МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т Y.2702

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2008)

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

Сети последующих поколений – Безопасность

Требования к аутентификации и авторизации для СПП варианта 1

Рекомендация МСЭ-Т Y.2702

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
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
Безопасность	**Y.2700–Y.2799**
Обобщенная мобильность	Y.2800–Y.2899

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

Рекомендация МСЭ-Т Y.2702

Требования к аутентификации и авторизации для СПП варианта 1

Резюме

В Рекомендации МСЭ-Т Y.2702 описаны требования к аутентификации и авторизации для сетей последующих поколений (СПП).

Источник

Рекомендация МСЭ-Т Y.2702 утверждена 12 сентября 2008 года 13-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

Ключевые слова

Атрибуты, аутентификация, авторизация, идентификаторы, управление определением идентичности (IdM), сети последующих поколений (СПП), привилегии и безопасность.

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.2702

Требования к аутентификации и авторизации для СПП варианта 1

1 Сфера применения

В настоящей Рекомендации представлены требования к аутентификации и авторизации для сетей последующих поколений (СПП), базирующиеся на [Y.2012]. К ним относятся требования к односторонней и взаимной аутентификации и авторизации по интерфейсу пользователь-сеть (UNI), интерфейсу сеть-сеть (NNI) и интерфейсу приложение-сеть (ANI), а также выполняемой в случае необходимости аутентификации и авторизации любого объекта с сетью на внутреннем уровне. Сфера применения настоящей Рекомендации включает следующие области:

1) аутентификация и авторизация пользователя для доступа в сеть (например, аутентификация и авторизация устройства конечного пользователя, шлюза домашней сети или шлюза предприятия для получения доступа в сеть или для присоединения к сети);
2) выполняемые поставщиком услуг аутентификация и авторизация пользователя для доступа к услугам/приложениям (например, аутентификация и авторизация пользователя, устройства или совместно пользователя/устройства, если аутентификация и авторизация применяется в целях получения доступа к услугам/приложениям СПП);
3) выполняемая пользователем аутентификация и авторизация сети (например, пользователь, выполняющий аутентификацию подлинности подсоединенной сети СПП или поставщика услуг);
4) одноранговая аутентификация и авторизация пользователя (например, аутентификация и авторизация вызываемого пользователя (или завершающего объекта), аутентификация и авторизация вызывающего объекта или аутентификация источника данных как функции сети);
5) взаимная сетевая аутентификация и авторизация (например, аутентификация и авторизация по интерфейсу NNI на транспортном уровне или на уровне услуг/приложений);
6) аутентификация и авторизация поставщика услуг/приложений;
7) использование услуги аутентификации и авторизации третьей стороны;
8) аутентификация объектов (например, прикладного процесса, идентификаторов контента сообщения и контента данных).

Перечисленные выше задачи включают аутентификацию потоков сигнализации, трафика канала передачи и трафика управления, в зависимости от случая.

ПРИМЕЧАНИЕ 1. – Аутентификация и авторизация СПП рассматривается как часть более широкой темы управления определением идентичности (IdM) в СПП. В частности, функции и возможности аутентификации и авторизации, описанные в настоящей Рекомендации, должны применяться для поддержки возможностей гарантированности подлинности для целей IdM в СПП.

ПРИМЕЧАНИЕ 2. – В настоящей Рекомендации использование термина "пользователь" не ограничено физическим лицом. Пользователем может быть физическое лицо, группы, компании или юридические лица.

ПРИМЕЧАНИЕ 3. – Аутентификация объекта не предназначена для указания положительного результата проверки достоверности лица.

2 Ссылки

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру, поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статуса рекомендации.

[ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.), Архитектура защиты взаимосвязи открытых систем для приложений МККТТ.

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

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

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

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

[ITU-T Y.2201] Recommendation ITU-T Y.2201 (2007), NGN release 1 requirements.

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

3 Определения

3.1 Определения из [ITU-T X.800]

В настоящей Рекомендации используются следующие термины, определенные в [ITU-T X.800]:

3.1.1 аутентификационная информация: Информация, используемая для установления действительности предъявленных идентификационных данных.

3.1.2 авторизация: Предоставление прав, включающее предоставление доступа на основе прав доступа.

3.1.3 полномочия: Данные, которые передаются для установления заявляемой идентичности.

3.1.4 аутентификация источника данных: Подтверждение того, что источник полученных данных соответствует предъявленной идентификационной информации.

3.1.5 одноранговая аутентификация объекта: Подтверждение того, что одноранговый объект в ассоциации соответствует предъявленным идентификационным данным.

3.2 Определения из [ITU-T X.810]

В настоящей Рекомендации используются следующие термины, определенные в [ITU-T X.810]:

3.2.1 доверие: Считается, что объект X доверяет объекту Y выполнение некоторого набора действий, только лишь если объект X полагается на определенность поведения объекта Y в отношении этих действий.

3.2.2 доверенная третья сторона: Орган обеспечения безопасности или его агент, который является доверенным в отношении некоторых связанных с безопасностью действий (в контексте политики обеспечения безопасности).

3.3 Определения из [ITU-T X.811]

В настоящей Рекомендации используются следующие термины, определенные в [ITU-T X.811]:

3.3.1 ассиметричный алгоритм аутентификации: Метод аутентификации, при котором не вся аутентификационная информация совместно используется обоими объектами.

3.3.2 аутентифицированная подлинность: Отличительный идентификатор администратора доступа, подтвержденный посредством аутентификации.

3.3.3 аутентификация: Обеспечение гарантированности подлинности предъявленных идентификационных данных объекта.

3.3.4 сертификат аутентификации: Сертификат безопасности, гарантированный органом аутентификации, который может использоваться для гарантирования подлинности объекта.

3.3.5 аутентификационный обмен: Последовательность из одной или нескольких передач обмена аутентификационной информацией (AI) для целей осуществления аутентификации.

3.3.6 аутентификационная информация (AI): Информация, используемая для целей аутентификации.

3.3.7 инициатор аутентификации: Объект, который начинает аутентификационный обмен.

3.3.8 предъявитель: Объект, который является администратором доступа или представляет администратора доступа для целей аутентификации. Предъявитель обладает функциями, необходимыми для участия в аутентификационных обменах от имени администратора доступа.

3.3.9 предъявляемая аутентификационная информация (предъявляемая AI): Информация, используемая предъявителем с целью генерации обмена аутентификационной информацией, необходимого для аутентификации администратора доступа.

3.3.10 обменная аутентификационная информация (обменная AI): Информация, которой обмениваются предъявитель и верификатор в процессе аутентификации администратора доступа.

3.3.11 администратор доступа: Объект, подлинность которого может быть аутентифицирована.

3.3.12 симметричный алгоритм аутентификации: Метод аутентификации, в котором оба объекта совместно используют общую аутентификационную информацию.

3.3.13 аутентификационная информация для верификации (AI для верификации): Информация, используемая верификатором для проверки подлинности идентификационной информации, предъявленной в составе обменной AI.

3.3.14 верификатор: Объект, который является объектом, требующим аутентифицированных идентификационных данных, или его представителем. Верификатор обладает функциями, необходимыми для участия в аутентификационных обменах.

3.4 Определения из [ITU-T Y.2701]

В настоящей Рекомендации используются следующие термины, определенные в [ITU-T Y.2701]:

3.4.1 пограничный элемент: Сетевой элемент, обеспечивающий функции для соединения разных доменов безопасности и административных доменов.

3.4.2 корпоративная сеть: Частная сеть, которая обеспечивает поддержку работы многих пользователей и может иметь несколько местоположений (например, предприятие, кампус).

3.4.3 домен безопасности: Совокупность элементов, политика безопасности, орган обеспечения безопасности и набор связанных с безопасностью действий, в рамках которых происходит управление элементами в соответствии с политикой безопасности. Применение политики выполняет орган обеспечения безопасности. Данный домен безопасности может охватывать несколько зон безопасности.

3.4.4 пограничный элемент оконечного оборудования: Пограничный элемент, обеспечивающий функции безопасности между оборудованием в помещении клиента и сетью поставщика услуг

3.5 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определен следующий термин:

3.5.1 соглашение об уровне обслуживания (SLA): Официальное соглашение между двумя и более сторонами, заключаемое по итогам переговоров, целью которых является определение характеристик услуг, ответственности и приоритетов каждой из сторон. SLA может включать заявления о безопасности, качестве работы, тарификации и выставлении счетов, обеспечении услуг и компенсациях.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

ACL Access Control List Список управления доступом

AI	Authentication Information		Аутентификационная информация
ANI	Application-to-Network Interface		Интерфейс "приложение-сеть"
AS	Application Server		Сервер приложений
BE	Border Element		Пограничный элемент
BSF	Bootstrapping Server Function		Функция удаленной начальной загрузки сервера
B-TID	Bootstrapping Transaction Identifier		Идентификатор транзакции начальной загрузки
CSCF	Call Session Control Function		Функция управления сеансами связи
DSL	Digital Subscriber Loop		Цифровой абонентский шлейф
ENI	ETS National Implementation		ETS, реализованная на национальном уровне
ETS	Emergency Telecommunication Service		Служба электросвязи в чрезвычайных ситуациях
FE	Functional Entities		Функциональные объекты
GAA	Generic Authentication Architecture		Общая архитектура аутентификации
GBA	Generic Bootstrapping Architecture		Общая архитектура начальной загрузки
GUSS	GBA User Security Settings		Установки безопасности пользователя в GBA
HSS	Home Subscriber System		Система абонентских данных
HTTP	Hypertext Transfer Protocol		Протокол передачи гипертекста
HTTPS	HTTP Security		Безопасность HTTP
IAD	Integrated Access Device		Интегрированное устройство доступа
I-CSCF	Interrogating Call Session Control Function		Запрашивающая функция управления сеансами связи
ID-FF	Identity Federation Framework		Инфраструктура федеративной безопасности
IdM	Identity Management		Управление определением идентичности
IdP	Identity Provider		Поставщик удостоверений
ID-WSF	Identity Web Services Framework		Единая платформа идентификации в интернете
IMS	IP Multimedia Service		Мультимедийные услуги на основе IP
IP	Internet Protocol		Протокол Интернет
ISDN	Integrated Services Digital Network	ЦСИС	Цифровая сеть с интеграцией служб
IWF	Interworking Function		Функция межсетевого взаимодействия
LUAD	Liberty enabled User Agent or Device		Liberty-агент или Liberty-устройство пользователя
MAC	Media Access Control		Управление доступом к среде
MS	Media Server		Медиасервер
NACF	Network Attachment Control Function		Функция управления присоединением к сети
NAF	Network Application Function		Сетевая прикладная функция
NAP	Network Access Point		Точка доступа в сеть
NGN	Next Generation Network	СПП	Сети последующих поколений
NNI	Network-to-Network Interface		Интерфейс "сеть-сеть"
OAM&P	Operations, Administration, Maintenance and Provisioning		Эксплуатация, администрирование, техническое обслуживание и обеспечение
OSI	Open System Interconnection	ВОС	Взаимодействие открытых систем

P-CSCF	Proxy Call Session Control Function	Функция управления сеансами вязи с прокси-элементом
PES	PSTN/ISDN Emulation Service	Услуга эмуляции КТСОП/ЦСИС
PIN	Personal Identification Number	Персональный идентификационный номер
PKI	Public Key Infrastructure	Сертификат открытого ключа
PII	Personally Identifiable Information	Персональная идентифицируемая информация
PSK	Pre-shared Keys	Общие ключи
RACF	Resource and Admission Control Function	Функция управления ресурсами и установлением соединений
RBAC	Role Based Access Control	Управление доступом на основе ролей
RP	Relying Party	Доверяющая сторона
RPH	Resource-Priority Header	Заголовок приоритета ресурса
RSVP	Resource Reservation Protocol	Протокол резервирования ресурсов
SAML	Security Assertion Markup Language	Язык разметки утверждений безопасности
SASL	Simple Authentication and Security Layer	Простой уровень аутентификации и безопасности
SBC	Session Border Controller	Пограничный контроллер сеансов связи
S-CSCF	Serving Call Session Control Function	Обслуживающая функция управления сеансами связи
SDP	Session Description Protocol	Протокол описания сеанса связи
SIM	Subscriber Identification Module	Модуль идентификации абонента
SLA	Service Level Agreement	Соглашение об уровне обслуживания
SLF	Subscriber Locator Function	Функция указателя абонента
SOAP	Simple Object Access Protocol	Простой протокол доступа к объектам
SP	Service Provider	Поставщик услуг
SSOS	Single-Sign-On Service	Однократная регистрация
TDR	Telecommunication for Disaster Relief	Электросвязь для оказания помощи при бедствиях
TE	Terminal Equipment	Оконечное оборудование
TE-BE	Terminal Equipment – Border Element	Оконечное оборудование – пограничный элемент
TLS	Transport Layer Security	Безопасность на транспортном уровне
UAI	User Authentication Interface	Интерфейс аутентификации пользователя
UE	User Equipment	Оборудование пользователя
UNI	User-to-Network Interface	Интерфейс "пользователь-сеть"
URL	Uniform Resource Locator	Унифицированный указатель ресурсов
WS	Web Server	Веб-сервер
XML	eXtensible Markup Language	Расширяемый язык разметки

5 Эталонные модели

5.1 Структура аутентификации МСЭ-Т X.811

В настоящей Рекомендации используются основные понятия аутентификации, определенные в [ITU-T X.811] и кратко представленные ниже.

