая информацию HDC-FE и информацию UE, объекту TAA-FE.

2) TAA-FE осуществляет выборку информации профиля пользователя, взаимодействуя с TUP-FE, и проверяет, имеет ли HDC-FE разрешение на инициирование создания ассоциации безопасности с UE.

3) Если HDC-FE имеет разрешение на инициирование создания ассоциации безопасности с UE, TAA-FE генерирует материал ключа для HDC-FE в соответствии с информацией HDC-FE и информацией UE. TAA-FE отправляет ответ на запрос начальной загрузки по инициативе сети, а также такую информацию, как материал ключа для HDC-FE, срок действия ключа, объекту HDC-FE.

4) HDC-FE отправляет информацию ассоциации безопасности, включая информацию аутентификации, оборудованию UE для создания ассоциации безопасности.

5) UE генерирует материал ключа для HDC-FE в соответствии с информацией аутентификации в информации ассоциации безопасности и осуществляет валидацию информации ассоциации безопасности. Между HDC-FE и UE создается ассоциация безопасности.

10.3 Предварительное установление ассоциации безопасности между UE и HDC-FE на основе PKI

Процедура установления ассоциации безопасности между UE и HDC-FE на основе PKI представлена на рисунке 15. Предварительным условием для процедуры установления ассоциации безопасности между UE и HDC-FE является знание оборудованием UE информации HDC-FE, такой как адрес, с помощью которой UE отправляет запрос ассоциации безопасности объекту HDC-FE. Способ получения UE информации HDC-FE не входит в сферу применения настоящей Рекомендации.

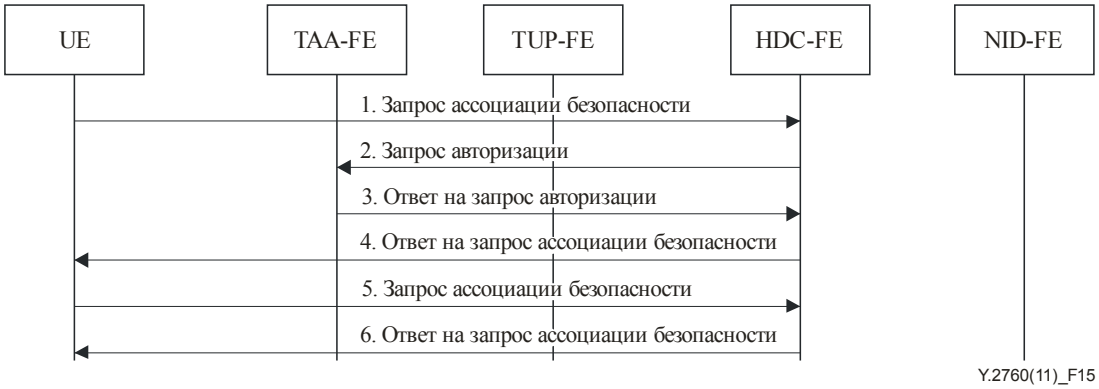

Рисунок 15 – Процедура установления ассоциации безопасности на основе PKI

1) UE отправляет запрос ассоциации безопасности, в том числе сертификат UE и информацию UE, объекту HDC-FE.

2) HDC-FE осуществляет валидацию сертификата UE и отправляет запрос авторизации, включая информацию UE и информацию HDC-FE, объекту TAA-FE.

3) TAA-FE проверяет авторизацию на основании информации UE и информации HDC-FE. Если UE имеет разрешение использовать HDC-FE, TAA-FE отправляет ответ на запрос авторизации, включая информацию авторизации и сертификат сервера, объекту HDC-FE.

4) HDC-FE принимает информацию авторизации и отправляет ответ на запрос ассоциации безопасности, включая сертификат сервера, оборудованию UE.

5) Если необходим материал общего ключа между UE и TAA-FE, TAA-FE отправляет информацию генерирования ключа оборудованию UE на шаге 4. UE генерирует материал общего ключа на основании принятой информации генерировании ключа и информации генерирования локального ключа. UE отправляет информацию генерирования локального ключа объекту HDC-FE.

