Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2703

(01/2009)

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

Сети последующих поколений – Безопасность

Применение услуги AAA в СПП

Рекомендация МСЭ-Т Y.2703

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	
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

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

Рекомендация МСЭ-Т Y.2703

Применение услуги AAA в СПП

Резюме

В Рекомендации МСЭ-Т Y.2703 обусловливается применение аутентификации, авторизации и учета (AAA) в СПП варианта 1.

Источник

Рекомендация МСЭ-Т Y.2703 утверждена 23 января 2009 года 13-й Исследовательской комиссией МСЭ-Т (2009–2012 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

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 извещения 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.2703

Применение услуги AAA в СПП

1 Сфера применения

В настоящей Рекомендации описывается применение аутентификации, авторизации и учета (AAA) для сетей последующих поколений (СПП) на основе [b-ITU-T Y.2201] "Требования к СПП версии 1", [b-ITU-T Y.2012] "Функциональные требования и архитектура СПП версии 1 (FRA)", [b-ITU-T Y.2701] "Требования к безопасности для СПП версии 1" и [b-ITU-T Y.2702] "Аутентификация СПП". Настоящая Рекомендация применяется к процессу аутентификации, авторизации и учета при доступе к СПП с использованием клиента AAA и сервера AAA. В частности, в настоящей Рекомендации функция учета рассматривается только с точки зрения ее вклада в учет в системе безопасности.

Сфера применения настоящей Рекомендации является следующей:

1) процесс регистрации;
2) функции и процедуры аутентификации;
3) функции и процедуры авторизации;
4) функции и процедуры учета в системе безопасности.

2 Справочные документы

Нет.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 аутентификация (authentication) [b-ITU-T X.811]: Обеспечение гарантии заявленной идентичность объекта.

3.1.2 сертификат аутентификации (authentication certificate) [b-ITU-T X.811]: Сертификат безопасности, гарантированный органом аутентификации, который может использоваться для гарантирования идентичность объекта.

3.1.3 аутентификационная информация (authentication information) [b-ITU-T X.811]: Информация, используемая для целей аутентификации.

3.1.4 авторизация (authorization) [b-ITU-T X.800]: Предоставление прав, которое включает предоставление доступа на основании прав доступа.

3.1.5 заявитель (claimant) [b-ITU-T X.811]: Объект, который является администратором доступа или представляет его для целей аутентификации. Заявитель обладает функциями, необходимыми для участия в аутентификационных обменах от имени администратора доступа.

3.1.6 данные проверки безопасности (security audit trail) [b-ITU-T X.800]: Данные, которые собраны и могут использоваться для содействия проверке безопасности.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяется следующий термин:

3.2.1 учет в системе безопасности (security accounting): Роль, с помощью которой отслеживаются связанные с безопасностью действия или события, которые могут быть включены в качестве ресурсов в функцию проверки безопасности.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения:

AAA	Authentication, Authorization and Accounting		Аутентификация, авторизация и учет
AM-FE	Access Management Functional Entity		Функциональный объект управления доступом
ANI	Application-to-Network Interface		Интерфейс "приложение-сеть"
EAP	Extensible Authentication Protocol		Расширяемый протокол аутентификации
ID	Identity – as defined by the network, service, or entity being accessed		Идентичность, как она определяется сетью, услугой или объектом, к которым осуществляется доступ
NAS	Network Access Server		Сервер сетевого доступа
NGN	Next Generation Network	СПП	Сеть последующего поколения
NNI	Network to Network Interface		Интерфейс "сеть-сеть"
NP	Network Provider		Поставщик доступа к сети
OAMP	Operations Administration Maintenance and Provision		Эксплуатация, администрирование, техническое обслуживание и обеспечение
RACF	Resource Access Control Function		Функция управления доступом к ресурсам
SCTP	Stream Control Transport Protocol		Транспортный протокол управления потоком
SR	Service Resource		Ресурс услуги
TAA-FE	Transport Authentication and Authorization Functional Entity		Функциональный объект аутентификации и авторизации транспорта
TE	Terminal Equipment		Оконечное оборудование
TUP-FE	Transport User Profile Functional Entity		Функциональный объект профиля пользователя транспорта
UNI	User-to-Network Interface		Интерфейс "пользователь-сеть"

5 Условные обозначения

Нет.

6 Общие концепции для услуги AAA

В настоящем разделе рассматриваются базовые концепции AAA.

6.1 Обзор

Услуга по аутентификации, авторизации и учету обеспечивает функции, с помощью которых проверяется идентичность пользователя (аутентификация), предоставляется доступ к услугам (авторизация), а также средства, с помощью которых измеряется потребление ресурсов (учет).

6.2 Процесс AAA

Отдельные процессы в рамках структуры AAA являются следующими:

При аутентификации выполняется валидация идентичности конечного пользователя до того, как ему предоставляется доступ к сети. Конечный пользователь предъявляет набор регистрационных данных, таких как комбинация имени пользователя/пароля, ключ защиты, сертификат или биометрические данные (например, отпечатки пальцев). Как правило, такие регистрационные данные согласовываются во время процесса регистрации. Верификация регистрационных данных приводит к процессу авторизации.

При авторизации определяются привилегии и услуги, которые предоставляются конечному пользователю, как только ему разрешен доступ к сети. Этот процесс должен включать предоставление адреса IP или применение фильтра для определения того, какие приложения или протоколы поддерживаются. И аутентификация, и авторизация осуществляются в среде, управляемой с помощью AAA.

Учет обеспечивает методику для сбора информации о потреблении ресурсов конечного пользователя, которая затем может обрабатываться для целей выставления счетов, аудита и планирования мощности. Некоторые учетные данные имеют отношение к разработке данных проверки безопасности.

Эти три процесса объединены в набор функций, которые совместно обеспечивают управление доступом.

6.3 Процедура AAA

Система услуги AAA состоит из сервера AAA и клиента AAA.

Сервер AAA имеет доступ к базе данных профилей пользователей и данным конфигурации. Для предоставления распределенных услуг AAA он связывается с клиентами AAA на основе сетевых компонентов, таких как NAS (сервер сетевого доступа) и маршрутизаторы.

Сценарии услуг AAA сводятся к следующим этапам:

- Конечный пользователь подключается к входному устройству и запрашивает доступ к сети.
- Клиент AAA направляет регистрационную информацию по идентичности/аутентификации конечного пользователя серверу AAA.
- Сервер AAA аутентифицирует пользователя на основе полученной регистрационной информации. Если аутентификация проходит успешно, то затем сервер определяет, какая услуга (услуги) разрешена, и направляет клиенту AAA ответ "принято/отклонено" и другие соответствующие данные.
- Клиент AAA уведомляет конечного пользователя о том, что доступ к указанным ресурсам предоставлен или отклонен.

Для сбора и хранения записей во время установления и завершения соединения клиент AAA посылает серверу AAA учетное сообщение.

7 Прикладная модель аутентификации и авторизации в СПП

Настоящая Рекомендация основана на требованиях к безопасности для СПП, установленных в [b-ITU-T Y.2701], и эталонной модели аутентификации в СПП, представленной в [b-ITU-T Y.2702]. В эталонной модели аутентификации в СПП (рисунок 7-1) показаны восемь эталонных точек для аутентификации; три из них рассматриваются/учитываются в настоящей Рекомендации.

Такими точками являются:

1) доступ пользователя к сети;

2) доступ пользователя к предоставляемой сетью услуге;

4) доступ поставщика услуги к получающему ее пользователю.

Эталонные точки (1) и (4) относятся к транспорту трафика пользователя и могут рассматриваться как зависящие от "горизонтального" управления доступом на уровне управления транспортом, тогда как эталонные точки (2) и (8) могут рассматриваться как зависящие от данных управления на уровнях управления транспортом и услугой и поэтому считаться "вертикальными". Такая зависимость показана на рисунке 7-2.