5.1.1 Основные понятия аутентификации

Аутентификация обеспечивает гарантированность подлинности предъявленных идентификационных данных объекта. Аутентификация имеет значение только в контексте взаимоотношений администратора доступа и верификатора. Выделяются два важных случая:

– администратор доступа представлен предъявителем, который имеет определенные взаимоотношения по связи с верификатором (аутентификация объекта); и

– администратором доступа является источник элемента данных, доступный для верификатора (аутентификация источника данных).

Аутентификация объекта обеспечивает подтверждение подлинности администратора доступа в контексте взаимоотношений по связи. Аутентифицированные идентификационные данные администратора доступа гарантируются только при условии привлечения службы аутентификации.

ПРИМЕЧАНИЕ 1. – В случае аутентификации источника данных необходима также адекватная гарантированность того, что эти данные не были изменены. Этого можно добиться с помощью услуги проверки целостности, например:

– используя условия, при которых данные не могут быть изменены;

– путем верификации соответствия полученных данных и цифрового "отпечатка пальца" этих данных при отправке;

– используя механизм цифровой подписи; или

– используя симметричного криптографического алгоритма.

ПРИМЕЧАНИЕ 2. – Термин "отношения по связи", используемый в определении аутентификации объекта, может интерпретироваться в широком смысле слова и может относиться, например, к соединению в рамках ВОС, связи между процессами или взаимодействию между пользователем и терминалом.

5.1.2 Идентификаторы

Администратор доступа – это объект, подлинность которого может аутентифицироваться. Администратор доступа имеет один или несколько связанных с ним отличительных идентификаторов. Для верификации предъявленных идентификационных данных объект может использовать услуги аутентификации. Прошедшая таким образом верификацию подлинность администратора доступа называется аутентифицированной подлинностью.

Примерами администраторов доступа, которые могут быть идентифицированы и, следовательно, аутентифицированы, могут служить в том числе:

– пользователи-люди;

– поставщики СПП;

– процессы;

– реальные открытые системы;

– объекты уровней ВОС;

– предприятия; и

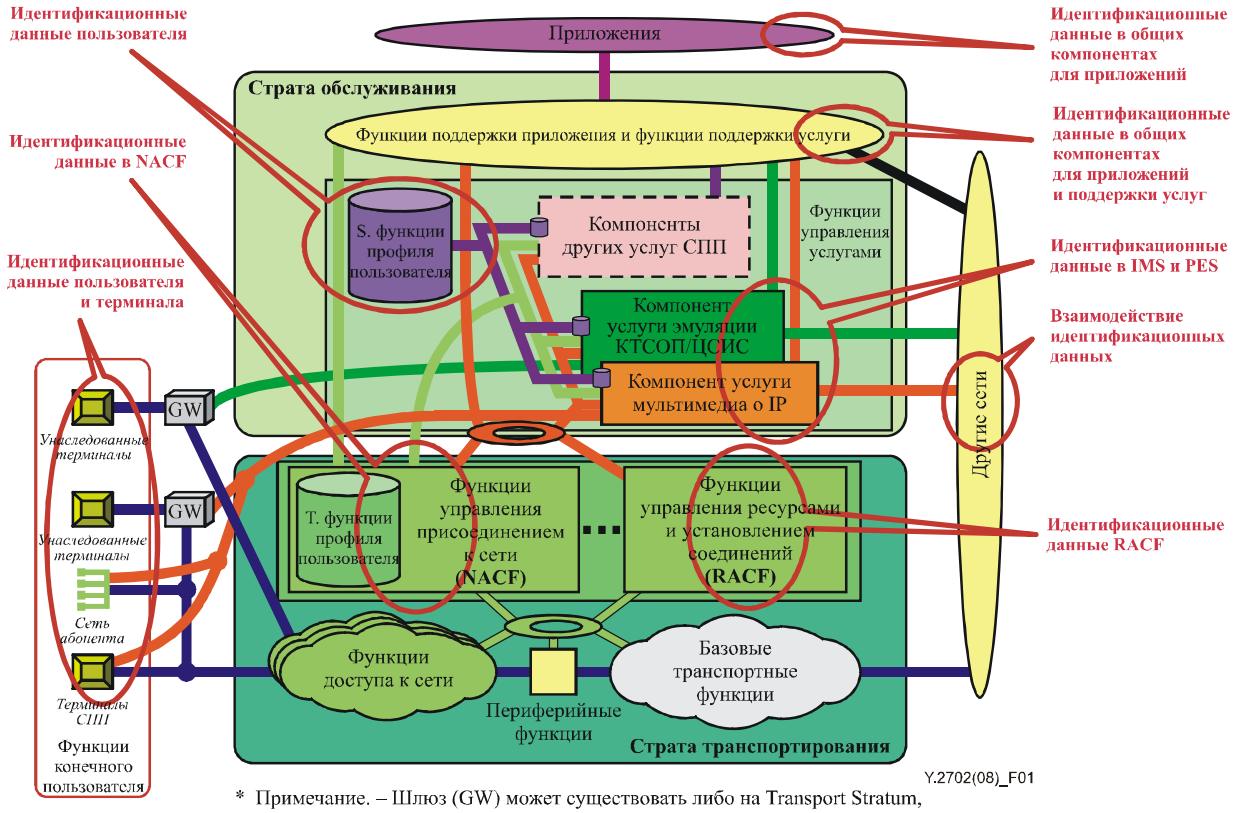
– потоки в канале передачи, трафике сигнализации и управления.

Отличительные идентификаторы используются для однозначного заявления подлинности в пределах данного домена безопасности. Отличительные идентификаторы отличают администратора доступа от других объектов в том же домене одним из следующих способов:

1) в силу членства в группе объектов, рассматриваемых эквивалентными для целей аутентификации (в этом случае вся группа рассматривается как один администратор доступа и имеет один отличительный идентификатор); или

2) путем идентификации одного и только одного объекта.

Если аутентификация осуществляется между разными доменами безопасности, отличительный идентификатор может оказаться недостаточным для однозначной идентификации объекта, поскольку органы разных доменов безопасности могут использовать те же отличительные идентификаторы. В этом случае для обеспечения однозначного идентификатора объекта отличительные идентификаторы должны использоваться в сочетании с идентификатором домена безопасности.



* Примечание. – Шлюз (GW) может существовать либо на Transport Stratum, либо в составе функций конечного пользователя.

Рисунок 1 – Пример идентификаторов СПП

Идентификационные данные для идентификации администратора доступа или объекта могут использоваться компонентами и функциональными элементами в разных стратах и уровнях СПП. На рисунке 1 показан пример идентификаторов для СПП на основе рисунка 8 (Компоненты СПП) [ITU-T Y.2012].

Примерами типичных отличительных идентификаторов являются:

– имена в справочниках;
– сетевые адреса;
– AP-заголовки и AE-заголовки;
– идентификаторы объекта;
– имена лиц (единственные в пределах данного домена);
– пятиэлементные группы, в состав которых входят:
  • IP-адрес источника;
  • IP-адрес пункта назначения;
  • номер порта источника;
  • номер порта пункта назначения; и
  • номер протокола.

5.1.3 Объекты аутентификации

Термин "предъявитель" используется для описания объекта, который является администратором доступа или представляет администратора доступа для целей аутентификации. Предъявитель обладает функциями, необходимыми для участия в аутентификационном обмене, от имени администратора доступа.

Термин "верификатор" используется для описания объекта, который является объектом, требующим аутентифицированных идентификационных данных, или его представителем. Верификатор обладает функциями, необходимыми для участи в аутентификационном обмене в целях запроса верификации предъявленных идентификационных данных.

Объект, участвующий во взаимной аутентификации, принимает на себя обе роли – предъявителя и верификатора.

Термин "доверенная третья сторона" используется для описания органа обеспечения безопасности или его агента, который пользуется доверием остальных объектов в отношении связанных с безопасностью действий. В контексте настоящей Рекомендации доверенная третья сторона является доверенной по отношению к предъявителю и/или верификатору для целей аутентификации.

ПРИМЕЧАНИЕ. – Предъявитель или верификатор может включать несколько функциональных элементов, возможно, постоянно находящихся в других открытых системах.

5.1.4 Аутентификационная информация

В настоящем стандарте описаны следующие виды аутентификационной информации:

– обменная аутентификационная информация (обменная AI);

– предъявляемая аутентификационная информация (предъявляемая AI);

– аутентификационная информация для верификации (AI для верификации).

Термин "аутентификационный обмен" используется для описания последовательности из одной или нескольких передач обменной AI для целей осуществления аутентификации.

На рисунке 2 показана взаимосвязь между предъявителем, верификатором и доверенной третьей стороной. Кроме того, на рисунке 2 показаны также все три вида аутентификационной информации, которые могут составлять содержание аутентификационного обмена.

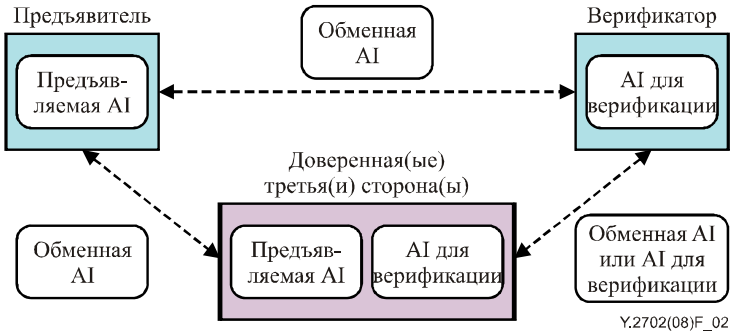


Рисунок 2 – Взаимосвязь между предъявителем, верификатором и доверенной третьей стороной

В некоторых случаях для генерирования обменной AI у предъявителя может возникнуть необходимость взаимодействия с доверенной третьей стороной. Аналогично, для верификации обменной AI у верификатора может возникнуть необходимость взаимодействия с доверенной третьей стороной. В этих случаях доверенная третья сторона может сохранять AI для верификации, относящуюся к администратору доступа.

Также возможно участие доверенной третьей стороны в передаче обменной AI. В зависимости от обмена эта третья сторона может принимать по отношению к верификатору роль предъявителя.

Для объектов может также оказаться необходимым сохранять аутентификационную информацию, которая должна использоваться при аутентификации доверенной третьей стороны.

5.1.5 Многофакторная аутентификация

Многофакторная аутентификация включает проверку аутентичности идентификационных данных администратора доступа путем проверки многих идентификаторов и атрибутов, связанных с администратором доступа. В общем, многофакторная аутентификация может быть организована на основании следующего группирования атрибутов аутентификации:

1) нечто личное (например, физические параметры поведенческих характеристик конечного пользователя либо характеристика или атрибут клиента, который может сравниваться в качестве неизменного шаблона, распознавание голоса);

2) нечто имеющееся (например, водительские права, жетон безопасности);

3) нечто известное (например, пароль, PIN-номер, секретное изображение).

Наиболее общим примером однофакторной аутентификации является пароль (нечто известное). Часто пароли, сами по себе, не обеспечивают достаточной уверенности в подлинности объекта, а для доступа к определенным ресурсам, приложениям и услугам СПП требуются более строгие формы аутентификации, включающие другие аутентификационные ключи. Это определяется риском, связанным с вероятностью получения доступа к ресурсам, приложениям и услугам СПП объектами, не имеющими соответствующих прав.

Аутентификационные факторы и ключи должны выбираться исходя из подлежащих учету рисков. В частности, необходимо оценивать последствия получения доступа к ресурсам, приложениям и услугам СПП объектами, не имеющими соответствующих прав, в аспекте определения требуемой формы аутентификации. Примерами электронных аутентификационных ключей являются:

– пароли;

– аппаратные жетоны;

– программные жетоны;

– устройства-жетоны одноразового пароля.