6) HDC-FE генерирует материал ключа на основании принятой информации генерирования ключа и информации генерирования локального ключа. HDC-FE отправляет ответ на запрос ассоциации безопасности оборудованию UE. Устанавливается ассоциация безопасности между UE и HDC-FE.

11 Безопасность между UE и NID-FE

11.1 Установление ассоциации безопасности между UE и NID-FE по инициативе хост-узла

Процедура установления ассоциации безопасности между UE и NID-FE по инициативе хост-узла представлена на рисунке 16. Существует два предварительных условиях для установления ассоциации безопасности между UE и NID-FE: 1) UE и TAA-FE имеют материал общего ключа. Материал общего сеансового ключа может генерироваться после процедуры взаимной аутентификации. 2) UE знает информацию NID-FE, такую как адрес, с помощью которой UE отправляет запрос ассоциации безопасности объекту NID-FE. Способ получения UE информации NID-FE не входит в сферу применения настоящей Рекомендации.

Рисунок 16 – Установление ассоциации безопасности по инициативе хост-узла

1) UE отправляет запрос ассоциации безопасности объекту NID-FE.

2) NID-FE отправляет запрос материала ключа, включая информацию NID-FE и информацию UE, объекту TAA-FE. Если NID-FE не поддерживает отправку запроса аутентификации напрямую TAA-FE, NID-FE отправляет запрос аутентификации объекту TAA-FE через HDC-FE.

3) TAA-FE взаимодействует с TUP-FE и генерирует материал ключа для NID-FE.

4) TAA-FE отправляет ответ на запрос материала ключа, а также информацию аутентификации, объекту HDC-FE. Информация аутентификации включает материал общего ключа и его срок действия. Если TAA-FE не поддерживает отправку запроса аутентификации напрямую NID-FE, TAA-FE отправляет запрос аутентификации объекту NID-FE через HDC-FE.

5) NID-FE отправляет защищаемый общим ключом ответ на запрос ассоциации безопасности, в том числе информацию аутентификации, оборудованию UE.

6) UE генерирует материал общего ключа и осуществляет валидацию ответа на запрос ассоциации безопасности. Ассоциация безопасности создается объектом NID-FE и UE на основе материала общего ключа.

11.2 Установление ассоциации безопасности между UE и NID-FE по инициативе сети

Процедура установления ассоциации безопасности между UE и NID-FE по инициативе сети представлена на рисунке 17. Существует два предварительных условия для установления ассоциации безопасности между UE и NID-FE: 1) UE и TAA-FE имеют материал общего ключа. Материал общего сеансового ключа может генерироваться после процедуры взаимной аутентификации. 2) UE знает информацию NID-FE, такую как адрес, с помощью которой UE отправляет запрос ассоциации безопасности объекту NID-FE. Способ получения UE информации NID-FE не входит в сферу применения настоящей Рекомендации.