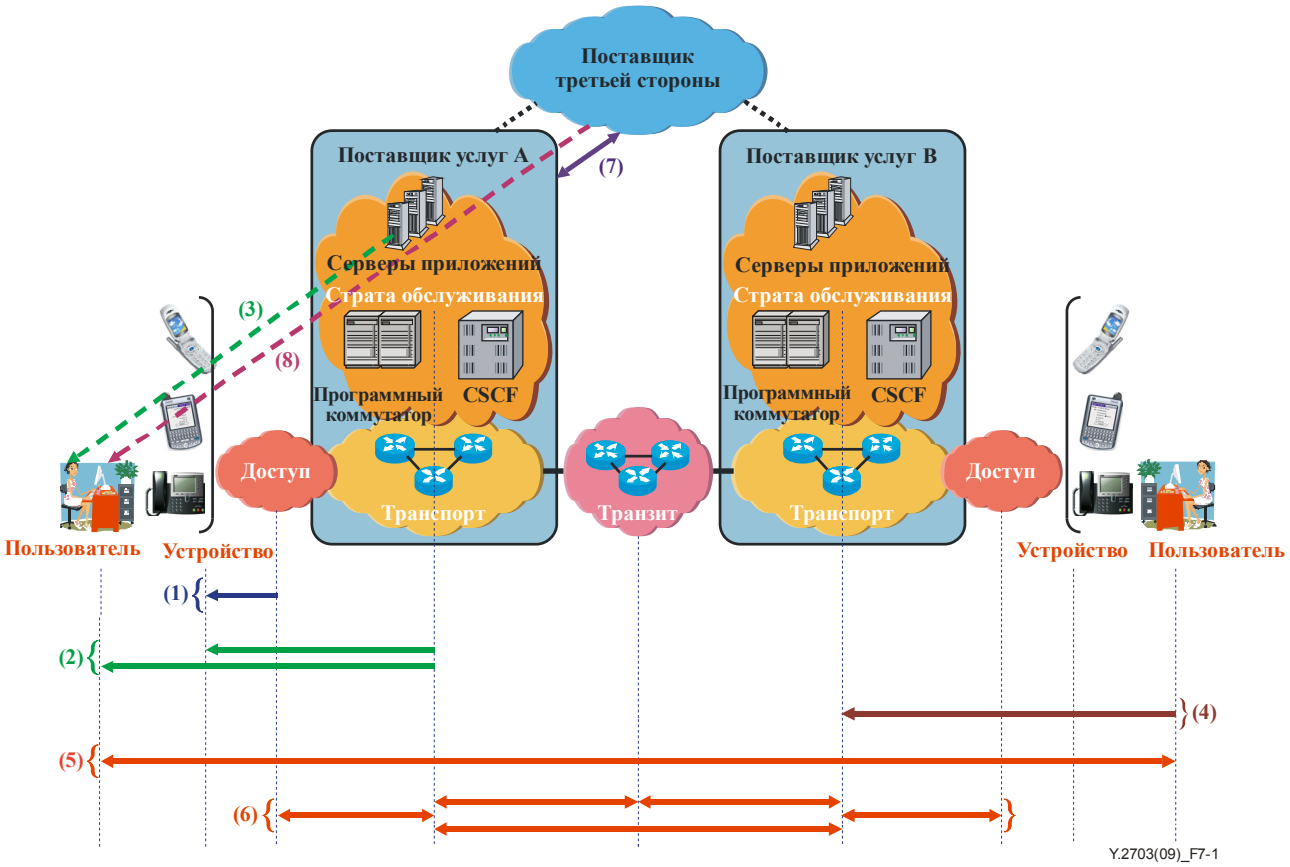

Рисунок 7-1 – Сквозная эталонная модель архитектуры (Y.2702 "Аутентификация в СПП")

Рисунок 7-2 – Архитектура СПП и соответствующие домены ААА (Y.2702 "Аутентификация в СПП")

8 Архитектура ААА в СПП

В этом разделе описывается взаимосвязь между эталонной моделью ААА и моделью функциональной архитектуры, описанной в [b-ITU-T Y.2012].

8.1 Доступ "пользователь-сеть"

Рисунок 8-1 – Аутентификация и авторизация пользователя для доступа к сети

На рисунке 8-1 показано приложение AAA для пользователя с целью доступа к сети (т. е. приложение типа 1 на рисунке 7-1, выше).

Как только объект в функциях управления транспортом (как правило, T-14 AM-FE) обнаруживает запрос на установление соединения от терминала пользователя, он начинает действовать как клиент AAA. Он запрашивает объекты в функциях управления транспортом, которые играют роль сервера AAA (такие как T-11 TAA-FE и T-12 TUP-FE), для аутентификации пользователя и авторизации для использования ресурсов СПП. Для этой процедуры запросов и ответов могут использоваться такие протоколы, как RADIUS или Diameter. На основе запроса от клиента AAA сервер AAA аутентифицирует пользователя с помощью явных (например, EAP) или неявных (например, аутентификация линии доступа) процедур. После успешной авторизации пользователя в зависимости от профиля пользователя (обычно управляемого с помощью TUP-FE) сервер AAA запрашивает RACF для резервирования и распределения ресурсов СПП этому пользователю. Как только RACF предоставлена, сервер AAA уведомляет клиента AAA о том, что получено разрешение на подключение оборудования этого пользователя.

8.2 Подключение услуги "пользователь-сеть"

Рисунок 8-2 – Аутентификация и авторизация пользователя для доступа к услуге

На рисунке 8-2 показано приложение AAA для пользователя с целью доступа к услуге (т. е. приложение типа 2 на рисунке 7-1, выше).

Аналогичному тому, как это происходит в предыдущем случае, показанном на рисунке 8-1, клиент AAA в функциях управления услугами (как правило, S-1 S-CES-FE) обнаруживает запрос на установление соединения от терминала пользователя. Он запрашивает сервер AAA (такой, как S-5 SUP-FE или S-6 SAA-FE) для аутентификации и авторизации запрашиваемой услуги. Услуга, которая основана на запросе на услугу, либо предоставляется, либо отклоняется, в зависимости от результатов аутентификации и авторизации.

Как только пользователь подключен к сети или услуге, каждый клиент AAA доводит до своего сервера AAA информацию о ресурсах СПП, потребленных пользователем, для помощи серверу AAA в сборе учетной информации, связанной с этим пользователем.

8.3 Аутентификация и авторизация пользователя для доступа к услуге третьей стороны

В СПП варианта 1 не рассматриваются услуги третьей стороны, доступные с помощью ANI. Следовательно, аутентификация и авторизация пользователя для доступа к услугам третьей стороны не входит в сферу охвата настоящей Рекомендации. В настоящей Рекомендации не показана эталонная модель для услуг третьей стороны. Однако сценарий использования, иллюстрирующий аутентификацию и авторизацию услуги третьей стороны, описывается в Дополнении III.

9 Регистрация

Необходимым условием для AAA является идентификация объекта, который должен быть аутентифицирован, например пользователя или устройства. Регистрационные данные, которые идентифицируют объект, устанавливаются с помощью процесса регистрации, при котором создается уникальная идентичность пользователя/устройства. Регистрационные данные также используются в процессе аутентификации в каждом случае, когда запрашивается доступ к услуге (услугам). Процесс регистрации может включать согласие с положениями и условиями, а также финансовые договоренности. Хотя первоначальная проверка идентичности и регистрационных данных называется регистрацией, последующий доступ к услугам и проверка регистрационных данных известны как прием в систему. Точные условия регистрации будут зависеть от политики поставщиков, характера услуг и т. д.

10 Аутентификация

В настоящей Рекомендации используются базовые концепции аутентификации, описанные в [b-ITU-T X.811]. Для уменьшения угроз, связанных с попытками получения несанкционированного доступа, требуются услуги и возможности по аутентификации для доступа к сетям и услугам. Дополнительная информация по цифровому сертификату приводится в Дополнении II.

10.1 Объекты аутентификации

Термин "заявитель" используется для описания любого объекта, который запрашивает аутентификацию. Заявитель обладает функциями, необходимыми для участия в аутентификационных обменах.

Клиент AAA обеспечивает специальную функцию, которая является частью пути доступа в систему между заявителем и проверяющим объектом для каждого запроса на доступ, и обеспечивает выполнение решения, принятого верификатором.

В среде, управляемой AAA, сервер AAA является проверяющим объектом, который после успешной аутентификации выдает заявителю сертификат аутентификации.

10.2 Процедура аутентификации

В среде, управляемой AAA, сервер AAA предоставляет пользователю услугу аутентификации. Он идентифицирует объект, запрашивающий доступ, что достаточно для определения того, к каким услугам может быть разрешен доступ и за какие услуги может начисляться плата. Сертификат аутентификации может быть выдан сервером AAA.

10.2.1 Успешные аутентификации

Перечисленные ниже этапы и рисунок 10-1 представляют пример потока сообщений для успешной аутентификации.

Этап 1. Объект запрашивает доступ у клиента AAA.

Этап 2. Клиент AAA запрашивает аутентификацию объекта у сервера AAA.

Этап 3. Сервер AAA запрашивает регистрационные данные объекта у клиента AAA для начала аутентификации.

Этап 4. Клиент AAA запрашивает у объекта регистрационные данные, требуемые для аутентификации.

Этап 5. Объект, который теперь является заявителем, посылает запрашиваемые регистрационные данные клиенту AAA.

Этап 6. Клиент AAA направляет запрашиваемые регистрационные данные серверу AAA для аутентификации.

Этап 7. Сервер AAA проверяет полученные регистрационные данные в сравнении с профилем пользователя заявителя.