Широко применяется аутентификация на основе пароля. Пароль – это секретные данные, которые запоминает и использует для установления своей подлинности предъявитель. Паролями, как правило, являются строки символов или изображения, которые запоминает абонент и которые он должен идентифицировать, если они представлены наряду с другими аналогичными изображениями. Система паролей, однако, чувствительна ко многим видам атак. Для защиты паролей может использоваться дополнительная защита канала связи, но это не обеспечит предотвращения всех атак.

Аппаратные жетоны – это специальные устройства, которые защищают секретную информацию (обычно шифроключи) и выполняют криптографические операции. Аутентификация заключается в доказательстве владения таким устройством и управления ключом. Криптографические операции поддерживают аутентификацию обеих сторон и защиту канала, используемого для аутентификационного обмена.

Программные жетоны – это по сути программная реализация аппаратных жетонов, обладающая многими преимуществами аппаратных жетонов (например, шифроключ, который, как правило, хранится на диске или ином носителе). Программный ключ-жетон может кодироваться с использованием ключа, полученного из определенных данных активирования. Обычно данными активирования является известный только пользователю пароль, поэтому для активирования жетона требуется пароль. Аутентификация заключается в доказательстве владения и управления ключом. Как и в случае аппаратных жетонов, программные жетоны поддерживают аутентификацию обеих сторон и защиту канала, используемого для аутентификационного обмена.

Устройство-жетон одноразового пароля – это персональное аппаратное устройство, генерирующее "одноразовые" пароли для аутентификации. Системы одноразовых паролей основаны на последовательности паролей, которые генерируются по специальному алгоритму. Пароль в такой последовательности называется одноразовым паролем, поскольку он отличается от других генерируемых паролей и может использоваться только один раз. Существует широкий спектр систем одноразового пароля, которые обеспечивают различную степень защиты от атак.

5.2 Угрозы в отношении аутентификации

Аутентификационный факторы и ключи могут подвергаться следующим атакам:

1) "нечто личное" – дублирование сравниваемых характеристик или атрибутов клиента (например, отпечатков пальцев, неизменных шаблонов т. д.);

2) "нечто имеющееся" – получение или копирование того, чем обладает клиент;

3) "нечто известное" – определение информации, которая известна клиенту.

В целом, угрозы для аутентификации можно разделить на угрозы, которые включают атаки в отношении протокола аутентификации, и прочие угрозы, которые направлены либо на обнаружение значений жетона, либо на раскрытие конфиденциальной информации.

Использование многофакторной аутентификации повышает уровень безопасности, поскольку вынуждает преодолевать несколько методов защиты. Применение аппаратного устройства (нечто имеющееся), копирование которого осуществить непросто, также сужает границы атаки, поскольку предполагается, что владелец заметит пропажу устройства. Аутентификационные ключи, базирующиеся на программных или аппаратных жетонах, могут применяться в сочетании с данными активирования (например, паролем), образуя таким образом двухфакторную аутентификацию, для которой недостаточно только обладания жетоном.

Клиент может преодолеть систему аутентификации, умышленно открывая сообщнику свой ключ однофакторной аутентификации и позже отказываясь от него, с тем чтобы отрицать последующие удачные аутентификации. Использование нескольких аутентификационных факторов делает такой отказ менее достоверным и может останавливать атаки этого вида.

5.2.1 Угрозы в отношении протокола аутентификации

Примеры угроз в отношении протокола аутентификации включают:

1) Перехватчики:
   - перехватчики осуществляют наблюдение за обменом сообщениями протокола аутентификации для дальнейшего их анализа;
   - перехватчики в целом пытаются получить жетоны, с тем чтобы представляться в роли предъявителей.
2) Самозванцы:
   - самозванцы-предъявители, связываясь с верификатором, выдают себя за абонентов с целью проверки предполагаемых жетонов или получения иной информации о конкретном абоненте;
   - самозванцы-верификаторы выдают себя за верификаторов с целью легализации предъявителей-абонентов для получения жетонов, которые впоследствии возможно использовать для имитирования абонентов в целях легализации верификаторов;
   - самозванцы – доверяющие стороны, связываясь с верификатором, выдают себя за систему доверяющих сторон для получения требующей защиты пользовательской информации.
3) Угонщики:
   - угонщики перехватывают аутентифицированный сеанс и, связываясь с доверяющей стороной, выдают себя за абонентов в целях получения требующей защиты информации или введения неверной информации;
   - угонщики перехватывают аутентифицированный сеанс и, связываясь с верификаторами, выдают себя за доверяющую сторону в целях получения требующей защиты информации или введения неверной информации.

Таким атакам можно противостоять следующим образом:

– требуя элемент обновления для каждой аутентификации, с тем чтобы избежать атак путем замещения оригинала;

– атакам со стороны перехватчиков и угонщиков сеансов можно противостоять, используя криптографию для защиты канала сигнализации (канальное шифрование), по которому осуществляется аутентификационный обмен (например, TLS в анонимном режиме);

– атакам со стороны "посредников" и имитации верификатора можно противостоять ограниченным образом, используя защиту, аналогичную случаю атак со стороны перехватчиков и угонщиков сеансов. Защиту от таких атак усиливает сочетание шифрования с дополнительными криптографическими методами (например, использование двустороннего обмена "рукопожатиями" на основе повсеместной криптографии, – такой как TLS в аутентифицированном режиме, – с шифроключами, хранящимися у клиента и у верификатора, позволяет добиться жесткой взаимной аутентификации);

– шифрование обеспечивает лишь ограниченное противостояние атакам со стороны "посредников" и имитации верификатора, поскольку безопасность обмена может быть нарушена без нарушения шифрования. Например, клиент может быть убежден в том, что он ведет аутентификационный обмен с верификатором, в то время как это не соответствует действительности. Криптографические методы взаимной аутентификации могут применяться между клиентом и верификатором.

5.2.2 Угрозы в отношении аутентификационного жетона

Если совершающий атаку объект сможет получить управление жетоном, он получит возможность выдавать себя за владельца этого жетона. Угрозы в отношении жетонов могут быть разбиты на категории атак в отношении аутентификационных ключей следующим образом:

– Нечто имеющееся может быть похищено у владельца или имитироваться атакующим. Например, имеющая доступ к компьютеру владельца нападающая сторона может скопировать программный жетон. Аппаратный жетон может быть похищен или дублирован.

– Нечто известное может стать известным атакующему. Нарушитель может догадаться о содержании пароля или номера PIN. Если жетон перестает быть секретным, атакующий может получить доступ к верификатору и узнать секретное значение. Для получения таких данных нападающая сторона может установить вредоносное программное обеспечение (например, программу-перехватчика вводимой с клавиатуры информации). Кроме того, атакующий может определить секретные данные путем офлайновых атак на сетевой трафик процесса аутентификации.

– Нечто личное может быть дублировано. Нападающая сторона может получить копию идентификационных данных владельца жетона и создать его точную копию.

Для противостояния таким атакам существует ряд методов:

– Наличие нескольких факторов создает порог для атак. Если нападающей стороне необходимо похитить шифроключ и догадаться о содержании пароля, фактор трудоемкости может оказаться слишком высоким.

– Во избежание похищения или дублирования жетона могут использоваться средства физической защиты. Средства физической защиты могут обеспечивать фиксацию, обнаружение взлома и ответные меры.

– Сложные пароли могут снизить вероятность правильного угадывания. Требование использования длинных паролей, которые отсутствуют в общих словарях, может вынудить нарушителя опробовать каждый возможный пароль.

– Для предотвращения получения нападающей стороной доступа к системе или установления ею вредоносного программного обеспечения могут использоваться функции управления безопасностью системы и сети.

5.2.3 Другие угрозы в отношении аутентификации

Цели атак не ограничиваются собственно протоколом аутентификации. Возможны иные атаки, а именно:

– атаки посредством вредоносного кода, который может нарушить секретность аутентификационных жетонов;

– атаки-вторжения для получения удостоверения или жетонов путем проникновения к абоненту/предъявителю, в орган безопасности или систему верификатора;

– внутрисистемные угрозы, направленные на нарушение секретности аутентификационных жетонов;

– внешние атаки для получения жетона иным путем, такие как психологические атаки на абонента, с тем чтобы вынудить его сообщить нападающему свой пароль, или атаки типа "взгляд через плечо";

– атаки, целью которых является введение в заблуждение предъявителей, с тем чтобы они использовали незащищенный протокол, полагая, что используют защищенный, или обманным путем заставить их обойти контроль безопасности (например, принимая сертификаты сервера, которые не могут быть проверены);

– преднамеренное отрицание со стороны абонентов, умышлено нарушивших секретность своих жетонов.

Обучение клиентов и предоставление им консультаций – методы борьбы с вредоносным программным кодом и психологическими атаками. Обнаружение отклонения от нормального состояния широко используется для противодействия атакам на клиентов с целью мошенничества. Применение нескольких аутентификационных ключей может предотвращать атаки на клиентов в целях мошенничества. Внутрисистемным атакам можно противостоять путем проведения личного досмотра, контроля и (в надлежащих случаях) используя разделение обязанностей и двустороннее управление.

5.3 Гарантированность аутентификации

Для защиты ресурсов, приложений и услуг СПП поставщики СПП должны определять требуемый уровень гарантированности в процессе аутентификации, предназначенной для доступа в сеть и транзакций с приложениями/услугами.

Все поставщики СПП должны разработать и внедрить процесс гарантированности аутентификации. Процесс гарантированности аутентификации включает метод определения категорий доверия (то есть доверия к содержащейся в идентификационных данных информации, электронным образом представленной поставщику услуг) для механизмов аутентификации и представляемой для аутентификации информации.

Процесс гарантированности аутентификации заключается в определении и использовании относительных и дискретных уровней гарантированности для количественного измерения доверия к процессу аутентификации. Например, может использоваться "n" уровней гарантированности аутентификации. Уровень 0 может представлять низший уровень гарантированности, а уровень "n" – высший. Для определения уровня гарантированности в аспекте вероятных последствий (например, характера потенциальных воздействий) ошибки аутентификации, исходя из допущения, что все используемые при аутентификации идентификаторы не являются равными или необязательно имеют то же аутентификационное значение, будут использоваться "n" уровней.

Ниже представлен пример метода определения гарантированности аутентификации:

Пример метода аутентификации	
Уровень гарантированности	**Относительное доверие**
Уровень 0	Отсутствие доверия к утверждению о достоверности идентификационных данных (например, управление на основе списков доступа)
Уровень 1	Определенное доверие к утверждению о достоверности идентификационных данных
Уровень 2	Высокая степень доверия к утверждению о достоверности идентификационных данных
–	–
Уровень n	Высшая степень доверия к утверждению о достоверности идентификационных данных

Поставщик СПП должен оценивать потенциальные риски, связанные с последствиями ошибок аутентификации, или определять надлежащий уровень гарантированности подлинности объекта (например, конечного пользователя). В случае ошибок аутентификации, вызывающих потенциально худшие последствия, требуются более высокие уровни гарантированности.

Риск ошибки аутентификации является функцией двух факторов:

a) потенциальное причинение вреда или воздействие;

b) вероятность такого причинения вреда или воздействия.

Категории причинения вреда и воздействия включают, в том числе, следующие:

– неудобство, опасность или ущерб, связанные с положением или репутацией;

– финансовые потери;

– ответственность поставщика СПП или клиента;

– причинение вреда инфраструктуре, ресурсам, приложениям, службам или общественным интересам поставщика СПП;

– причинение вреда общественным и государственным интересам (например, связь критического характера, такая как ETS и TDR);

– несанкционированное разглашение конфиденциальной информации;

– причинение вреда службам личной безопасности;

– гражданские и уголовные правонарушения.

5.4 Авторизация и управление привилегиями

Аутентификации, самой по себе, недостаточно для определения того, какие действия разрешены аутентифицированному объекту по получении им доступа. Аутентификация должна применяться в сочетании с авторизацией и механизмами управления привилегиями, а также подходами, направленными на обеспечение управления доступом к услугам и ресурсам СПП. Например, назначение ролей и привилегий конечным пользователям/абонентам для контроля доступа к услугам и приложениям, а также интерфейсам управления для реализации управления их подписками и профилями. Другим примером является управление доступом на основе ролей (RBAC) для контроля доступа к OAM&P.

Авторизация или привилегии могут рассматриваться как атрибут подлинности объекта. В зависимости от политики обеспечения безопасности привилегии авторизации объекта могут проверяться посредством аутентификации.