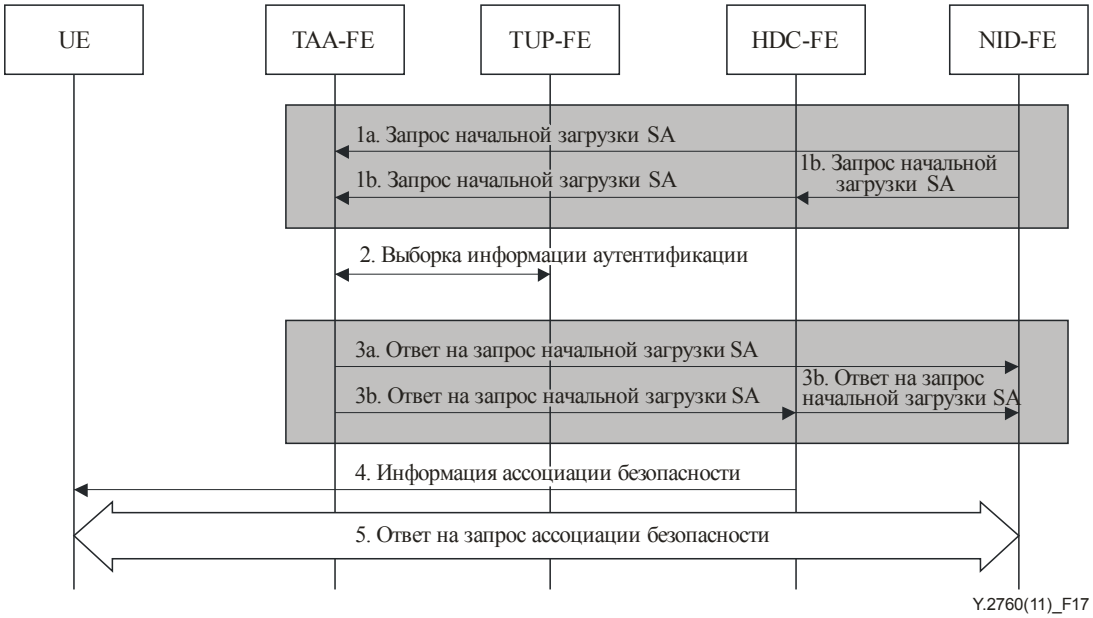

Рисунок 17 – Установление ассоциации безопасности по инициативе сети

1) NID-FE отправляет запрос начальной загрузки SA, включая информацию NID-FE, объекту TAA-FE. Если NID-FE не поддерживает отправки запроса начальной загрузки SA напрямую объекту TAA-FE, NID-FE отправляет запрос начальной загрузки SA объекту TAA-FE через HDC-FE.

2) TAA-FE взаимодействует с TUP-FE и генерирует материал ключа для NID-FE.

3) TAA-FE отправляет запрос начальной загрузки SA, включая информацию аутентификации, объекту NID-FE. Информация аутентификации включает материал ключа и его срок действия. Если TAA-FE не поддерживает отправки запроса начальной загрузки SA напрямую объекту NID-FE, TAA-FE отправляет запрос начальной загрузки SA объекту NID-FE через HDC-FE.

4) NID-FE отправляет информацию ассоциации безопасности, включая информацию аутентификации, оборудованию UE под защитой материала общего ключа.

5) UE генерирует материал общего ключа и осуществляет валидацию информации ассоциации безопасности. Ассоциация безопасности создается объектом NID-FE и UE на основе материала общего ключа.

11.3 Процедура установления ассоциации безопасности между UE и NID-FE на основании PKI

Процедура установления ассоциации безопасности между UE и NID-FE на основании PKI представлена на рисунке 18. Предварительное условие для установления ассоциации безопасности между UE и NID-FE заключается в том, что UE знает информацию NID-FE, такую как адрес, с помощью которой UE отправляет запрос ассоциации безопасности объекту NID-FE. Способ получения UE информации NID-FE не входит в сферу применения настоящей Рекомендации.