Этап 8. Если регистрационные данные можно проверить, сервер AAA приступает к процессу авторизации, не уведомляя об этом клиента AAA или заявителя.

Этап 9. После процесса авторизации сервер AAA посылает клиенту AAA сообщение о том, что доступ разрешен.

Этап 10. Клиент AAA направляет заявителю сообщение о том, что доступ разрешен.

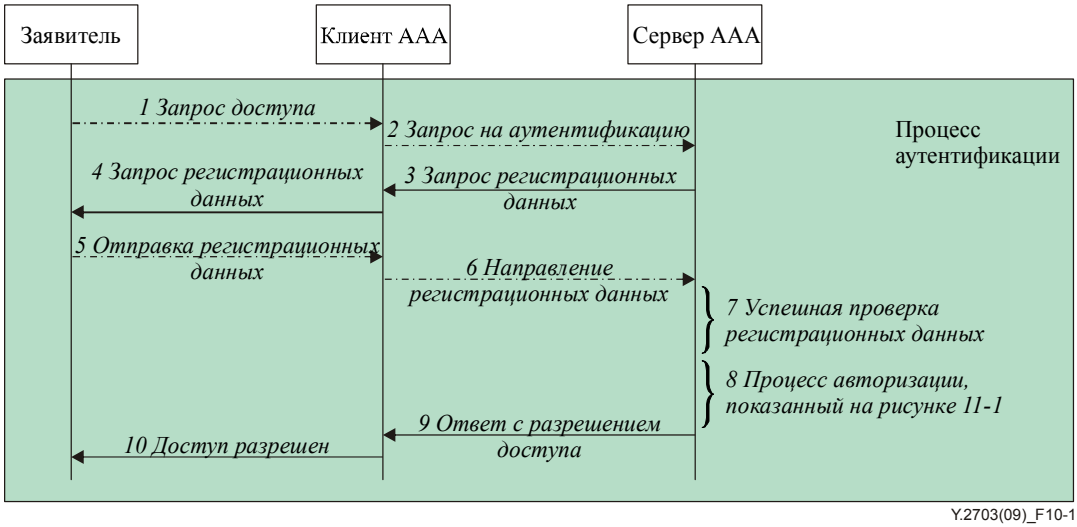

Рисунок 10-1 – Поток сообщений для успешной аутентификации

10.2.2 Неуспешная аутентификация

Перечисленные ниже этапы и рисунок 10-2 представляют пример потока сообщений для неуспешной аутентификации.

Этап 1. Объект запрашивает доступ у клиента AAA.

Этап 2. Клиент AAA запрашивает аутентификацию объекта у сервера AAA.

Этап 3. Сервер AAA запрашивает регистрационные данные объекта у клиента AAA для начала аутентификации.

Этап 4. Клиент AAA запрашивает у объекта регистрационные данные, требуемые для аутентификации.

Этап 5. Объект, который теперь является заявителем, посылает запрашиваемые регистрационные данные клиенту AAA.

Этап 6. Клиент AAA направляет запрашиваемые регистрационные данные серверу AAA для аутентификации.

Этап 7. Сервер AAA проверяет полученные регистрационные данные в сравнении с профилем пользователя заявителя.

Этап 8. Если регистрационные данные нельзя проверить, сервер AAA посылает клиенту AAA сообщение о том, что в доступе отказано.

Этап 9. Клиент AAA направляет заявителю сообщение о том, что в доступе отказано.

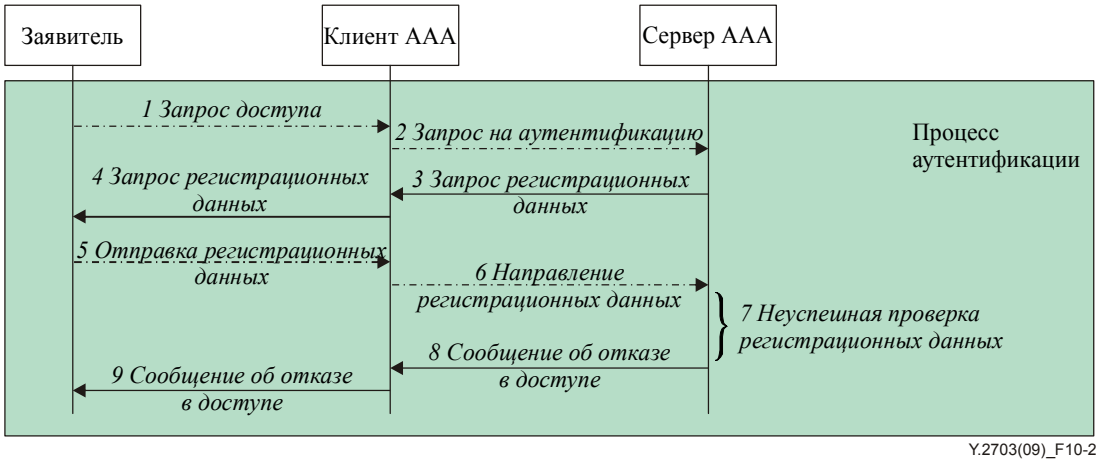

Рисунок 10-2 – Поток сообщений для неуспешной аутентификации

11 Авторизация

Авторизация определяется как действие по установлению того, можно ли предоставить какую-либо конкретную привилегию предъявителю конкретных регистрационных данных. Привилегия может представлять собой право доступа к ресурсу услуги (SR) и, в зависимости от действующей политики, может включать ресурсы чтения, письма или внесения изменений. Процесс авторизации следует за аутентификацией и подтверждает доступ или отказывает в доступе к услуге СПП в зависимости от результатов предыдущих этапов аутентификации и от действующей политики.

11.1 Аспекты авторизации для СПП

Цель авторизации состоит в предоставлении доступа и управлении доступом к разрешенным для аутентифицированного пользователя услугам. В СПП сервер AAA устанавливает связь с элементами сети, содержащими привилегии доступа зарегистрированных объектов.

В настоящей Рекомендации аутентификация и авторизация рассматриваются как связанные между собой процессы, осуществляемые, как правило, последовательно для зарегистрированных объектов каждый раз, когда запрашивается доступ. Однако политика поставщика может разрешать объекту запрашивать прямой доступ/права пользования без повторной аутентификации или регистрации. Такой случай здесь не рассматривается.

Авторизация пользователя услуги выполняется сервером AAA, который сообщает и получает информацию об авторизации от соответствующих элементов сети. По завершении сервером AAA процесса авторизации подтверждающая информация направляется пользователю, запрашивающему услугу.

Получение подтверждающей информации означает успешное завершение набора процессов аутентификации и авторизации, и осуществляющий доступ объект считается подключенным к сети или авторизованному SR.

11.2 Объекты авторизации

Процесс авторизации осуществляется сервером AAA автоматически после аутентификации без участия осуществляющего доступ объекта. Сервер AAA обеспечивает специальную функцию, которая принимает решения об авторизации с применением правил политики управления доступом.

11.3 Процедура авторизации

Процедура процесса авторизации показана на рисунке 11-1:

Этап A. После успешной авторизации объекта сервер AAA определяет услуги и ресурсы, которые имеются и доступны для заявителя.

Этап B. После завершения этапа A сервер AAA рекомендует функции управления транспортом и услугами для присвоения/распределения авторизованных услуг и ресурсов с целью использования заявителем.

Этап C. Сервер AAA посылает клиенту AAA сообщение о том, что доступ разрешен.

Этап D. Клиент AAA направляет заявителю сообщение о том, что доступ разрешен.