5.5 Сквозная эталонная модель архитектуры

В данном подразделе представлено описание сквозной эталонной модели, используемой в настоящей Рекомендации для организации и группирования требований к аутентификации. Эталонная модель иллюстрирует:

1) Аутентификацию и авторизацию пользователя для доступа в сеть (например, аутентификация и авторизация устройства конечного пользователя, шлюза домашней сети или шлюза предприятия для получения доступа в сеть или присоединения к сети).
2) Выполняемые поставщиком услуг аутентификацию и авторизацию пользователя для доступа к услугам/приложениям (например, аутентификация и авторизация пользователя, устройства или совместно пользователя/устройства, если аутентификация и авторизация применяются в целях получения доступа к услугам/приложениям СПП).
3) Выполняемые поставщиком услуг аутентификацию и авторизацию пользователя для доступа к определенным услугам/приложениям (например, специальная аутентификация и авторизация для ETS и TDR[1]).
4) Выполняемая пользователем аутентификация и авторизация сети (например, пользователь, выполняющий аутентификацию подлинности подсоединенной сети СПП или поставщика услуг).
5) Выполняемая пользователем одноранговая аутентификация и авторизация (например, аутентификация и авторизация вызываемого пользователя (или завершающего соединение пользователя), аутентификация и авторизация вызывающего объекта или аутентификация источника данных как сетевые функции).
6) Взаимная сетевая аутентификация и авторизация (например, аутентификация и авторизация по интерфейсу NNI на транспортном уровне или на уровне услуг/приложений).
7) Аутентификация и авторизация поставщика услуг/приложений.
8) Использование услуги аутентификации третьей стороны.

На рисунке 3 показаны опорные точки аутентификации, описанные выше.

В настоящей Рекомендации использование термина “пользователь” не ограничено физическим лицом. Пользователем может быть физическое лицо, группы, компании или юридические лица.

---

[1] Аутентификация для ETS может включать дополнительные требования, выходящие за пределы базовых требований.

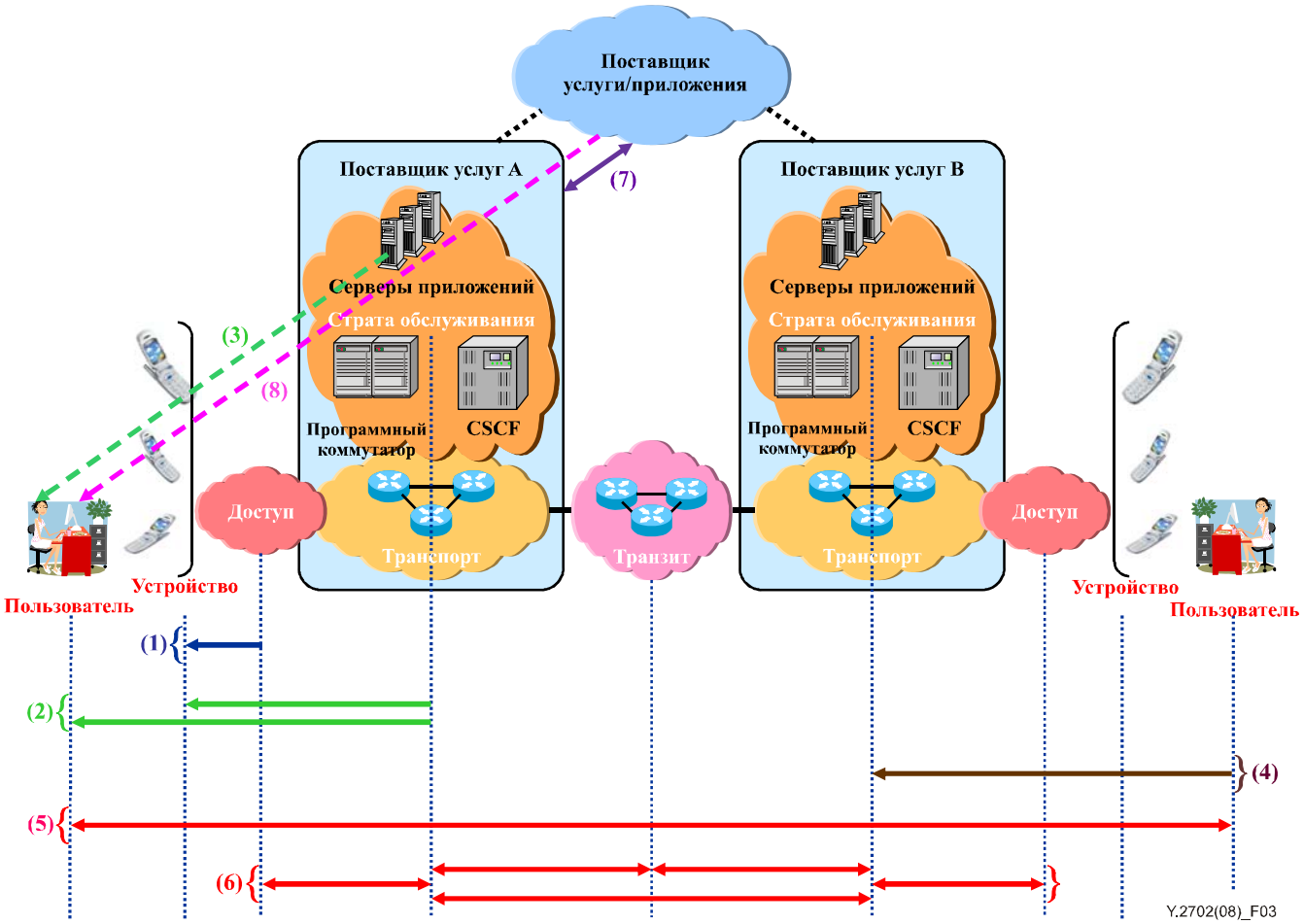


Рисунок 3 – Сквозная эталонная модель архитектуры

Как показано на рисунке 3 и аутентификация, и авторизация выполняются на транспортном уровне и на уровне услуг/приложений. Кроме того, возможны привязка и связка аутентификации. Например, поставщик услуг может организовать привязку/связку аутентификации пользователя и устройства пользователя, с тем чтобы обеспечить более высокий уровень гарантированности аутентификации. По большей части горизонтальная аутентификация выполняется от участка к участку. Основным исключением из этого является аутентификация пользователь-пользователь, которая имеет характер сквозной аутентификации. За исключением пользователя, выполняющего аутентификацию и авторизацию сети, взаимосвязи требуют взаимной аутентификации.

5.6 Взаимосвязь с архитектурой СПП, описанной в [ITU-T Y.2012]

В данном пункте описана взаимосвязь между эталонной моделью, представленной в настоящей Рекомендации, и функциональной моделью архитектуры, описанной в [ITU-T Y.2012]. В частности, выделено следующее:

– взаимосвязь одноранговой аутентификации рисунок 1 из [ITU-T Y.2012] "Общая схема архитектуры СПП";

– функциональные элементы на рисунке 1 из [ITU-T Y.2012], выполняющие функции аутентификации;

– функциональные элементы на рисунке 1 из [ITU-T Y.2012], осуществляющие управление идентификационными данными, корреляции и связки;

– функциональные элементы на рисунке 1 из [ITU-T Y.2012], обеспечивающие реализацию управления доступом на основе отказа в аутентификации.

На рисунке 4 представлен рисунок 1 из [ITU-T Y.2012] для иллюстрации взаимосвязей одноранговой аутентификации, определение которой приведено в пункте 5.5 настоящей Рекомендации. Взаимосвязи одноранговой аутентификации обозначены двунаправленными стрелками черного цвета. На рисунке не показана точка 5) – выполняемая пользователем одноранговая аутентификация и авторизация. Следует заметить, что даже если поставщиком приложений для пользователя является поставщик СПП (то есть интерфейс ANI отсутствует), тем не менее существует аутентификационная взаимосвязь между конечным пользователем и приложением, а также между стратой и приложением.

Рисунок 4 – Опорные точки одноранговой аутентификации

На рисунке 5 выделены функциональные объекты (FE) на основе эталонной модели [ITU-T Y.2012], которые обеспечивают или могут обеспечивать функции аутентификации и авторизации.

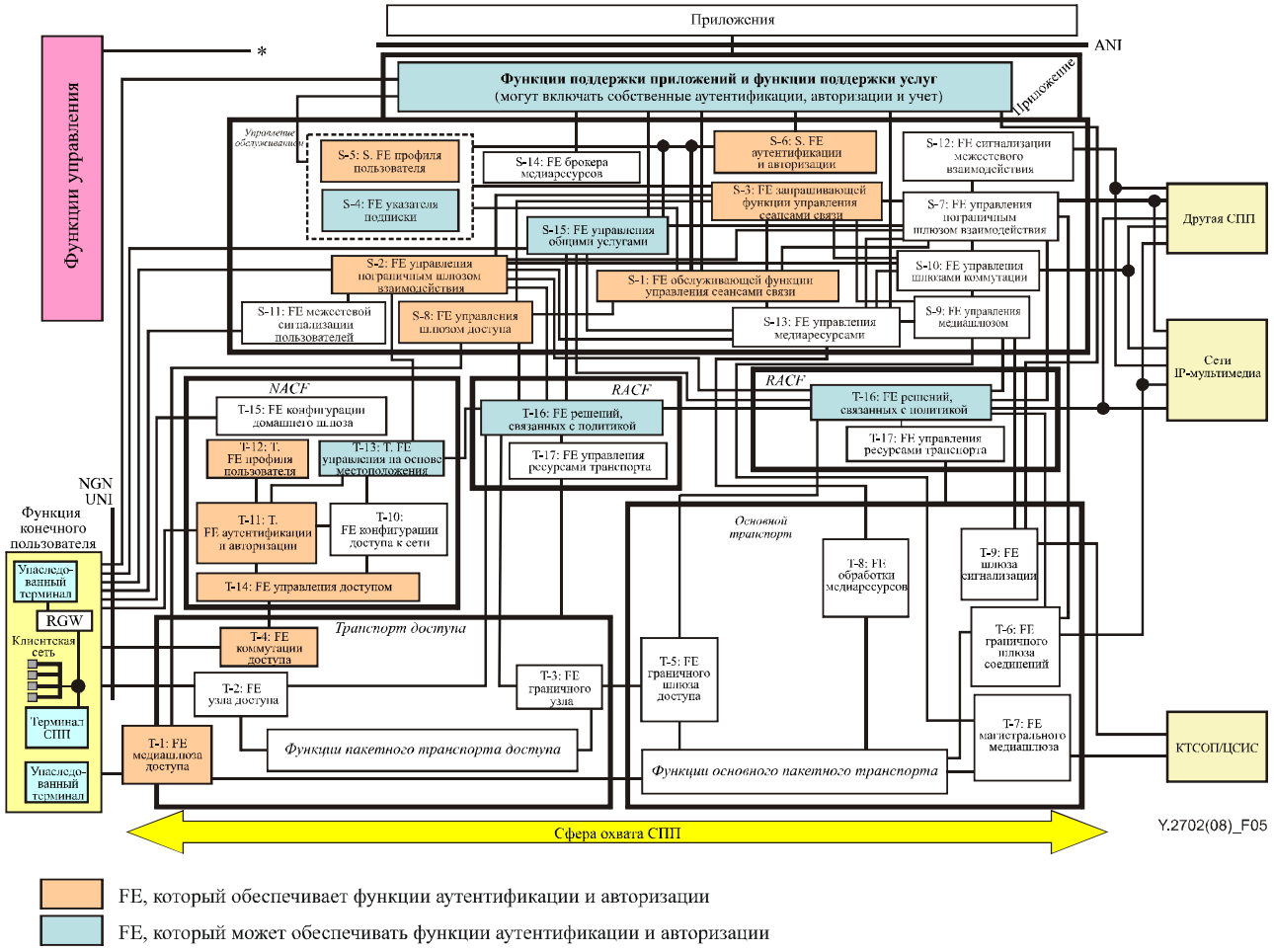


Рисунок 5 – Функциональные элементы аутентификации и авторизации [ITU-T Y.2012]

6 Общие требования

В настоящей Рекомендации необходима поддержка следующих общих требований к идентификации, аутентификации и санкционированию, определенных в [ITU-T Y.2701] и [ITU-T Y.2201]:

(R-1) – Должно обеспечиваться выполнение требований, определенных в пункте 7.3.2 (Аутентификация).