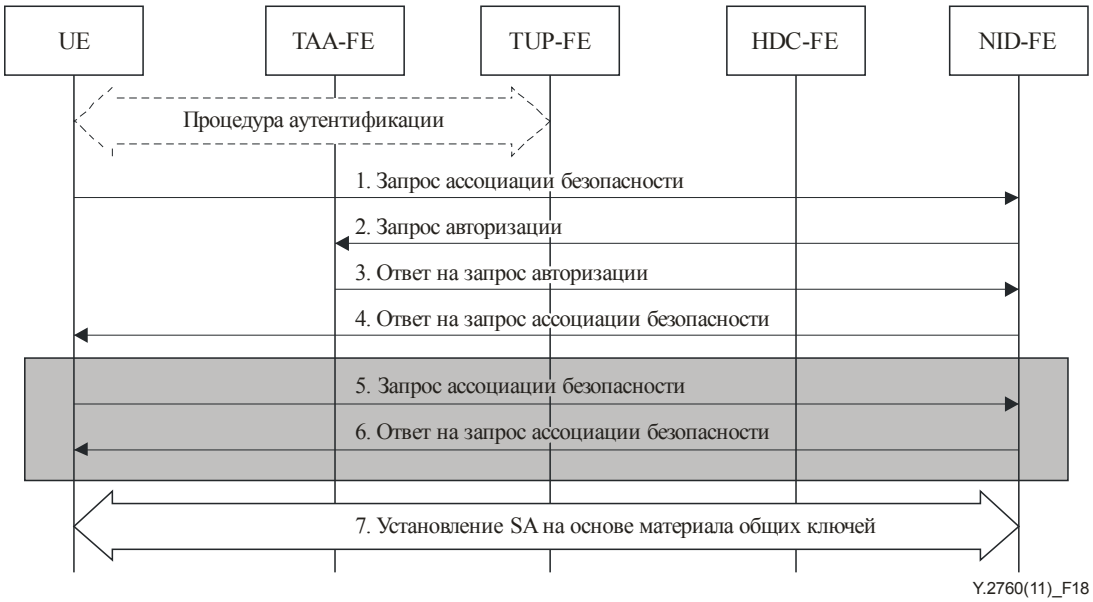

Рисунок 18 – Процедура установления ассоциации безопасности на основе PKI

По завершении процедуры аутентификации между TUP-FE и TAA-FE, выполняются следующие шаги.

1) UE отправляет запрос ассоциации безопасности, в том числе сертификат UE и информацию UE, объекту NID-FE.

2) NID-FE осуществляет валидацию сертификата UE и отправляет запрос авторизации, включая информацию UE и информацию NID-FE, объекту TAA-FE.

3) TAA-FE проверяет авторизацию на основании информации UE и информации NID-FE. Если UE имеет разрешение использовать NID-FE, TAA-FE отправляет ответ на запрос авторизации, включая информацию авторизации и сертификат сервера, объекту NID-FE.

4) NID-FE принимает информацию авторизации и отправляет ответ на запрос ассоциации безопасности, включая сертификат сервера, оборудованию UE.

5) Если необходим материал общего ключа между UE и TAA-FE, TAA-FE отправляет информацию генерирования ключа оборудованию UE на шаге 4. UE генерирует материал общего ключа на основании принятой информации генерирования ключа и информации генерирования локального ключа. UE отправляет информацию генерирования локального ключа объекту NID-FE в качестве части запроса ассоциации безопасности.

6) NID-FE генерирует материал ключа на основании принятой информации генерирования ключа и информации генерирования локального ключа. NID-FE отправляет ответ на запрос ассоциации безопасности оборудованию UE.

7) Устанавливается ассоциация безопасности между UE и NID-FE.

12 Безопасность для функций транспортирования

12.1 Безопасность между UE и функциональным объектом узла доступа

Трафик между UE и AN-FE следует защищать. Ассоциация безопасности между UE и AN-FE основана на материале общего ключа. Если процедура аутентификации между UE и TAA-FE завершается успешно, UE и TAA-FE генерируют материал ключа, такой как сеансовый ключ, для защиты трафика между UE и AN-FE. TAA-FE отправляет материал ключа объекту AN-FE через AM-FE, AR-FE.

12.2 Безопасность между UE и L3HEF (функция передачи обслуживания уровня 3)

Трафик между UE и L3HEF следует защищать. Ассоциация безопасности между UE и L3HEF основана на материале заранее определенного общим ключа. Если процедура аутентификации завершается успешно, UE и TAA-FE генерируют материал ключа, такой как сеансовый ключ, для защиты трафика между UE и L3HEF. L3HEF получает материал ключа напрямую от TAA-FE. L3HEF также получает материал ключа от TAA-FE через AM-FE или HDC-FE.