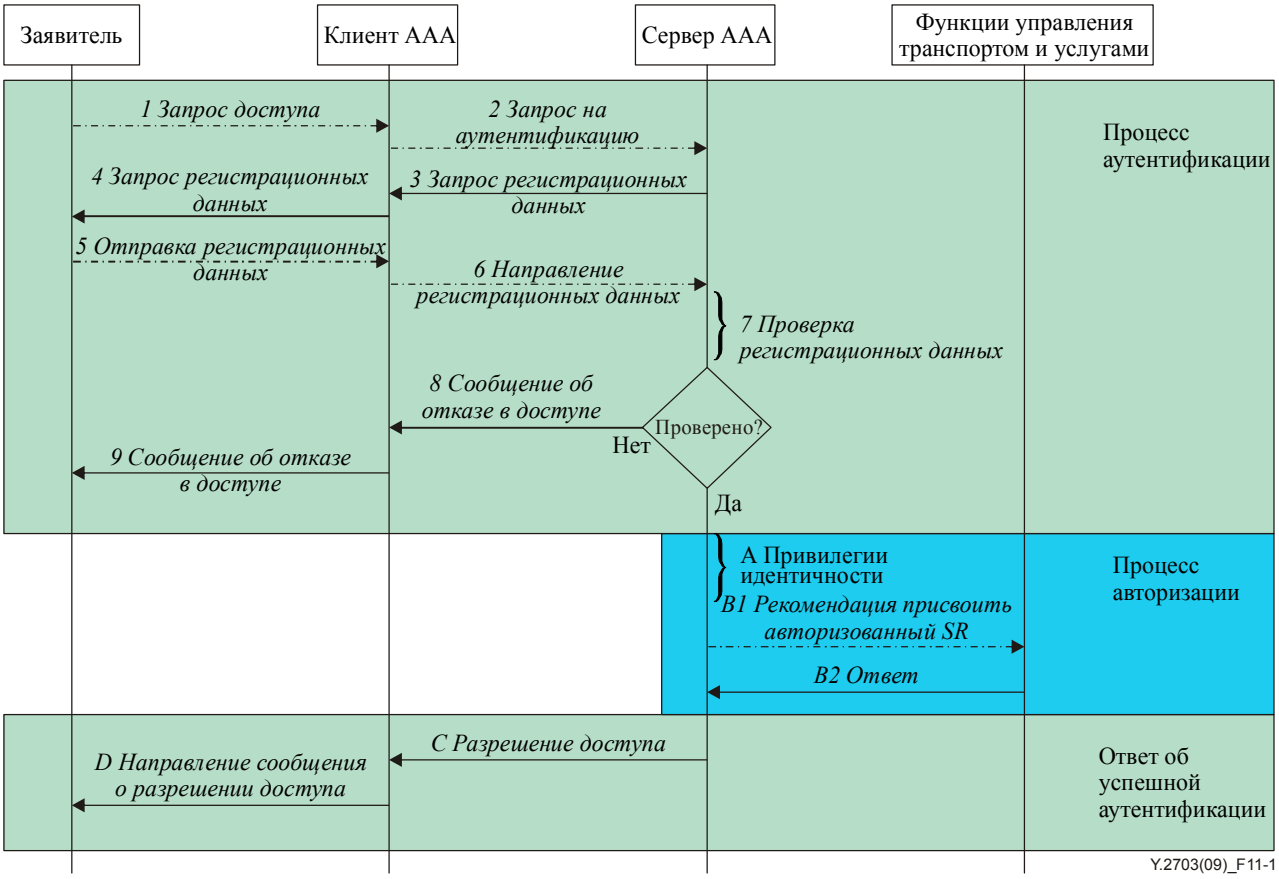

Рисунок 11-1 – Поток сообщений для процесса авторизации

12 Учет

В сокращении "AAA" последняя буква "A" означает учет (accounting). В контексте AAA учет включает элемент безопасности, который может использоваться в сочетании с другими данными о событиях в системе безопасности для поддержки функции учета.

12.1 Учет в системе безопасности

В учете событий в системе безопасности используется та подгруппа функций учета, которая обеспечивает учетные данные, используемые затем при разработке данных проверки безопасности для применения в функции проверки безопасности. Подробность данных проверки безопасности зависит от потребностей в проверке безопасности и политики, определенной поставщиком доступа к СПП для этого конкретного контекста, например время начала и завершения успешного или неуспешного доступа к сети или услуге, услуга, к которой осуществляется доступ, и информация, подтверждающая идентичность осуществляющего доступ объекта (для успешных случаев аутентификации). Фактическая функция проверки не входит в сферу охвата настоящей Рекомендации. Процедура учета в системе безопасности показана на рисунке 12-1.

12.2 Функции учета в системе безопасности

Учет в системе безопасности – это зона обслуживания, выполняющая такие функции, как:

1) Сбор данных: отвечает за приобретение поддающихся обнаружению данных о событии и за предоставление информации, касающейся контекста безопасности. Данные, сбор которых необходимо осуществлять, могут включать:
   - результаты аутентификации;
   - информацию, касающуюся аннулирования аутентификации и/или сертификата;
   - информацию о гарантии аутентификации;
   - другую информацию, касающуюся процесса аутентификации.

2) Хранение: сохраняет обозначения, которые выдает функция сбора данных.

3) Рассмотрение: направлено на точное описание события с помощью: проверки точности собранных данных, распознавания фактов путем изучения собранных данных.

4) Отчетность: информация берется из функции рассмотрения и направляется для функции проверки.

5) Проверка: проверяется правильность отчета об учете в системе безопасности или соответствие политике использования и руководящим указаниям в области безопасности. Для функции проверки может требоваться возможность незамедлительного оповещения.

Следует отметить, что функцией AAA является только сбор данных, а хранение, рассмотрение, отчетность и проверка – это управленческие функции. Такие функции не входят в сферу охвата настоящей Рекомендации.

Рисунок 12-1 – Пример процесса учета в системе безопасности

Дополнение I

Протокол аутентификации для ААА в СПП

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В настоящем Дополнении рассматриваются протокол EAP, который транспортируется по уровням каналов передачи данных, и протоколы ААА, которые обеспечивают структуру ААА в различных приложениях.

I.1 Протокол EAP для услуги ААА в СПП

Протокол EAP определяет структуру аутентификации, которая поддерживает различные методы аутентификации. EAP работает в одноранговом узле сети и сервере аутентификации через аутентификатор. EAP транспортируется напрямую по уровням каналов передачи данных, таких как IEEE 802 и PPP (протокол двухточечной связи).

Однако из-за свойства зависимости канала связи протокол EAP требует более низкого уровня, такого как EAPoL, IEEE 802.1X и IEEE 802.11i. На рисунке I.1 описана модель мультиплексирования, относящаяся к EAP. Уровень, применяемый при методе EAP, включает алгоритм аутентификации. Одноранговый узел сети и аутентификатор EAP имеют соответствующие функциональные характеристики, такие как клиент аутентификации и аутентификатор. Уровень EAP выполняет доставку сообщений EAP. Более низкий уровень передает или принимает кадры EAP между одноранговым узлом сети и аутентификатором. Поскольку уровень канала передачи состоит из различных протоколов каналов передачи, для EAP требуются разные более низкие уровни для каждого протокола канала передачи.

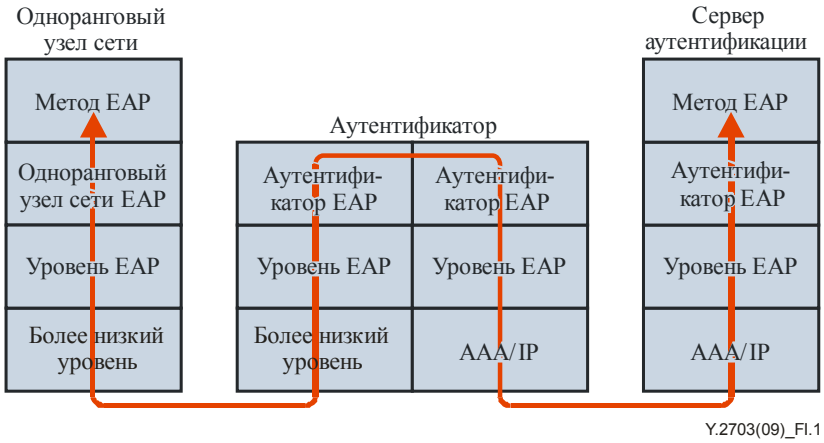

Рисунок I.1 – Модель передачи при EAP

Для EAP требуется более низкий уровень для надежной доставки сообщений, обнаружения ошибок и упорядочения сообщений следующим образом:

- Поскольку в EAP не известно, что одноранговый узел сети получает сообщение от аутентификатора, для EAP требуется надежный канал между одноранговым узлом сети и аутентификатором.
- EAP не обеспечивает доставку сообщений EAP в место назначения без ошибок. Для EAP требуется функция обнаружения ошибок с более низкого уровня.
- Порядок сообщений в EAP мог бы изменяться или они могли бы дублироваться по любой причине. Таким образом, для EAP требуются обнаружение случаев дублирования и упорядочение для гарантирования правильных операций.
- На более низком уровне не известно, включает или нет более высокий уровень протокол аутентификации. Для EAP требуется указание на протокол аутентификации.

I.2 Протоколы AAA

Первоначально протоколы AAA, такие как RADIUS, использовались для обеспечения доступа с набором номера к PPP и серверу терминала. С расширением интернета и внедрением новых технологий доступа был разработан протокол Diameter. В таблице I.1 приводится сравнение протоколов AAA.

Таблица I.1 – Сравнение протоколов AAA

	RADIUS	**DIAMETER**
Размер сети	Небольшая	Большая
Транспорт	UDP	SCTP/TCP
Кодирование	Только пароль	Полный пакет
Аутентификация/авторизация	Сочетание	Сочетание
Стандарт	IETF	IETF
Архитектура протокола	C/S	P2P
Масштабируемость	Низкая	Высокая

В случае протокола RADIUS управление распределенным последовательным каналом и группами модемов для большого числа пользователей может приводить к необходимости существенной административной поддержки. Поскольку группы модемов по определению являются каналом передачи во внешний мир, они требуют пристального внимания к безопасности, авторизации и учету. Лучше всего это можно достичь с помощью управления единой "базой данных" пользователей, которая предусматривает аутентификацию (проверку имени пользователя и пароля), а также информацию о конфигурации с подробными данными о типе услуги, которую необходимо предоставить пользователю.