(R-2) – Должно обеспечиваться выполнение требований, определенных в пункте 6.12 (Идентификация, аутентификация и санкционирование) Рекомендации [ITU-T Y.2201].

7 Аутентификация и авторизация пользователя для доступа в сеть

7.1 Описание

Услуги и возможности аутентификации и авторизации пользователя для доступа в сеть необходимы для уменьшения объема угроз, связанных с несанкционированным доступом. Услуги аутентификации и авторизации для доступа в сеть требуются для проверки идентификационных данных и для определения того, должен ли быть предоставлен доступ оборудованию конечного пользователя (то есть оконечному оборудованию (TE) и оконечному оборудованию – пограничному элементу (TE-BE)), запрашивающему установление связи с СПП.

Общие допущения:

a) Конечный пользователь не ограничен физическим лицом. Конечным пользователем могут быть физическое лицо, группы, компании или юридические лица.

b) Согласно [ITU-T Y.2012] не делается никаких допущений относительно различных интерфейсов конечного пользователя и сетей конечного пользователя, которые могут быть подсоединены к сети доступа СПП. В СПП поддерживаются все категории оборудования конечного пользователя, от унаследованных однолинейных телефонов до составных корпоративных сетей. Оборудование конечного пользователя может быть либо мобильным, либо стационарным.

c) Определение сетевых элементов, реализующих услуги доступа и авторизации, не входит в сферу применения настоящей Рекомендации.

d) Функции доступа в сеть и авторизации могут выполняться как часть общей функции управления присоединением к сети (NACF), определенной в [ITU-T Y.2012].

7.2 Общая эталонная модель

На Рисунке 6 представлена эталонная модель аутентификации и авторизации для доступа в сеть/ присоединения к сети, в которую входят следующие домены безопасности:

1) Домен клиента – не доверенный домен, образуемый оборудованием пользователя, которое принадлежит клиенту и управляется им, например:

   a) унаследованное TE и TE-BE:

      - унаследованное TE – это унаследованные пользовательские устройства, подсоединенные по технологии узкополосного доступа (например, аналоговые линии и линии ЦСИС). Это TE получает доступ в IP-сеть через шлюз поставщика СПП (например, шлюз доступа или медиашлюз);
      - унаследованное TE-BE – это оборудование пользователя, выполняющее функции суммарных конечных точек (например, шлюзы сети предприятия и домашней сети), подсоединенное по технологии узкополосного доступа (например, аналоговые линии и линии ЦСИС). Это TE-BE получает доступ в IP-сеть через шлюз поставщика СПП (например, шлюз доступа или медиашлюз);

   b) унаследованное TE и TE-BE с интегрированным устройством доступа (IAD):

      - унаследованное TE с IAD – унаследованные пользовательские устройства, подсоединенные по технологии широкополосного доступа (например, xDSL или кабель). Это TE получает доступ в IP-сеть через IAD в домене клиента;
      - унаследованное TE-BE – это оборудование пользователя, выполняющее функции суммарных конечных точек (например, шлюзы сети предприятия и домашней сети), подсоединенное по технологии широкополосного доступа (например, xDSL или кабель). Это пользовательское оборудование получает доступ в IP-сеть через IAD в домене клиента;

   c) TE и TE-BE СПП:

      - TE СПП – это пользовательские устройства в домене клиента, обладающие IP-возможностями для поддержки прямого установления соединения с IP-сетью (например, используя xDSL и широкополосный доступ по кабелю);
      - TE-BE СПП – это оборудование пользователя, выполняющее функции суммарных конечных точек (например, шлюзы сети предприятия и домашней сети), обладающее IP-возможностями для поддержки прямого установления соединения с IP-сетью.

2) Домен поставщика СПП доступа: сеть доступа, управляемая поставщиком СПП (например, узкополосная, xDSL и кабель). Поставщик доступа в СПП может быть или может не быть одновременно поставщиком услуг СПП. Доверительные взаимоотношения между поставщиками СПП регулируются соглашениями об уровне обслуживания (SLA).

3) Домен поставщика услуг СПП: поставщик услуг СПП предоставляет своим абонентам прикладные услуги СПП. Взаимоотношения между поставщиками СПП регулируются соглашениями SLA.

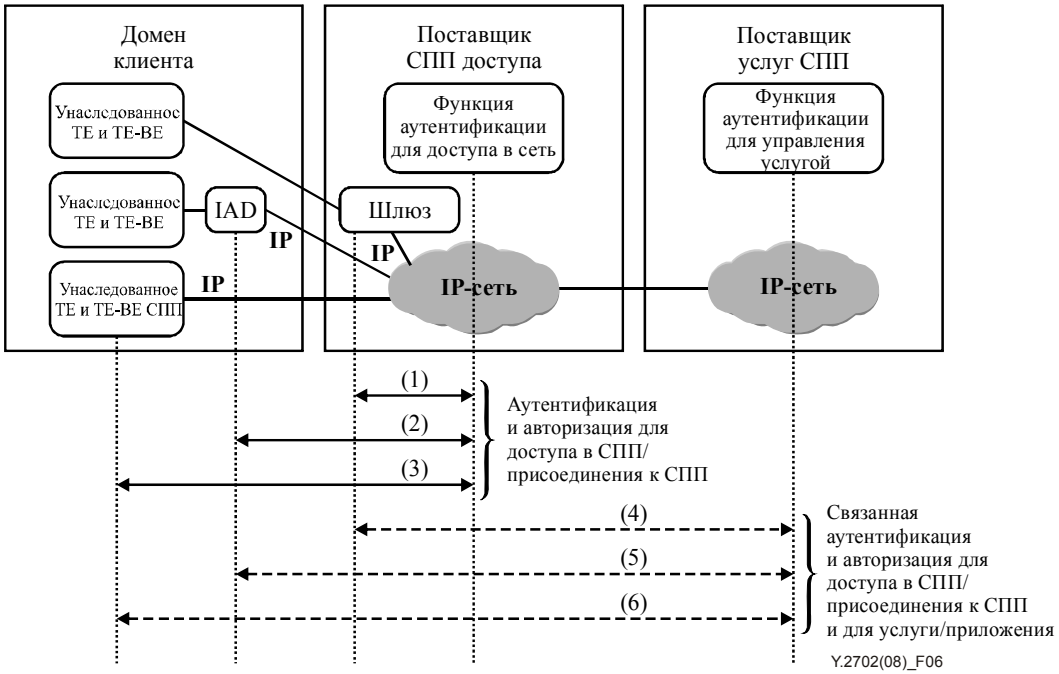


Рисунок 6 – Эталонная модель аутентификации и авторизации для доступа в сеть/присоединения к сети

На рисунке 6 показаны взаимосвязи при аутентификации и авторизации для доступа в сеть/ присоединения к сети:

а) Аутентификация и авторизация устройства для доступа в СПП/присоединения к СПП – услуги и возможность выполнения идентификации, аутентификации и авторизации доступа пользовательских устройств в IP-сеть доступа или присоединения к ней.

1) Этот информационный поток представляет услуги и возможности выполнения идентификации, аутентификации и авторизации унаследованного ТЕ и ТЕ-ВЕ для доступа в IP-сеть доступа/присоединения к ней. Данный информационный поток существует между шлюзом (предъявитель) в домене СПП доступа и соединяет унаследованное ТЕ и ТЕ-ВЕ в домене клиента и сетевой элемент (например, точку доступа в сеть) в домене СПП доступа, обеспечивающий функции аутентификации и авторизации для доступа в СПП/присоединения к СПП. Функции аутентификации и авторизации для доступа в СПП/присоединения к СПП (верификатор) могут быть частью общей функции управления присоединением к сети (NACF), определенной в [ITU-T Y.2012]. Однако, если эта функция реализована, она определяется конкретной реализацией.

2) Этот информационный поток представляет услуги и возможности выполнения идентификации, аутентификации и авторизации унаследованного ТЕ и ТЕ-ВЕ, оборудованных IAD, в домене клиента для доступа в IP-сеть доступа/присоединения к ней. Данный информационный поток существует между IAD (предъявитель) в домене клиента и сетевым элементом (например, точкой доступа в сеть) в домене СПП доступа, обеспечивающим функции аутентификации и авторизации для доступа в СПП/присоединения к СПП. Функции аутентификации и авторизации для доступа в СПП/присоединения к СПП (верификатор) могут быть частью общей функции управления присоединением к сети (NACF), определенной в [ITU-T Y.2012]. Однако, если эта функция реализована, она определяется конкретной реализацией.

3) Этот информационный поток представляет услуги и возможности выполнения идентификации, аутентификации и авторизации ТЕ и ТЕ-ВЕ СПП, обладающих IP-возможностями, в домене клиента для доступа в IP-сеть/присоединения к IP-сети. Данный информационный поток существует между ТЕ или ТЕ-ВЕ СПП (предъявитель) в домене клиента и сетевым элементом (например, точкой доступа в сеть) в домене СПП доступа, обеспечивающим функции аутентификации и авторизации для доступа в

СПП/присоединения к СПП. Функции аутентификации и авторизации для доступа в СПП/присоединения к СПП (верификатор) могут быть частью общей функции управления присоединением к сети (NACF), определенной в [Y.2012]. Однако, если эта функция реализована, она определяется конкретной реализацией.

b) Связанные аутентификация и авторизация устройства для доступа в СПП/присоединения к СПП и выполняемая услугой/приложением аутентификация и авторизация – услуги и возможности связать выполняемую поставщиком СПП доступа аутентификацию пользовательского устройства с выполняемой поставщиком услуг СПП аутентификацией и авторизацией пользователя:

   1) Этот информационный поток представляет услуги и возможности для поставщика услуг СПП выполнить однозначную идентификацию и авторизацию унаследованного ТЕ и ТЕ-ВЕ. Данный информационный поток существует между шлюзом (предъявитель) в домене сети доступа и доменом поставщика услуг СПП (верификатор).

   2) Этот информационный поток представляет услуги и возможности для поставщика услуг СПП выполнить однозначную идентификацию и авторизацию унаследованного ТЕ и ТЕ-ВЕ, оборудованного IAD. Данный информационный поток существует между IAD (предъявитель) в домене клиента и доменом поставщика услуг СПП (верификатор).

   3) Этот информационный поток представляет услуги и возможности для поставщика услуг СПП выполнить прямую идентификацию, аутентификацию и авторизацию ТЕ и ТЕ-ВЕ СПП в домене клиента. Данный информационный поток существует между ТЕ и ТЕ-ВЕ СПП (предъявитель) в домене клиента и доменом поставщика услуг СПП (верификатор).

Эталонная модель для обеспечения кочевого характера связи

На рисунке 7 представлена эталонная модель для обеспечения кочевого характера связи. Эта эталонная модель аналогична общей эталонной модели, за исключением того, что при таком сценарии существуют посещаемая СПП и домашняя СПП, которые надлежит учитывать.

1) Домен посещаемой СПП: СПП, управляемая поставщиком посещаемой СПП. Предоставляет функции посещаемой сети поставщику другой СПП (например, поставщику домашней сети). Доверительные отношения регулируются соглашениями SLA. Помещаемая сеть может предоставлять услуги СПП и может иметь собственных абонентов.

2) Домен домашней СПП: СПП, управляемая поставщиком домашней СПП. Поставщик домашней СПП предоставляет услуги СПП своим абонентам. Доверительные отношения регулируются соглашениями SLA.