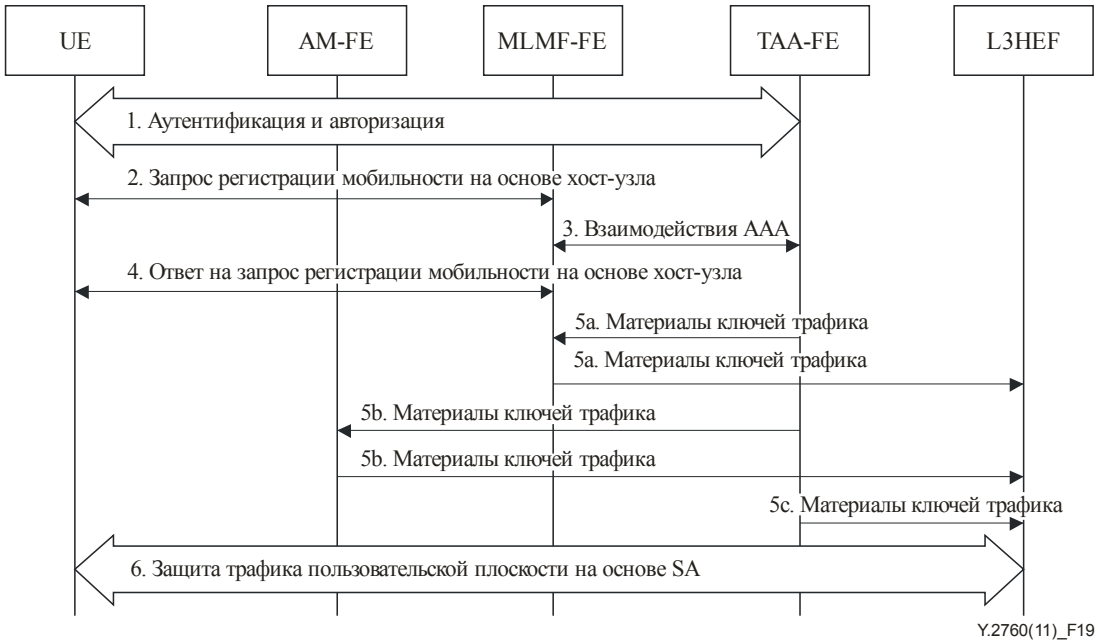

Рисунок 19 – Процедура безопасности трафика пользовательской плоскости между UE и L3HEF

1) Установлено соединение между UE и TAA-FE. После завершения взаимной аутентификации UE и TAA-FE имеют материал общего ключа, такой как материал переходного ключа и материал сеансового ключа.

2) UE отправляет объекту MLM-FE запрос регистрации мобильности на базе хост-узла в целях создания ассоциации безопасности мобильности хост-узла.

3) MLM-FE получает материал ключа, взаимодействуя с TAA-FE. MLM-FE выполняет аутентификацию UE на основе материала ключа. После успешного завершения аутентификации MLM-FE создает ассоциацию безопасности с UE на основе материала ключа.

4) MLM-FE отправляет ответ на запрос регистрации мобильности на базе хост-узла оборудованию UE. UE выполняет валидацию сообщения ответа на запрос регистрации мобильности на базе хост-узла и создает ассоциацию безопасности с MLM-FE.

5) После создания ассоциации безопасности между UE и MLM-FE складываются три ситуации.

   5a) TAA-FE генерирует материал ключа трафика и отправляет материал ключа трафика объекту L3HEF через MLM-FE.

   5b) TAA-FE генерирует материал ключа трафика и отправляет материал ключа трафика объекту L3HEF через MLM-FE и AM-FE.

   5c) TAA-FE отправляет материал ключа трафика напрямую L3HEF.

6) L3HEF использует материал ключа трафика для защиты трафика пользовательской плоскости между UE и L3HEF.

Дополнение I

(Настоящее Дополнение составляет неотъемлемую часть данной Рекомендации.)