Базовый протокол Diameter может использоваться сам по себе для приложений учета, но при использовании в случаях аутентификации и авторизации он всегда расширяется для конкретного приложения.

Дополнение II

Цифровые сертификаты X.509 в качестве регистрационных данных

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Общим методом обеспечения гарантии аутентификации является использование цифровых сертификатов, как это описано в [b-ITU-T X.509] и [b-ITU-T X.811]. Сертификат, определенный в [b-ITU-T X.509], который повсеместно используется, содержит следующие типы данных:

– ***version*** представляет собой версию кодированного сертификата. Если в сертификате присутствует компонент extensions, должна быть версия v3. Если присутствует компонент issuerUniqueIdentifier или subjectUniqueIdentifier, должна быть версия v2 или v3.

– ***serialNumber*** представляет собой целое число, присваиваемое CA каждому сертификату. Значение serialNumber должно быть уникальным для каждого сертификата, выданного заданным CA (т. е. имя выдавшего органа и порядковый номер однозначно определяют сертификат).

– ***signature*** содержит идентификатор алгоритма для алгоритма и хэш-функции, используемой CA при подписании сертификата (например, md5WithRSAEncryption, sha-1WithRSAEncryption, id-dsa-with-sha1 и т. д.).

– ***issuer*** определяет объект, подписавший и выдавший сертификат.

– ***validity*** представляет собой интервал времени, в течение которого CA гарантирует, что он будет поддерживать информацию о статусе сертификата.

– ***subject*** определяет объект, связанный с открытым ключом, содержащимся в поле открытого ключа субъекта.

– ***subjectPublicKeyInfo*** используется для передачи сертифицируемого открытого ключа и для определения алгоритма, примером которого является данный открытый ключ (например, rsaEncryption, dhpublicnumber, id-dsa и т. д.).

– ***issuerUniqueIdentifier*** используется для однозначного определения выдавшего органа в случае повторного использования имени.

– ***subjectUniqueIdentifier*** используется для однозначного определения субъекта в случае повторного использования имени.

– ***extensions field*** делает возможным добавление в структуру новых полей.

Дополнение III

Сценарий использования аутентификации и авторизации

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Сценарий использования услуги AAA, приведенный в настоящем дополнении, основан на эталонной модели, которая представлена в [b-ITU-T Y.2702].

III.1 Аутентификация и авторизация пользователя для доступа в сеть

Услуги по аутентификации и авторизации при доступе в сеть необходимы для проверки данных идентичность и определения того, следует ли предоставлять доступ для оборудования конечного пользователя.

III.1.1 Аутентификация и авторизация устройства для доступа/подключения к СПП

В этом случае имеются три типа аутентификации и авторизации устройства для доступа/подключения к СПП. Эти услуги и возможности по идентификации, аутентификации и авторизации для доступа или подключения пользовательских устройств к IP-сети доступа включают в себя:

– идентификацию, аутентификацию и авторизацию традиционного оконечного оборудования (TE) и оконечного оборудования – пограничного элемента (TE-BE) для доступа/подключения к IP-сети доступа ((1) на рисунке III.1);

– идентификацию, аутентификацию и авторизацию традиционного TE и TE-BE с интегрированным устройством доступа (IAD) в домене клиента для доступа/подключения к IP-сети доступа ((2) на рисунке III.1);

– идентификацию, аутентификацию и авторизацию TE и TE-BE СПП с возможностями IP в домене клиента для доступа/подключения к IP-сети (3) на рисунке III.1).

Клиент AAA предоставляет услугу по аутентификации для устройства и поставщика доступа к сети: при необходимости он автоматически разрешает устройству доступ к сети поставщика.

Показанная на рисунке III.1 в части (1) процедура идентификации является следующей.

Этап 1. Шлюз (заявитель) запрашивает доступ/подключение к сети у клиента AAA.

Этап 2. Клиент AAA запрашивает идентификацию шлюза у сервера AAA (верификатора), который идентифицирует шлюз.

Этап 3. Сервер AAA посылает результаты идентификации клиенту AAA.

Этап 4. Клиент AAA направляет результаты шлюзу, если клиент AAA хранит список случаев доступа шлюза.

В случаях (2) и (3), IAD и TE СПП являются, соответственно, заявителями. В остальном процесс идентичен процедуре (1).

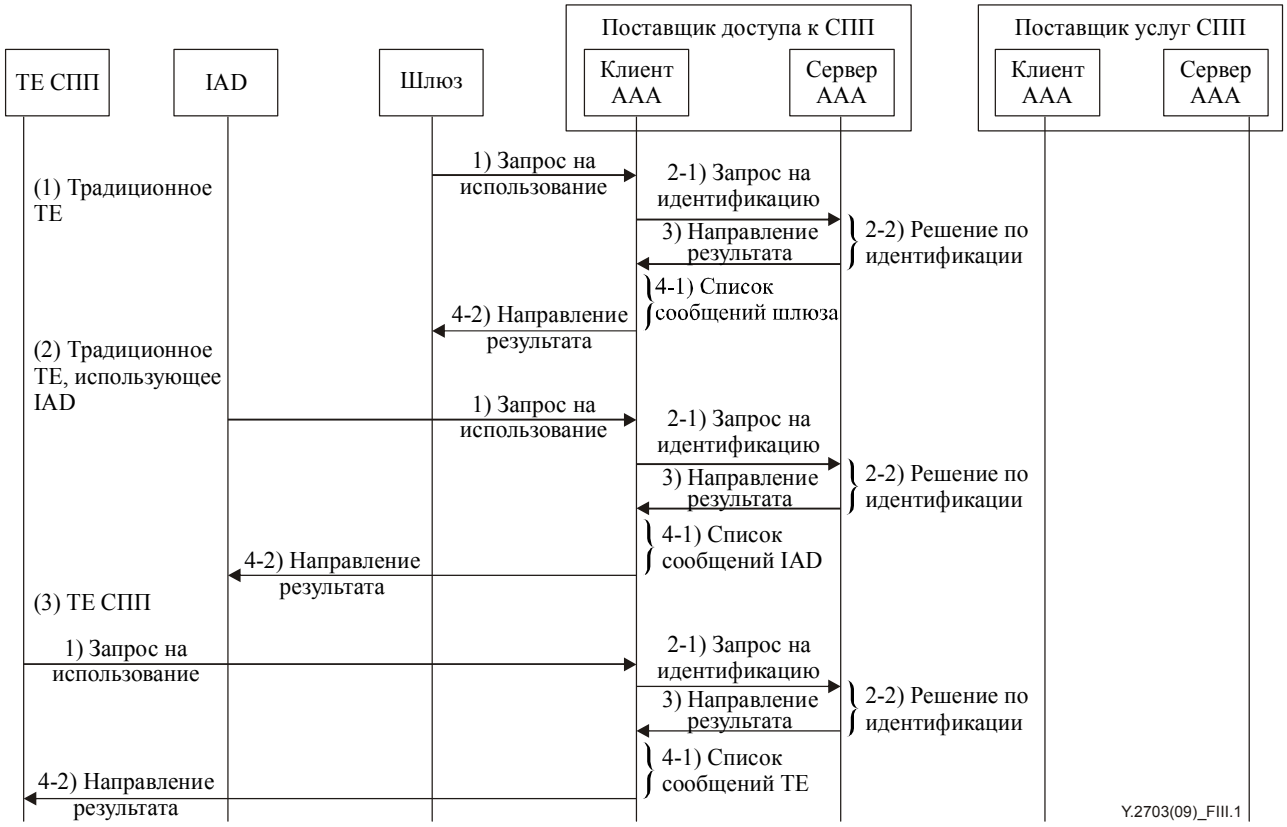

Рисунок III.1 – Процедура идентификации устройства для доступа к сети СПП

III.1.2 Объединенные аутентификация и авторизация устройства для доступа/подключения к СПП, а также услуги/приложения

В этом случае имеются три типа аутентификации и авторизации для доступа/подключения к СПП. Эти услуги и возможности объединяют аутентификацию устройства пользователя поставщиком доступа к СПП и аутентификацию устройства поставщиком услуг СПП следующим образом:

– услуги и возможности поставщика услуг СПП по неявной идентификации и авторизации традиционного ТЕ и ТЕ-ВЕ ((1) на рисунке III.2);

– услуги и возможности поставщика услуг СПП по неявной идентификации и авторизации традиционного ТЕ и ТЕ-ВЕ с IAD ((2) на рисунке III.2);

– услуги и возможности поставщика услуг СПП по прямой идентификации, аутентификации и авторизации ТЕ и ТЕ-ВЕ СПП в домене пользователя ((3) на рисунке III.2).