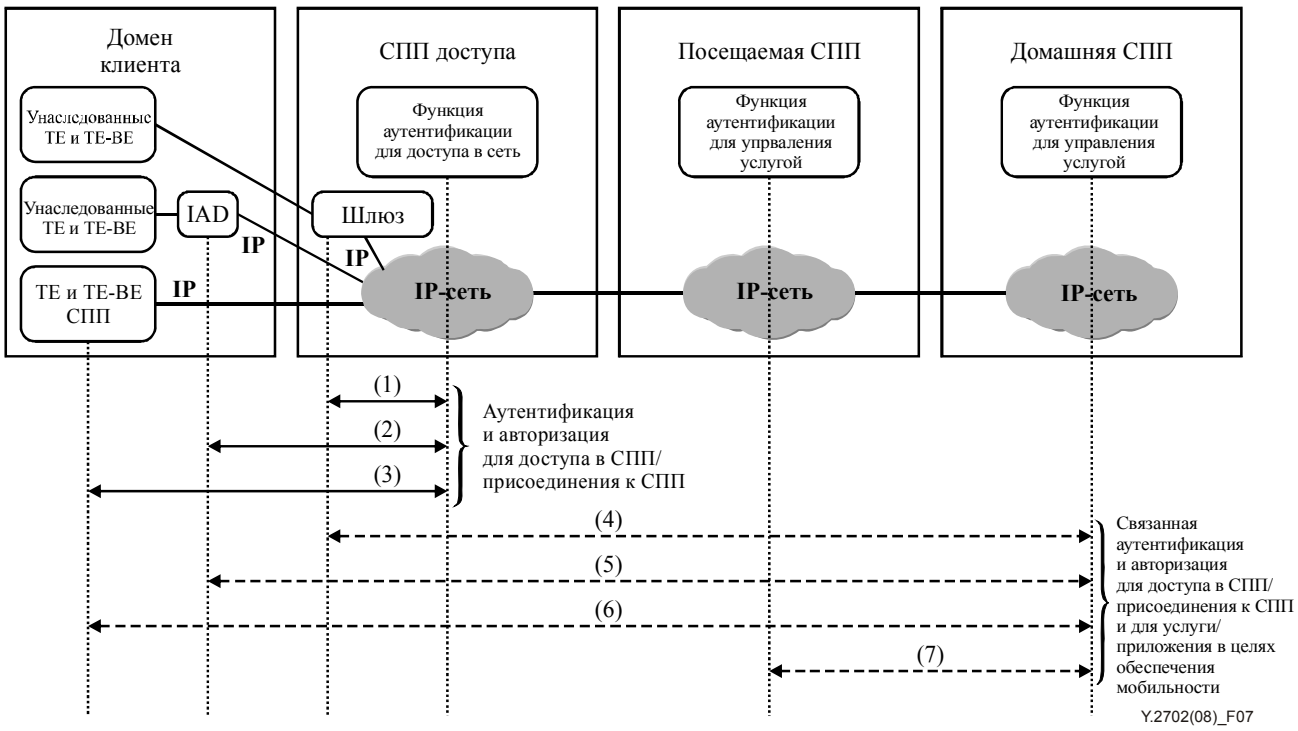


Рисунок 7 – Эталонная модель для обеспечения кочевого характера связи

На эталонной модели показаны информационные потоки между разными доменами для связи аутентификации и авторизации пользовательского устройства и аутентификации и авторизации пользователя в целях обеспечения кочевого характера связи. Данные информационные потоки представляют услуги и возможности для связи выполняемой поставщиком посещаемой СПП аутентификации и авторизации пользовательского устройства и выполняемой поставщиком домашней СПП аутентификации и авторизации пользователя в целях обеспечения кочевого характера связи:

1)–6) – Эти информационные потоки аналогичны потокам, описанным для сценария с одним поставщиком услуг на рисунке 6.

7) – Этот информационный поток представляет услуги и возможности обмена информацией идентификации, аутентификации и авторизации, обеспечиваемые для поставщика посещаемой СПП и поставщика домашней СПП в целях поддержки кочевого характера связи.

7.3 Требования

7.3.1 Общие требования

Ниже представлены общие требования, относящиеся к идентификации, аутентификации и авторизации устройства для доступа в сеть/присоединения к сети.

(R-3) – Необходимо, чтобы СПП обладали способностью однозначной идентификации устройств конечного пользователя/абонента (например, ТЕ и ТЕ-ВЕ) на основании политики поставщика СПП.

(R-4) – Необходимо, чтобы СПП обладали способностью идентификации, аутентификации и авторизации ТЕ и ТЕ-ВЕ в точках доступа в сеть (NAP).

(R-5) – Необходимо, чтобы доступ в сеть предоставлялся только зарегистрированному ТЕ и ТЕ-ВЕ.

(R-6) – В случае многосетевых схем необходимо, чтобы административный домен каждой сети (например, провайдера СПП доступа, провайдера посещаемой СПП и провайдера домашней СПП), осуществляя идентификацию, аутентификацию и авторизацию ТЕ и ТЕ-ВЕ для доступа в сеть/присоединения к сети (например, используя соглашения SLA), обеспечивал соблюдение принятой политики (например, доверительные взаимоотношения).

(R-7) – Необходимо, чтобы СПП поддерживали возможности защиты информации аутентификации и авторизации (например, профилей пользователей, информации подписки, идентификационных шаблонов) от несанкционированного доступа, манипуляции с данными и повреждения данных.

(R-8) – Необходимо, чтобы СПП поддерживали возможности обеспечения конфиденциальности и целостности защиты сообщений и информации, участвующих в обмене в целях аутентификации и авторизации.

(R-9) – Необходимо, чтобы СПП поддерживали возможности защиты от атак (например, атак типа повторная передача перехваченного сообщения и отказ в обслуживании), предпринимаемых в отношении функций и возможностей аутентификации и авторизации.

(R-10) – Необходимо, чтобы СПП обладали способностью обнаружения и регистрации предпринимаемых попыток несанкционированного доступа (например, может быть установлен конфигурируемый порог системы для некоторого числа попыток несанкционированного доступа, при превышении которого генерируется регистрируемый и сообщаемый системе управления сигнал тревоги).

7.3.2 Унаследованное TE и TE-BE

Точки NAP, поддерживающие доступ в сеть для унаследованного TE и TE-BE, должны поддерживать возможности идентификации, аутентификации и авторизации такого доступа.

(R-11) – Необходимо, чтобы точки доступа в сеть (NAP), поддерживающие унаследованное TE и TE-BE, поддерживали возможности однозначной идентификации линии фиксированной связи для присоединения или подключения к СПП. Для идентификации линии фиксированной связи (например, MAC или адрес уровня канала передачи) может использоваться адрес уровня 2. Эта функция может обеспечиваться как часть общей функции NACF, определенной в [ITU-T Y.2012].

(R-12) – Необходимо, чтобы точки NAP, поддерживающие унаследованное TE и TE-BE, поддерживали возможности аутентификации и авторизации линии фиксированной связи для присоединения или подключения к СПП. Для авторизации доступа линии фиксированной связи в СПП могут использоваться списки управления доступом (ACL) и информация подписки/профиля пользователя страты транспортирования. Эти функции могут обеспечиваться как часть общей функции NACF, определенной в [ITU-T Y.2012].

(R-13) – Необходимо, чтобы точки NAP, поддерживающие унаследованное TE и TE-BE, поддерживали возможность установления связи и связывания идентификационных данных линии фиксированной связи с IP-адресом, используемым для подключения в целях доступа к СПП. Эта функция может обеспечиваться как часть общей функции NACF, определенной в [ITU-T Y.2012].

7.3.3 Унаследованное TE и TE-BE, оборудованное IAD

Точки NAP, поддерживающие доступ в сеть для унаследованного TE и TE-BE с IAD, в домене клиента должны поддерживать возможности идентификации, аутентификации и авторизации такого доступа.

(R-14) – Необходимо, чтобы точки NAP, поддерживающие унаследованное TE и TE-BE с IAD, в домене клиента поддерживали возможности однозначной идентификации линии фиксированной связи и IAD для присоединения или подключения к СПП. Для идентификации линии фиксированной связи (например, MAC или адрес уровня канала передачи) может использоваться адрес уровня 2. Эта функция может обеспечиваться как часть общей функции NACF, определенной в [ITU-T Y.2012].

(R-15) – Необходимо, чтобы точки NAP, поддерживающие унаследованное TE и TE-BE с IAD, в домене клиента поддерживали возможности аутентификации и авторизации IAD для подсоединения или подключения к СПП. Получать присоединение или сетевое подключение к СПП разрешается только зарегистрированным IAD. Для авторизации доступа IAD и линии фиксированной связи в СПП могут использоваться списки управления доступом (ACL) и информация подписки/профиля пользователя страты транспортирования. Эти функции могут обеспечиваться как часть общей функции NACF, определенной в [ITU-T Y.2012].

(R-16) – Необходимо, чтобы точки NAP, поддерживающие унаследованное TE и TE-BE с IAD, в домене клиента поддерживали возможность установления связи и связывания идентификационных данных линии фиксированной связи с идентификационными данными IAD. Эта функция может обеспечиваться как часть общей функции NACF, определенной в [ITU-T Y.2012].

7.3.4 Оборудование TE и TE-BE СПП

Точки NAP, поддерживающие доступ в сеть для унаследованного TE и TE-BE СПП, в домене клиента должны поддерживать возможности идентификации, аутентификации и авторизации такого доступа в СПП.

(R-17) – Необходимо, чтобы точки NAP, поддерживающие TE и TE-BE СПП (то есть прямое IP-подключение), поддерживали возможности однозначной идентификации пользовательских устройств в рамках своего домена в целях присоединения и подключения к СПП. Оборудование TE и TE-BE СПП может однозначно идентифицироваться посредством идентификационных данных устройства и сетевых адресов (например, идентификационные данные оборудования, содержащие SIM карты, жетоны безопасности, IP-адреса и т. д.).

(R-18) – Необходимо, чтобы точки NAP, поддерживающие TE и TE-BE СПП (то есть прямое IP-подключение), поддерживали возможности аутентификации и авторизации пользовательских устройств в рамках своего домена для присоединения или подключения к СПП. Аутентификация и авторизация может базироваться на информации подписки/профиля пользователя страты транспортирования. Получать присоединение или сетевое подключение к СПП разрешается только зарегистрированному TE и TE-BE СПП. Эти функции могут обеспечиваться как часть общей функции NACF, определенной в [ITU-T Y.2012].

7.3.5 Связанная аутентификация и авторизация пользователя и устройства пользователя

Исходя из оценки риска, в случае если необходим более высокий уровень гарантированности подлинности, может потребоваться комбинация аутентификации и авторизации пользователя и устройства пользователя. СПП может поддерживать возможности связывания функций аутентификации для доступа в СПП/присоединения к СПП и доступа к услуге/приложению на базе информации страты транспортирования (например, информация, связанная с устройством пользователя и доступом в сеть) и страты обслуживания (например, подписка/профиль пользователя).

(R-19) – Необходимо, чтобы поддерживались возможности однозначной идентификации и связывания комбинации пользователя и устройства пользователя на основании политики поставщика СПП.

(R-20) – Необходимо, чтобы возможности аутентификации и авторизации комбинации пользователя и устройства пользователя поддерживались на основании политики поставщика СПП. Получать присоединение или сетевое подключение и доступ к услугам/приложениям разрешается только зарегистрированным пользователям и устройствам пользователей.

7.3.6 Связанная аутентификация и авторизация пользователя и устройства пользователя для обеспечения кочевого характера связи

Аутентификация и авторизация пользователя и устройства пользователя могут поддерживаться для обеспечения более высокого уровня гарантированности подлинности в целях обеспечения кочевого характера связи. Могут поддерживаться возможности обмена информацией идентификации, аутентификация и авторизация (например, информацией профилей пользователей) и совместного использования такой информации в разных административных доменах (то есть поставщика СПП доступа, поставщика посещаемой СПП и поставщика домашней СПП) для целей IdM (см. п. 8.2.2).

(R-21) – Необходимо, чтобы поддерживались возможности однозначной идентификации комбинации пользователя и устройства пользователя в целях обеспечения кочевого характера связи на основании политики поставщика СПП.

(R-22) – Необходимо, чтобы возможности аутентификации и авторизации комбинации пользователя и устройства пользователя для обеспечения кочевого характера связи поддерживались на основании политики поставщика СПП. В случае если услуга является не зависимой от устройства пользователя, в целях обеспечения более высокого уровня гарантированности подлинности аутентификации информации доступа, такая как линия фиксированной связи, местоположение или адрес доступа, может комбинироваться с аутентификацией пользователя.

8 Выполняемая поставщиком услуг СПП аутентификация и авторизация пользователя для доступа к услуге/приложению

8.1 Описание

Для уменьшения объема угроз, связанных с несанкционированным доступом к услугам и средствам, обеспечиваемым поставщиком СПП, требуются определенные возможности. Услуги и возможности аутентификации и авторизации требуются для проверки идентификационных данных пользователя и для определения того, следует ли разрешить этому пользователю получить услугу или выполнить некоторое действие, исходя из имеющихся у него привилегий. Аутентификация и авторизация для услуги/приложения может включать проверку идентификационных данных и авторизацию привилегий следующих объектов:

– пользователь;

– устройство пользователя;

– комбинация пользователя и устройства пользователя.

Согласно определенной в [ITU-T Y.2012] архитектуре функции аутентификации и авторизации для услуги/приложения будут поддерживаться в страте обслуживания с использованием информации подписки и профиля пользователя.