I.1 Пример процедуры полной аутентификации

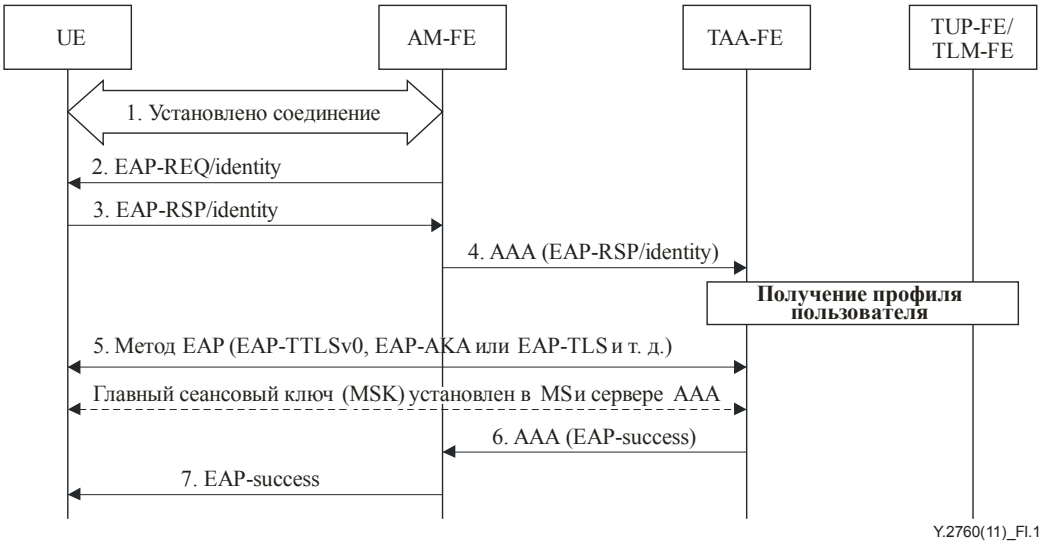

Рисунок I.1 – Процедура полной аутентификации

ПРИМЕЧАНИЕ. – Идентичность на шаге 2–4 означает идентичность UE.

Начальная загрузка для аутентификации представлена на рисунке I.1.

1) Установлено соединение между UE и AM-FE.
2) AM-FE отправляет запрос EAP/Идентичность – (EAP-REQ)/Identity – оборудованию UE [b-IETF RFC 3748].
3) UE отправляет сообщение ответа (EAP-RSP)/Identity.
4) AM-FE пересылает EAP-RSP/Identity к TAA-FE; после этого TAA-FE обменивается информацией с TUP-FE/TLM-FE, а объект TUP-FE/TLM-FE отправляет информацию пользователя, включая профиль, объекту TAA-FE.
5) Процесс выработки и распределения ключа выполняется в TAA-FE и UE. Может рассматриваться ряд методов, например EAP-TTLS, EAP-AKA, EAP-TLS и т. д.
6) TAA-FE отправляет сообщение об успешном EAP – EAP-Success – объекту AM-FE.
7) AM-FE сообщает оборудованию UE об успешной аутентификации с помощью сообщения EAP-Success. Теперь процесс обмена ключами на основе EAP успешно выполнен, и UE и AM-FE совместно используют материал ключа, выработанный в ходе этого обмена.

I.2 Пример процедуры быстрой повторной аутентификации

После осуществления передачи обслуживания непрерывность обслуживания с малыми задержками может поддерживать быстрая повторная аутентификация. Для быстрой повторной аутентификации необходимо использование идентификатора быстрой повторной аутентификации и нет необходимости в обмене информацией об аутентификации между TAA-FE и TUP-FE/TLM-FE.

Ниже представлена общая процедура быстрой повторной аутентификации.