Клиент AAA предоставляет услугу по аутентификации для устройства и поставщика услуги/приложения: в случае необходимости он автоматически разрешает устройству доступ к поставщику услуги/приложения.

Показанная на рисунке III.2 в части (1) процедура идентификации является следующей:

Этап 1. Шлюз (заявитель) запрашивает использование услуги/приложения у клиента AAA.

Этап 2. Клиент AAA запрашивает идентификацию шлюза у сервера AAA (верификатора) в домене сети доступа, если сервер AAA идентифицирует шлюз.

Этап 3. Сервер AAA посылает результаты идентификации и одновременно клиенту AAA и серверу AAA в домене поставщика услуг СПП.

Этап 4. Клиент AAA направляет результаты шлюзу, если клиент AAA хранит список случаев доступа шлюза.

Показанная на рисунке III.2 в части (2) процедура идентификации является следующей:

Этап 1. IAD (заявитель) запрашивает использование услуги/приложения у клиента AAA.

Этап 2. Клиент AAA запрашивает идентификацию IAD у клиента AAA в домене поставщика услуг СПП, если сервер AAA (верификатор) в домене поставщика услуг СПП идентифицирует IAD.

Этап 3. Сервер AAA посылает результаты идентификации клиенту AAA.

Этап 4. Клиент AAA направляет результаты IAD, если клиент AAA хранит список случаев доступа IAD.

В случае (3) ТЕ СПП является заявителем. В остальном процесс идентичен процедуре (2).

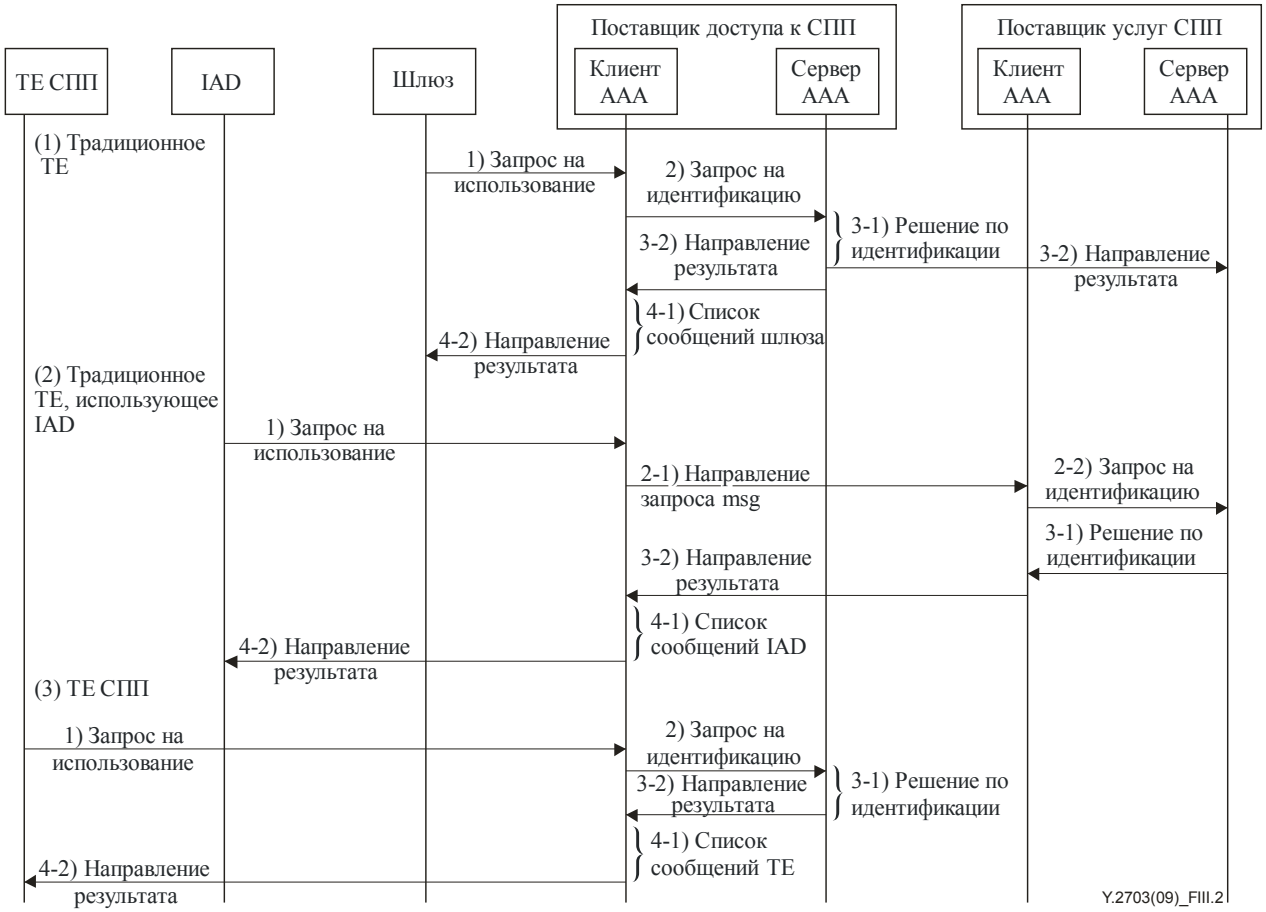

Рисунок III.2 – Процедура идентификации устройства для использования поставщика услуги/приложения

III.2 Аутентификация и авторизация пользователя поставщиком услуг СПП для доступа к услуге/приложению

В этом случае имеются три типа аутентификации и авторизации услуги/приложения у поставщика доступа ко многим сетям:

– Поставщик услуг СПП косвенно аутентифицирует устройство пользователя с помощью доверительных отношений с поставщиком доступа к СПП ((1) на рисунке III.3).

– Поставщик услуг СПП напрямую аутентифицирует и авторизует устройство пользователя ((2) на рисунке III.3).

– Поставщик услуг СПП напрямую аутентифицирует пользователя ((3) на рисунке III.3).

Клиент AAA предоставляет услугу по аутентификации пользователю и поставщику услуги/приложения: в случае необходимости он автоматически разрешает пользователю доступ у поставщика услуги/приложения.

Показанная на рисунке III.3 в части (1) процедура идентификации является следующей:

Этап 1: TE (заявитель) запрашивает использование услуги/приложения у клиента AAA.

Этап 2: Клиент AAA запрашивает идентификацию устройства у сервера AAA (верификатора) в домене сети доступа, если сервер AAA идентифицирует устройство.

Этап 3: Сервер AAA посылает результаты идентификации одновременно клиенту AAA и серверу AAA в домене поставщика услуг СПП.

Этап 4: Клиент AAA направляет результаты шлюзу, если клиент AAA хранит список случаев доступа устройства.

Показанная на рисунке III.3 в части (2) процедура идентификации является следующей.

Этап 1. TE (заявитель) запрашивает использование услуги/приложения у клиента AAA в домене поставщика услуг СПП.

Этап 2. Клиент AAA запрашивает идентификацию устройства у сервера AAA (верификатора) в домене поставщика услуг СПП, если сервер AAA идентифицирует устройство.

Этап 3. Сервер AAA посылает результаты идентификации клиенту AAA.

Этап 4. Клиент AAA направляет результаты устройству, если клиент AAA хранит список случаев доступа устройства.

Показанная на рисунке III.3 в части (3) процедура идентификации является следующей.

Этап 1. Пользователь (заявитель) запрашивает использование услуги/приложения у клиента AAA в домене поставщика услуг СПП.

Этап 2. Клиент AAA запрашивает аутентификацию пользователя у сервера AAA (верификатора) в домене поставщика услуг СПП, аутентифицирующего пользователя.

Этап 3. Сервер AAA посылает результаты аутентификации клиенту AAA.

Этап 4. Клиент AAA направляет результаты пользователю, если клиент AAA хранит список случаев доступа пользователя.