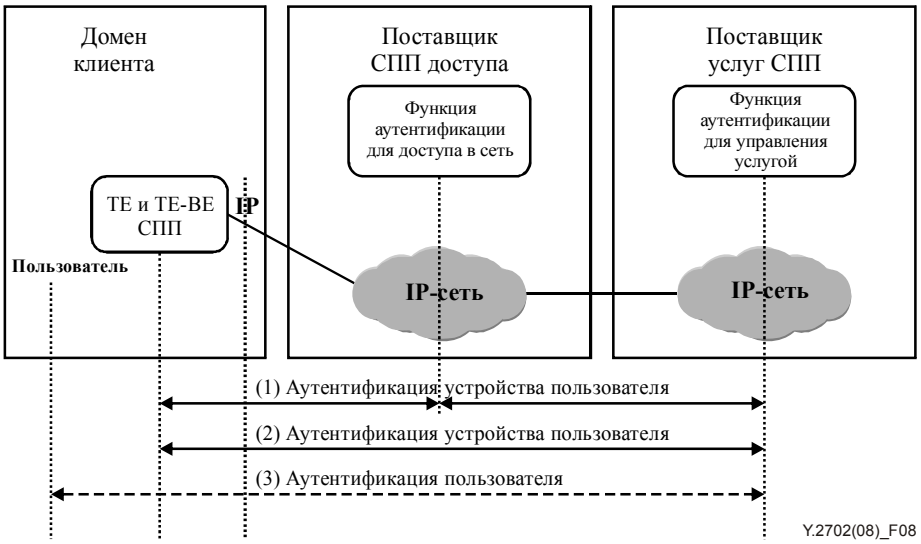


Рисунок 8 – Эталонная модель аутентификации и авторизации для доступа к услуге/приложению

На рисунке 8 представлен пример взаимосвязей при аутентификации и авторизации для доступа к услуге/приложению в случае сценария с несколькими поставщиками сети.

1 Этот информационный поток представляет поставщика услуг СПП на основе данных поставщика доступа к СПП для выполнения аутентификации устройства пользователя посредством доверительных взаимоотношений.

2 Этот информационный поток представляет выполняемую поставщиком услуг СПП аутентификацию устройства пользователя. Для этого случая устройство пользователя должно обладать определенными возможностями идентификации (например, SIM).

3 Этот информационный поток представляет выполняемую поставщиком услуг СПП аутентификацию пользователя (например, пользователь регистрируется и предоставляет пароль или PIN).

8.2 Требования

8.2.1 Общие требования

Ниже представлены общие требования, относящиеся к выполняемым поставщиком СПП идентификации, аутентификации и авторизации пользователя.

(R-23) – Необходимо, чтобы СПП поддерживали возможности идентификации пользователя, устройства пользователя и комбинации пользователя и устройства на основании данных подписки и профиля пользователя.

(R-24) – Необходимо, чтобы СПП поддерживали возможности аутентификации и авторизации пользователя, устройства пользователя и комбинации пользователя и устройства пользователя на основании информации подписки и профиля пользователя.

(R-25) – Необходимо, чтобы услуги СПП предоставлялись только зарегистрированным пользователям, устройству пользователя и комбинации пользователя и устройства пользователя.

(R-26) – Необходимо, чтобы СПП поддерживали возможности проверки и авторизации привилегий пользователя (например, разрешение пользователю выполнять определенные действия, только в случае авторизации его роли и привилегий).

(R-27) – В случае многосетевых схем необходимо, чтобы административный домен каждой сети (например, провайдер СПП доступа, провайдер посещаемой СПП и провайдер домашней СПП), осуществляя идентификацию, аутентификацию и авторизацию пользователя, устройства пользователя и комбинации пользователя и устройства пользователя, обеспечивал соблюдение принятой политики (например, соглашения SLA).

(R-28) – Необходимо, чтобы СПП поддерживали возможности обеспечения конфиденциальности и целостности защиты сообщений и информации, участвующих в обмене в целях аутентификации и авторизации пользователя, устройства пользователя и комбинации пользователя и устройства пользователя.

(R-29) – Необходимо, чтобы СПП поддерживали возможности защиты от несанкционированного доступа, манипуляции с информацией и повреждения информации аутентификации и авторизации для услуги (например, информация профилей пользователей и подписок).

(R-30) – Необходимо, чтобы СПП поддерживали возможности защиты от атак (например, атак типа повторная передача перехваченного сообщения и отказ в обслуживании), предпринимаемых в отношении функций и возможностей аутентификации и авторизации для услуги.

(R-31) – Необходимо, чтобы предусматривалась поддержка возможностей связывания аутентификации устройства пользователя, определяемой технологией сети доступа, с аутентификацией пользователя на основании политики поставщика СПП.

(R-32) – Необходимо, чтобы СПП обладали возможностью обнаружения и регистрации предпринимаемых попыток несанкционированного доступа к услугам и ресурсам СПП (например, может быть установлен конфигурируемый порог системы для некоторого числа попыток несанкционированного доступа, при превышении которого генерируется регистрируемый и сообщаемый системе управления сигнал тревоги).

(R-33) – Необходимо, чтобы СПП обладали возможностью обнаружения и регистрации попыток несанкционированного доступа (например, неразрешенные действия пользователя).

8.2.2 Совместное использование результатов аутентификации для целей IdM

У поставщика СПП может возникнуть потребность в обмене результатами аутентификации между разными услугами и/или приложениями в пределах своей сети и за ее пределами – с поставщиками других СПП – в целях поддержки служб управления идентификационными данными (IdM). Это может включать утверждения и иную информацию, актуальную для IdM, такого как, например (в том числе):

a) политика доверительных отношений;

b) метод аутентификации и информация, используемая для аутентификации (например, аутентификационные ключи);

c) уровни гарантированности;

d) информация управления привилегиями (например, назначенные и проверенные привилегии).

Возможности, обеспечивающие обмен в целях безопасности информацией о результатах аутентификации (например, утверждениями) и другой актуальной информацией, описанной выше, позволит поставщикам СПП проектировать платформы услуг/приложений, обладающие эффективными и удобными для пользователя средствами аутентификации и авторизации. Например, информация о результатах аутентификации может совместно использоваться системами (например, серверами приложений), поддерживающими разные услуги и/или приложения, с тем чтобы разрешить поставщику СПП поддержку функций и возможностей "однократной регистрации" для удобства пользователя. Представленные ниже требования применимы к обмену результатами аутентификации и к совместному их использованию с сетью поставщика СПП.

(R-34) – Необходимо, чтобы СПП поддерживали возможности, которые разрешают поддерживающим разные услуги и/или приложения системам и сетевым элементам (например, серверам приложений) обмениваться информацией о результатах аутентификации (например, утверждениями, информацией управления привилегиями, политикой доверия и уровнями гарантированности) безопасным образом и исходя из конкретных организации платформы услуг/приложений и политики обеспечения безопасности поставщика СПП.

(R-35) – Необходимо, чтобы связь между разными системами или сетевыми элементами (например, серверами приложений) для обмена информацией о результатах аутентификации или совместного использования этой информации была защищена от несанкционированного доступа, наблюдения, манипулирования или повреждения (например, защита конфиденциальности и целостности). Это включает защиту любой хранимой информации.

В многосетевой среде у поставщиков СПП может возникнуть потребность в обмене между собой результатами аутентификации и совместном использовании этих результатов безопасным образом на основе SLA. Следующие требования применимы к обмену результатами аутентификации и совместному использованию этих результатов разными поставщиками СПП.

(R-36) – Необходимо, что поставщики СПП поддерживали возможности, которые позволят поставщикам СПП обмениваться результатами аутентификации и совместно использовать эти результаты безопасным образом (например, по интерфейсам NNI и ANI), исходя из доверительных отношений, политики и соглашений SLA между поставщиками СПП.

(R-37) – Необходимо, чтобы связь между поставщиками СПП для обмена информацией о результатах аутентификации и совместного использования этой информации для целей IdM (то есть по интерфейсам NNI и ANI) была защищена от несанкционированного доступа, наблюдения, манипулирования или повреждения (например, защита конфиденциальности и целостности). Это включает защиту любой хранимой информации. Конкретные механизмы и практика обеспечения безопасности будут базироваться на доверительных отношениях, политике и соглашениях SLA, принятыми между поставщиками СПП.

(R-38) – Необходимо поддерживать возможности гарантирования метода аутентификации и передачи информации о методе(ах), который(е) использовался(ись) для аутентификации объектов для доверяющей стороны, а именно:

- метод проверки идентификационных данных пользователя;
- метод аутентификации (использование цифровых сертификатов, подписей, жетонов безопасности, биометрических данных, SIM и т. д.);
- политика доверительных отношений;
- уровни гарантированности аутентификации

Обмен информацией и результатами аутентификации осуществляются при условии соответствия соответствующим правилам, таким как национальные и региональные регуляторные положения и законодательства, касающиеся защиты персональной идентифицируемой информации (PII).

(R-39) – Требуется, чтобы оператор СПП обеспечил соответствие соответствующим правилам, таким как национальные и региональные регуляторные положения и законодательства, касающиеся защиты персональной идентифицируемой информации (PII). К ним относятся правила, основанные на следующих базовых принципах защиты данных:

- привязка данных к конкретной цели;
- обмен данными между приложениями не осуществляется в различных целях;
- ограничение данных минимально необходимыми для конкретной цели;

- право лиц на управление своей PII.

8.2.3 Выполняемая поставщиком услуг СПП аутентификация и авторизация пользователей для предоставления доступа к определенной услуге/приложению

Поставщики СПП должны будут осуществлять управление привилегиями пользователей для предоставления доступа (в том числе ролями пользователей и их привилегиями в отношении выполнения определенных действий) к определенным услуге/приложениям, таким как:

– услуги голосовой связи;

– услуги потоковой связи;

– услуги по передаче данных и сообщений;

– служба электросвязи в чрезвычайных ситуациях (ETS) и электросвязь для оказания помощи при бедствиях (TDR).

Каждая услуга может предъявлять свои собственные требования к уровню гарантированности в отношении проверки идентификационных данных и привилегий пользователя, устройства пользователя или комбинации пользователя и устройства пользователя, которые обусловливаются оценкой рисков, связанных с вероятностью получения доступа к ресурсам услуги не имеющими разрешения объектами. Необходимый уровень гарантированности аутентификации и проверки привилегий пользователя, устройства пользователя или комбинации пользователя и устройства пользователя должен устанавливаться и обеспечиваться для конкретной услуги на основании политики обеспечения безопасности СПП. Это будет включать поддержку и использование разных методов аутентификации от базовых методов аутентификации с использованием паролей и персональных идентификационных номеров (PIN) до более строгих методов с использованием аутентификационных ключей, таких как:

a) цифровые сертификаты (например, сертификат PKI X.509);

b) жетоны безопасности (аппаратные и программные жетоны) и интеллектуальные карты;

c) данные поведенческих характеристик (например, анализ нажатия на клавиши клавиатуры);

d) биометрические идентификационные данные (например, распознавание речи, отпечатки пальцев, идентификация по радужной оболочке или сетчатке).

ПРИМЕЧАНИЕ. – Аунтетификация объекта не предназначена для указания положительного результата проверки достоверности лица.

При организации аутентификации и авторизации необходимо принимать во внимание обеспечение простоты ее применения для пользователя. Это особенно важно для определенных типов услуг, таких как ETS и TDR. Желательно, чтобы процесс аутентификации был удобен для пользователя. В Дополнении II приводятся примеры аутентификации и авторизации для ETS.

К аутентификации и авторизации для доступа к конкретной услуге, кроме представленных в пп. 8.2.1 и 8.2.2, применимы следующие требования:

(R-40) – Необходимо, чтобы поддерживались методы аутентификации полномочий на основании политики поставщика СПП. Необходимо, чтобы поддерживались методы многофакторной аутентификации и использовались надлежащим образом, исходя из политики поставщика СПП для гарантированности подлинности и привилегий.

(R-41) – Необходимо обеспечивать возможность уникальной идентификации всех пользователей, связанных с подпиской на определенную услугу, на основании политики поставщика СПП. Это включает идентификацию агрегатных конечных пользователей, идентификационные данные которых могут не представляться поставщику СПП[2].

(R-42) – Исходя из политики поставщика СПП, необходимо обеспечивать возможность связывания числа индивидуальных пользователей, имеющих ту же подписку, с этой подпиской.

(R-43) – Необходимо обеспечивать возможность уникальной адресации каждого пользователя/ абонента, имеющего подписку на прикладную услугу, для целей связи.

---

[2] С суммарной конечной точкой могут быть связаны два и более агрегатных пользователей. Идентификационные данные этих пользователей могут быть известны только суммарной конечной точке и не известны поставщику СПП.