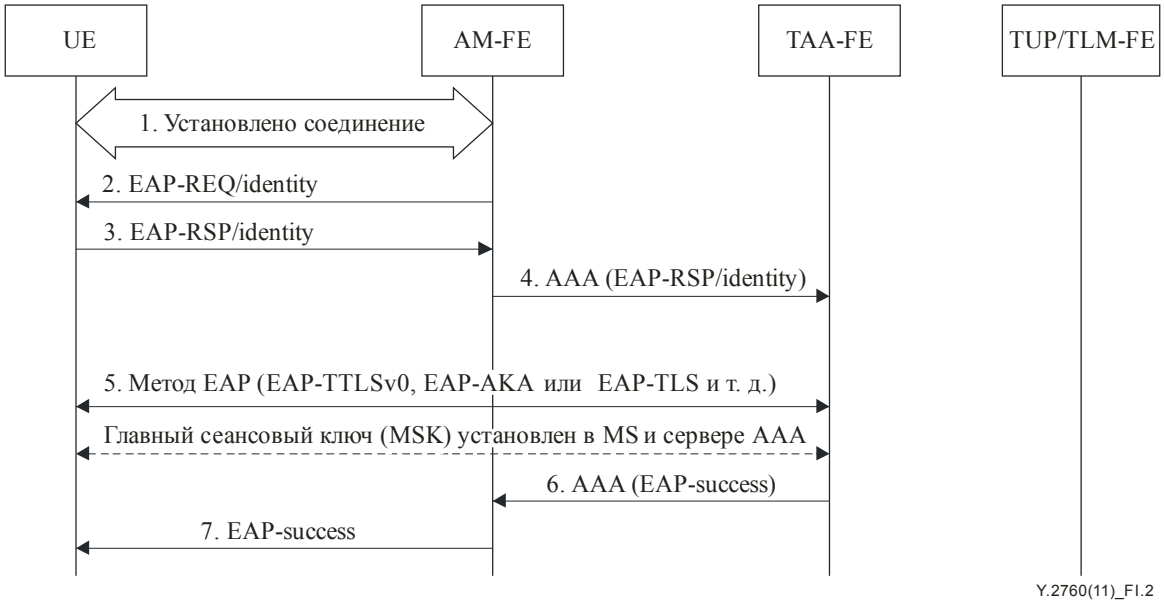

Рисунок I.2 – Процедура быстрой повторной аутентификации

1) Установлено соединение между UE и AM-FE.

2) AM-FE отправляет запрос EAP-REQ/Identity оборудованию UE, в котором содержится идентификатор повторной аутентификации.

3) UE отправляет ответное сообщение EAP Response/Identity.

4) AM-FE пересылает ответ EAP-RSP/Identity к TAA-FE.

5) Выполняется процесс выработки и распределения ключа. Могут рассматриваться несколько методов, например EAP-AKA, EAP-TLS и т. д.

6) TAA-FE отправляет объекту AM-FE сообщение об успешном выполнении EAP-Success.

7) AM-FE сообщает оборудованию UE об успешной аутентификации с помощью сообщения EAP-Success. Теперь процесс обмена ключами на основе EAP успешно выполнен, и UE и AM-FE I совместно используют материал ключа, выработанный в ходе этого обмена.

I.3 Пример мобильности на базе хост-узла

Для MIPv4 безопасность IP-мобильности базируется на расширениях аутентификации MIP, которые определены в [b-IETF RFC 3344]. Сообщения сигнализации IP-мобильности должны защищаться между UE и узлом, действующим в качестве HA (то есть MLM-FE), используя расширения аутентификации MIP, и необязательно защищаются сообщения между UE и узлом, действующим в качестве FA (то есть MLM-FE).