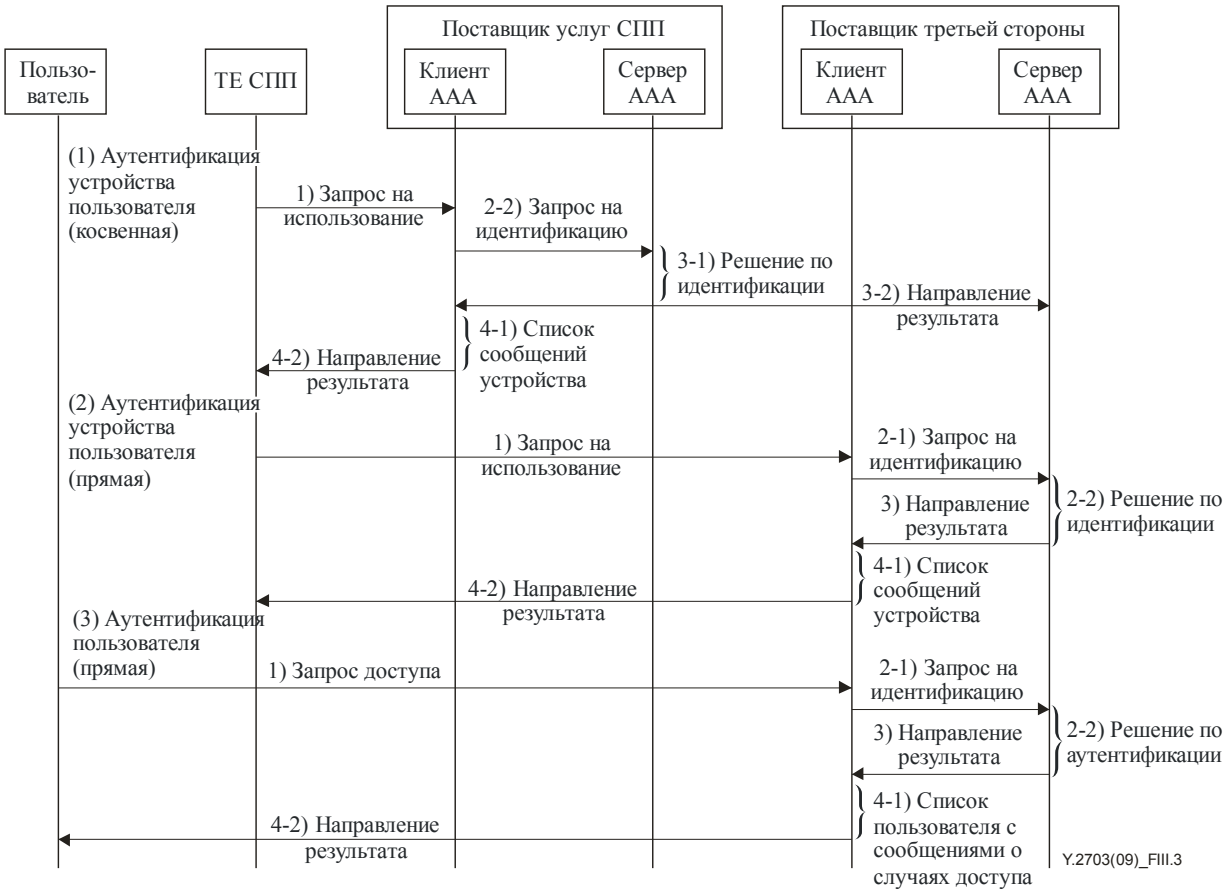

Рисунок III.3 – Процедура аутентификации и авторизации пользователя поставщиком услуг СПП

III.3 Аутентификация и авторизация пользователем поставщиков доступа к СПП

В этом случае имеются два типа аутентификации и авторизации сети пользователем:

– Аутентификация пользователем поставщика доступа к СПП для подключения сети ((1) на рисунке III.4).

– Аутентификация пользователем поставщика доступа к СПП для получения услуги ((2) на рисунке III.4).

Клиент AAA предоставляет услугу по аутентификации для аутентификации и авторизации сети пользователем: в случае необходимости он автоматически разрешает пользователю доступ у поставщика доступа к сети.

Показанная на рисунке III.4 в части (1) процедура идентификации является следующей:

Этап 1. Пользователь (заявитель) запрашивает аутентификацию пунктов доступа к сети (NAP) у верификатора третьей стороны.

Этап 2. Верификатор третьей стороны направляет NAP аутентификационную информацию (AI).

Этап 3. Обмен AI между верификатором третьей стороны и NAP.

Этап 4. Верификатор третьей стороны направляет результаты пользователю, если проверку проводит верификатор третьей стороны.

Показанная на рисунке III.4 в части (2) процедура идентификации является следующей:

Этап 1. Пользователь (заявитель) запрашивает аутентификацию сети у верификатора третьей стороны.

Этап 2. Верификатор третьей стороны направляет запрос пользователя клиенту AAA, если клиент AAA запрашивает AI у сервера AAA.

Этап 3. Сервер AAA посылает AI клиенту AAA и производит обмен AI между верификатором третьей стороны и клиентом AAA.

Этап 4. Верификатор третьей стороны направляет результаты пользователю, если проверку проводит верификатор третьей стороны.

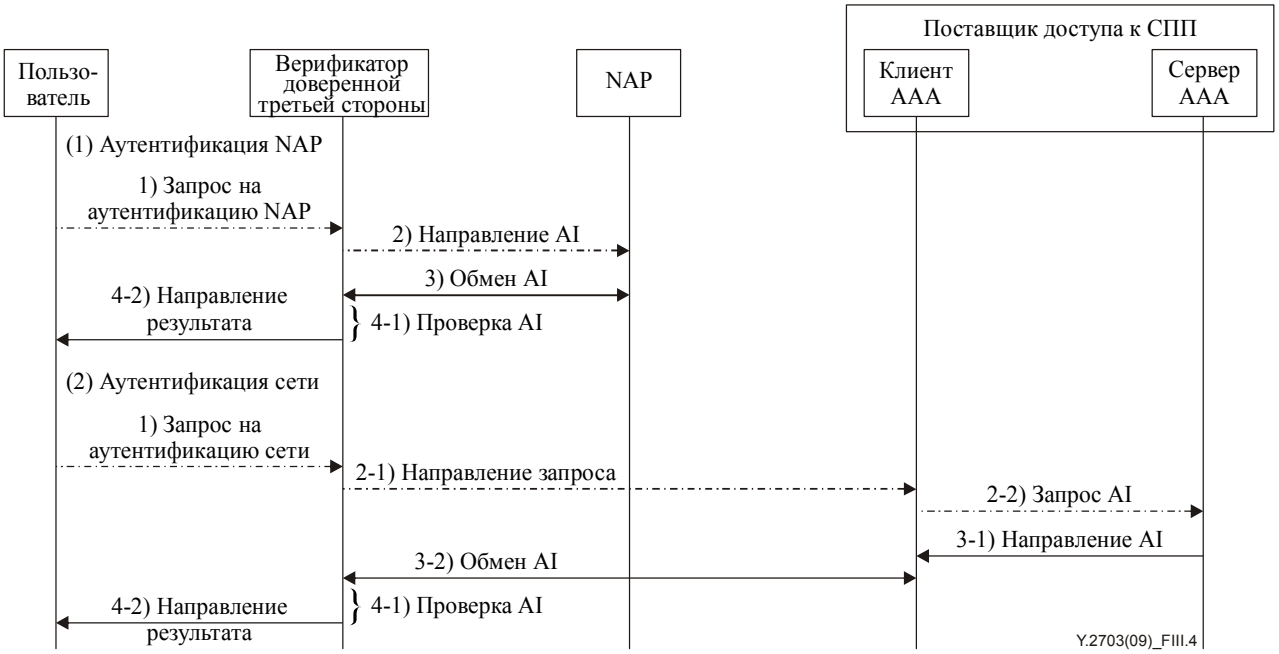

Рисунок III.4 – Процедура аутентификации и авторизации пользователем поставщиков доступа к СПП

III.4 Аутентификация и авторизация поставщиком доступа к СПП поставщика услуги/приложения третьей стороны

Могут существовать некоторые сценарии, при которых поставщик приложения или услуги отличается от поставщика доступа к СПП (т. е. поставщик услуги/приложения третьей стороны). Поставщику доступа к СПП потребуется аутентифицировать и авторизовать поставщика услуги/приложения третьей стороны.

Клиент AAA предоставляет услугу по аутентификации поставщику доступа к СПП, который аутентифицирует и авторизует поставщика услуги/приложения третьей стороны.

Показанная на рисунке III.5 процедура идентификации является следующей.

Этап 1. Клиент AAA (заявитель) поставщика доступа к СПП запрашивает аутентификацию поставщика услуги/приложения третьей стороны у верификатора третьей стороны.

Этап 2. Верификатор третьей стороны направляет запрос пользователя клиенту AAA поставщика услуги/приложения третьей стороны, и клиент AAA запрашивает AI у сервера AAA.

Этап 3. Сервер AAA направляет AI клиенту AAA и производит обмен AI между верификатором третьей стороны и клиентом AAA.

Этап 4. Верификатор третьей стороны направляет результаты клиенту AAA поставщика доступа к СПП, если проверку проводит верификатор третьей стороны, а результаты хранятся на сервере AAA.

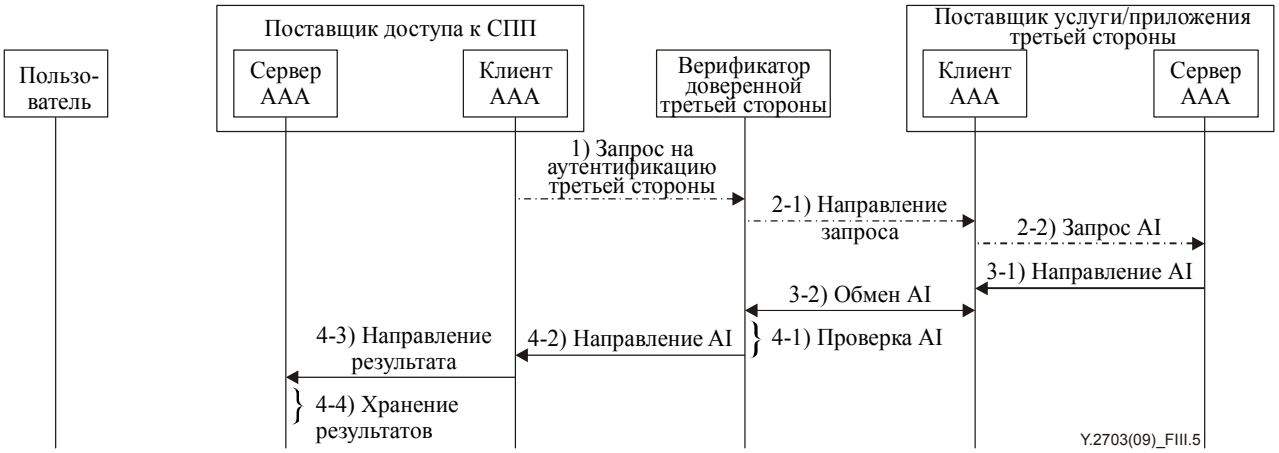

Рисунок III.5 – Процедура аутентификации и авторизации поставщиком доступа к СПП поставщика услуги/приложения третьей стороны

III.5 Использование услуги третьей стороны по аутентификации и авторизации

Поставщики услуг могут предоставлять услугу третьей стороны по аутентификации и авторизации. В этом случае имеются два типа использования услуги третьей стороны по аутентификации и авторизации:

– аутентификация пользователя для поставщика услуги ((1) на рисунке III.6);

– аутентификация поставщика услуги для пользователя ((2) на рисунке III.6).

III.5.1 Аутентификация пользователя для поставщика услуги

Клиент AAA предоставляет поставщику услуги услугу по аутентификации с целью аутентификации и авторизации пользователя: в случае необходимости он автоматически разрешает пользователю доступ у поставщика услуги/приложения третьей стороны.

Показанная на рисунке III.6 процедура идентификации является следующей:

Этап 1. Пользователь (заявитель) запрашивает доступ к сети у клиента AAA.

Этап 2. Клиент AAA запрашивает характеристики пользователя у сервера AAA поставщика услуги/приложения третьей стороны, если сервер AAA (верификатор) аутентифицирует пользователя.

Этап 3. Сервер AAA посылает результаты аутентификации клиенту AAA.

Этап 4. Клиент AAA направляет результаты пользователю, если клиент AAA хранит список случаев доступа пользователя.

Этап 5. Если доступ предоставлен, пользователь может иметь доступ к обозначенному ресурсу сети.

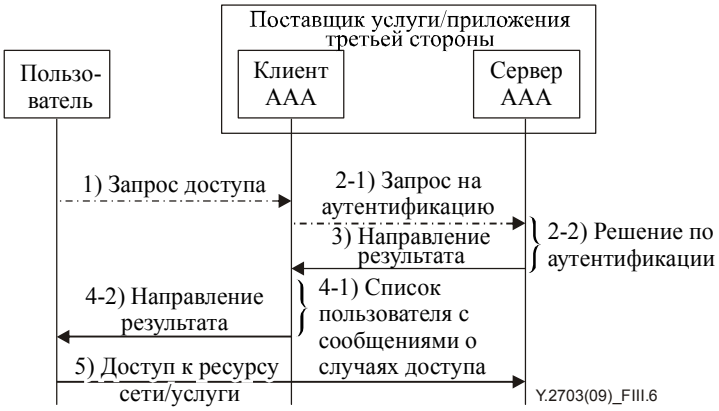

Рисунок III.6 – Процедура использования услуги третьей стороны по аутентификации и авторизации

III.5.2 Аутентификация поставщика услуги для пользователя

Клиент AAA предоставляет пользователю услугу по аутентификации с целью аутентификации поставщика услуги. Показанная на рисунке III.7 процедура идентификации является следующей:

Этап 1. Пользователь (заявитель) в собственном домене запрашивает аутентификацию поставщика услуги/приложения третьей стороны у верификатора третьей стороны.

Этап 2. Верификатор третьей стороны направляет запрос пользователя клиенту AAA поставщика услуги/приложения третьей стороны, и клиент AAA запрашивает AI у сервера AAA.

Этап 3. Сервер AAA направляет AI клиенту AAA и производит обмен AI между верификатором третьей стороны и клиентом AAA.

Этап 4. Верификатор третьей стороны направляет результаты клиенту AAA поставщика доступа к СПП, если верификатор третьей стороны производит проверку и хранит результаты.

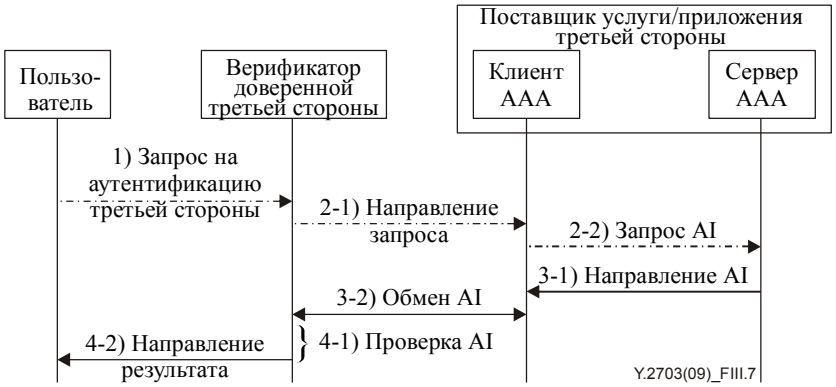

Рисунок III.7 – Процедура использования услуги третьей стороны по аутентификации и авторизации

Библиография

[b-ITU-T M.3410] Recommendation ITU-T M.3410 (2008), *Guidelines and requirements for security management systems to support telecommunications management*.

[b-ITU-T Q.3201] Recommendation ITU-T Q.3201 (2007), *EAP-based security signalling protocol architecture for network attachment*.

[b-ITU-T Q.3202.1] Recommendation ITU-T Q.3202.1 (2008), *Authentication protocols based on EAP-AKA for interworking among 3GPP, WiMax, and WLAN in NGN*.

[b-ITU-T X.509] Рекомендация МСЭ-Т X.509 (2005 г.) | ИСО/МЭК 9594-8:2005, *Информационные технологии – Взаимосвязь открытых систем – Справочник: Структуры сертификатов открытых ключей и атрибутов*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

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

[b-ITU-T X.810] Рекомендация МСЭ-Т X.810 (1995 г.) | ИСО/МЭК 10181-1:1996, *Информационные технологии – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Обзор*.

[b-ITU-T X.811] Рекомендация МСЭ-Т X.811 (1995 г.) | ИСО/МЭК 10181-2:1996, *Информационные технологии – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура аутентификации*.

[b-ITU-T X.812] Рекомендация МСЭ-Т X.812 (1995 г.) | ИСО/МЭК 10181-3:1996, *Информационные технологии – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура управления доступом*.

[b-ITU-T X.816] Рекомендация МСЭ-Т X.816 (1995 г.) | ИСО/МЭК 10181-7:1996, *Информационные технологии – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура аудита и аварийных извещений безопасности*.

[b-ITU-T Y.2001] Рекомендация МСЭ-Т Y.2001 (2004 г.), *Общий обзор СПП*.

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

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

[b-ITU-T Y.2201] Рекомендация МСЭ-Т Y.2201 (2007 г.), *Требования к сетям последующих поколений версии 1*.

[b-ITU-T Y.2233] Рекомендация МСЭ-Т Y.2233 (2008 г.), *Требования и структура, обеспечивающие возможности учета и начисления платы в СПП*.

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

[b-ITU-T Y.2702] Рекомендация МСЭ-Т Y.2702 (2008 г.), *Требования к аутентификации и авторизации для СПП варианта 1*.

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	Качество телефонной передачи, телефонные установки, сети местных линий
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 протокола Интернет и сети последующих поколений**
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2010 г.