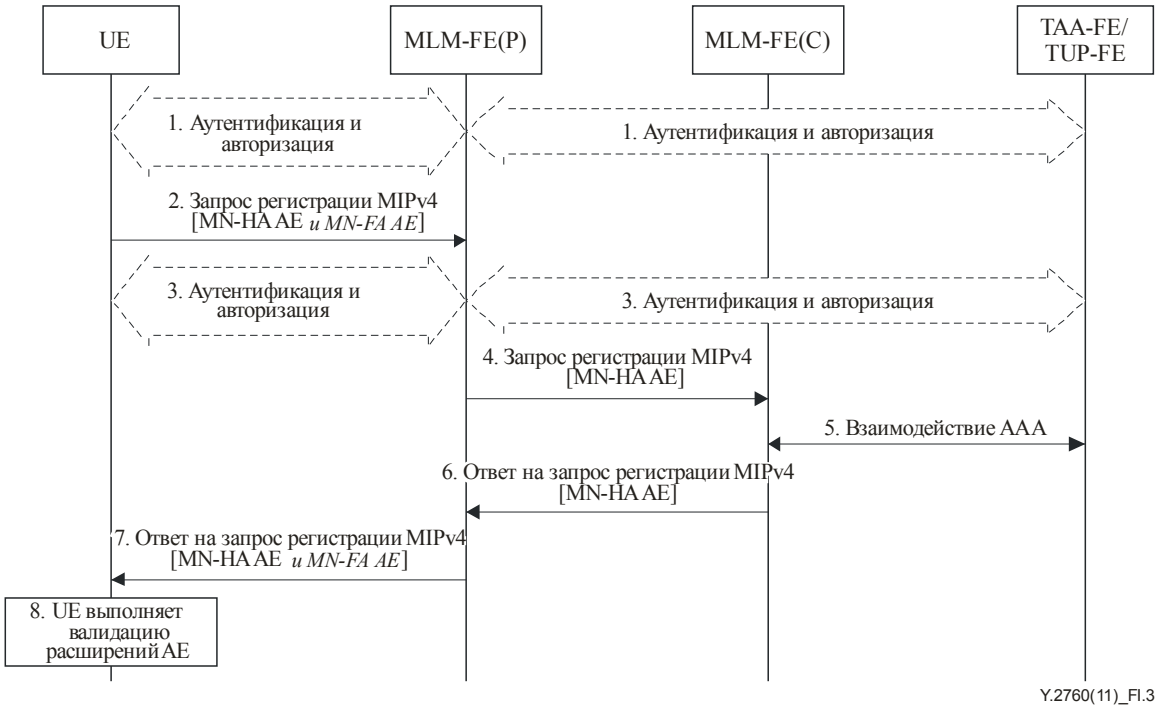

Рисунок I.3 – Процедура начальной загрузки MIPv4

Процедура начальной загрузки MIPv4, представленная на рисунке I.3, заключается в следующем.

1) Между UE и MLM-FE с помощью TAA-FE/TUP-FE создаются процессы аутентификации и авторизации.

2) UE отправляет сообщение запроса регистрации (RRQ) к агенту FA (MLM-FE). UE включает расширение аутентификации (AE) MN-HA и факультативно включает расширение аутентификации (AE) MN-FA, согласно определению в [b-IETF RFC 3344].

3) RRQ запускает процедуру аутентификации доступа.

4) FA обрабатывает сообщение согласно [b-IETF RFC 3344] и осуществляет валидацию расширения аутентификации MN-FA, если таковое представлено. Далее FA пересылает сообщение RRQ агенту HA(MLM-FE).

5) Избранный MLM-FE получает информацию аутентификации и авторизации от TAA-FE/TUP-FE.

6) MLM-FE осуществляет валидацию расширения аутентификации MN-HA. После успешной валидации расширения аутентификации MLM-FE отправляет ответ на запрос регистрации (RRP) оборудованию UE через FA.

7) FA обрабатывает RRP в соответствии с [b-IETF RFC 3344]. Далее FA пересылает сообщение RRP оборудованию UE. FA включает расширение аутентификации MN-FA, если FA принял расширение аутентификации MN-FA в сообщении RRQ.

8) UE осуществляет валидацию расширения аутентификации MN-HA и расширения аутентификации MN-FA, если таковое представлено.

Библиография

[b-IETF RFC 3220] IETF RFC 3220 (2002), *IP Mobility Support for IPv4*.

[b-IETF RFC 3344] IETF RFC 3344 (2002), *IP Mobility Support for IPv4*.

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)*.

[b-IETF RFC 3775] IETF RFC 3775 (2004), *Mobility Support in IPv6*.

[b-IETF RFC 4555] IETF RFC 4555 (2006), *IKEv2 Mobility and Multihoming Protocol (MOBIKE)*.

[b-IETF RFC 5213] IETF RFC 5213 (2008), *Proxy Mobile IPv6*.

[b-3GPP TS 33.102] 3GPP TS 33.102 V7.1.0 (2007), *3G Security: Security Architecture*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	**Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений**
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2012 г.