(R-44) – Исходя из политики поставщика СПП, необходимо обеспечивать возможность для конечного пользователя иметь доступ к услуге одновременно несколько раз и/или с нескольких устройств.

(R-45) – Необходимо обеспечивать возможность поддержки нескольких профилей подписки для индивидуального конечного пользователя. Необходимо, чтобы такие множественные профили подписки могли быть идентифицированы уникально.

В соответствии с политикой поставщика СПП может потребоваться периодическая аутентификация пользователя для обеспечения более высокого уровня гарантированности и безопасности.

(R-46) – Исходя из политики поставщика СПП, необходимо обеспечивать возможность периодической повторной аутентификации пользователя (например, конечного пользователя, элемента или объекта сети) в течение установленного сеанса или транзакции связи.

9 Выполняемая пользователем аутентификация и авторизация поставщика СПП

В данном разделе представлены требования, относящиеся к выполняемой пользователем аутентификации и авторизации сети (например, пользователь, аутентифицирующий подлинность сети СПП и поставщика услуг, с которым установлено соединение).

9.1 Описание

Архитектура СПП позволяет конечным пользователям получать услуги от нескольких поставщиков СПП. Кроме того, поставщик транспортных СПП (например, поставщик СПП доступа) может не являться поставщиком услуг СПП. В результате конечным пользователям может оказаться необходимым проведение проверки идентификационных данных поставщиков СПП (например, поставщиков доступа, транспорта и услуг). В частности, может потребоваться, чтобы поддерживались:

– возможности, позволяющие конечному пользователю выполнять идентификацию, аутентификацию и авторизацию поставщика услуг СПП в целях подключения к сети (например, к сети доступа);

– возможности, позволяющие конечному пользователю выполнять идентификацию, аутентификацию и авторизацию поставщика услуг СПП.

9.2 Цели и требования

8.2.1 Выполняемая пользователем аутентификация поставщика СПП для присоединения к сети

Точки доступа в сеть, поддерживающие доступ в сеть для оборудования ТЕ и ТЕ-ВЕ СПП, должны поддерживать возможности, позволяющие пользователю выполнять идентификацию, аутентификацию и авторизацию присоединения к сети.

(R-47) – Точки доступа в сеть (NAP), поддерживающие ТЕ и ТЕ-ВЕ СПП (то есть прямое IP-подключение), должны поддерживать возможности, позволяющие конечному пользователю выполнять однозначную идентификацию поставщика СПП для присоединения и подключения.

(R-48) – Точки доступа в сеть (NAP), поддерживающие ТЕ и ТЕ-ВЕ СПП (то есть прямое IP-подключение), должны поддерживать возможности, позволяющие конечному пользователю выполнять аутентификацию и санкционирование в отношении поставщика СПП для присоединения и подключения, если этого требует политика обеспечения безопасности. Эти функции могут обеспечиваться как часть общей функции NACF, определенной в [ITU-T Y.2012].

(R-49) – В случае многосетевых схем необходимо, чтобы административный домен каждой сети (например, провайдера СПП доступа, провайдера посещаемой СПП и провайдера домашней СПП), осуществляя идентификацию, аутентификацию и санкционирование присоединения к сети (например, используя соглашения SLA), обеспечивал соблюдение принятой политики (например, доверительных взаимоотношений).

9.2.2 Выполняемая пользователем аутентификация поставщика СПП для получения обслуживания

Могут обеспечиваться возможности, позволяющие конечному пользователю выполнять аутентификацию и авторизацию поставщика СПП для получения услуг СПП.

(R-50) – СПП должны поддерживать возможности, позволяющие конечному пользователю выполнять однозначную идентификацию поставщика СПП, предоставляющего услугу или комплекс услуг, если этого требует политика в области обеспечения безопасности.

(R-51) – СПП должны поддерживать возможности, позволяющие конечному пользователю выполнять аутентификацию и санкционирование в отношении поставщика СПП, предоставляющего услугу или комплекс услуг.

10 Поставщик СПП, поддерживающий выполняемую пользователем одноранговую аутентификацию и авторизацию

Данный раздел носит дополняющий и информационный характер.

Установление одноранговой связи является прозрачным для поставщика СПП, поскольку трафик пересекает сеть поставщика СПП только на транспортном уровне. Следует заметить, что в таких сценариях связи поставщик СПП может выполнять роль IdP, обеспечивающего услуги IdM (например, возможности для одноранговой аутентификации).

11 Взаимная сетевая аутентификация и авторизация

11.1 Описание

Взаимная сетевая аутентификация и авторизация необходима для сокращения объема угроз, связанных с несанкционированным доступом. Услуги взаимной сетевой аутентификации и авторизации для доступа в сеть необходимы для верификации идентификационных данных и определения того, должен ли быть предоставлен доступ в транспортную сеть и/или доступ к услугам и возможностям. Доступ в сеть может выполняться либо по интерфейсу NNI, или интерфейсу ANI.

На рисунке 9 представлена эталонная модель взаимной сетевой аутентификации и авторизации, в состав которой входят следующие домены безопасности:

1) Домен сети доступа: сеть доступа, управляемая поставщиком сети доступа (например, узкополосный доступ, xDSL и кабель), может быть или может не быть одновременно поставщиком услуг СПП. Доверительные взаимоотношения между поставщиком сети доступа и поставщиком СПП регулируются соглашениями об уровне обслуживания (SLA).
2) Домен посещаемой СПП: СПП, управляемая поставщиком посещаемой сети. Обеспечивает функции посещаемой сети поставщику другой СПП (например, поставщику домашней сети). Доверительные взаимоотношения регулируются соглашениями SLA. Посещаемая сеть может предоставлять услуги СПП и может иметь собственных абонентов. Кроме того, помещаемая сеть может иметь соглашения с поставщиком прикладных услуг третьей стороны. Также сопряжение посещаемой сети с домашней сетью может выполняться по транзитной сети, а доверительные отношения регулируются SLA.
3) Домен домашней СПП: СПП, управляемая поставщиком домашней СПП. Поставщик домашней СПП предоставляет услуги СПП своим абонентам. Кроме того, домашняя сеть может иметь соглашения с поставщиком прикладных услуг третьей стороны по интерфейсу ANI. Доверительные отношения между поставщиками посещаемой и домашней сетей регулируются соглашениями об уровне обслуживания (SLA). Также сопряжение домашней сети с посещаемой и другой сетью может выполняться по транзитной сети, а доверительные отношения регулируются SLA.
4) Домен транзитной сети: СПП, обеспечивающая только транспорт. Доверительные отношения между транспортной сетью и соседними сетями, включая любого поставщика третьей стороны, регулируются соглашениями об уровне обслуживания (SLA).
5) Домен другой сети: поставщик СПП или сети, не являющейся СПП. Доверительные взаимоотношения регулируются соглашениями об уровне обслуживания (SLA).

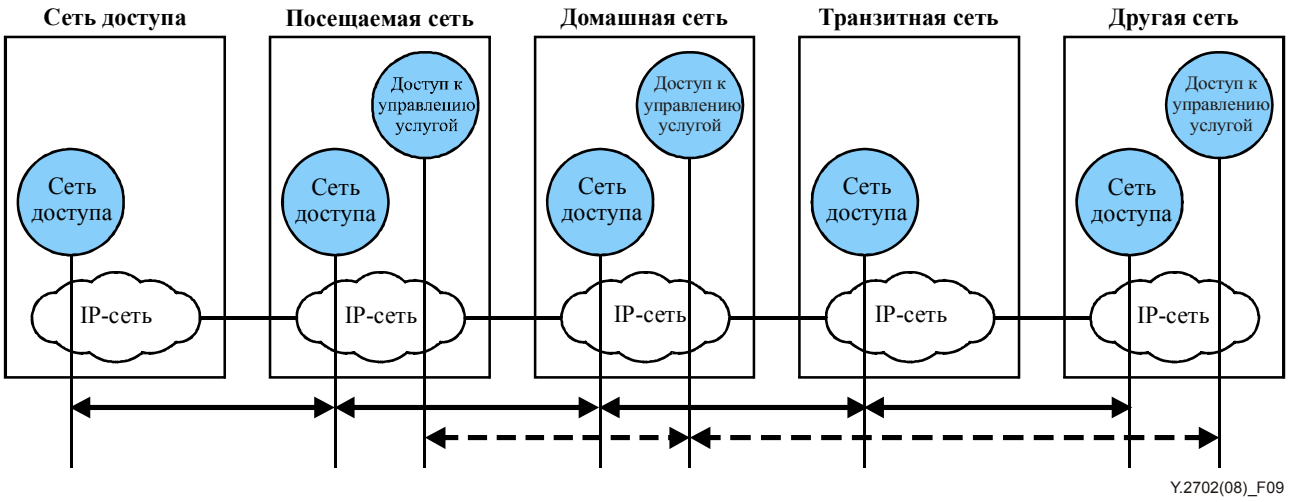


Рисунок 9 – Взаимная сетевая аутентификация

11.1.1 Аутентификация на транспортном уровне

Как показано на рисунке 9, аутентификация на транспортном уровне выполняется по принципу "от участка к участку", в результате чего аутентификация всегда осуществляется с соседней сетью на транспортном уровне. Это означает, что для домашней сети необязательно иметь соглашение SLA с другой сетью, показанной на рисунке, это скорее отношения на транспортном уровне между домашней сетью и транзитной сетью, а затем между транзитной сетью и другой сетью.

11.1.2 Аутентификация на уровне услуги/приложения

Как показано на рисунке 9, аутентификация на уровне услуги/приложения выполняется непосредственно между стратами управления услугами посещаемой, домашней и другой сети на одноранговом уровне услуги/приложения. Такие одноранговые отношения являются логическими, а не физическими. Физический путь проходит вертикально от управления услугой до доступа в сеть в одной сети, затем продолжается напрямую или через транзитную сеть, затем проходит вертикально от сети до доступа к управлению услугой в одноранговой сети услуги/приложения.

11.2 Требования к взаимной сетевой аутентификации

(R-52) – Необходимо, чтобы СПП поддерживали возможности однозначной идентификации соседних сетей на транспортном уровне.

(R-53) – Необходимо, чтобы СПП поддерживали возможности аутентификации и авторизации доступа из соседних сетей на транспортном уровне.

(R-54) – Необходимо, чтобы СПП поддерживали возможности однозначной идентификации соседних сетей на уровне услуги/приложения.

(R-55) – Необходимо, чтобы СПП поддерживали возможности аутентификации и авторизации доступа из соседних сетей на уровне услуги/приложения.

(R-56) – Необходимо, чтобы каждый поставщик СПП, осуществляя взаимную сетевую идентификацию, аутентификацию и авторизацию (например, используя соглашения SLA и доверительные отношения), обеспечивал соблюдение принятой политики.

(R-57) – В случае межсетевой связи необходимо обеспечивать возможность уникальной идентификации участвующих сетевых элементов путем сопоставления идентификаторов сетевых элементов с идентификаторами, связанными с поставщиком СПП, с которой установлено взаимное соединение.

(R-58) – Необходимо, чтобы СПП обеспечивали возможности защиты информации взаимной сетевой аутентификации и авторизации от несанкционированного доступа, манипулирования и повреждения.

(R-59) – Необходимо, чтобы СПП поддерживали возможности защиты от атак (например, атак типа повторная передача перехваченного сообщения и отказ в обслуживании), предпринимаемых в отношении функций и возможностей взаимной сетевой аутентификации и авторизации.

(R-60) – Необходимо, чтобы СПП обладали способностью обнаружения и регистрации предпринимаемых из других сетей попыток несанкционированного доступа (например, может быть установлен конфигурируемый порог системы для некоторого числа попыток несанкционированного доступа, при превышении которого генерируется регистрируемый и сообщаемый системе управления сигнал тревоги).

В соответствии с политикой поставщика СПП может потребоваться периодическая аутентификация пользователя для обеспечения более высокого уровня гарантированности и безопасности.

(R-61) – Исходя из политики поставщика СПП, необходимо обеспечивать возможность периодической повторной аутентификации поставщика СПП, с которым установлено взаимное соединение в течение установленного сеанса или транзакции связи.

12 Выполняемая поставщиком СПП аутентификация и авторизация поставщика услуг/приложений третьей стороны

12.1 Описание

Возможны сценарии, при которыхпоставщик приложения или услуги не является одновременно поставщиком СПП (то есть поставщик услуги/приложения третьей стороны). При таких сценариях поставщику СПП потребуется выполнение аутентификации и авторизации поставщика услуги/приложения третьей стороны, как это показано на рисунке 10.

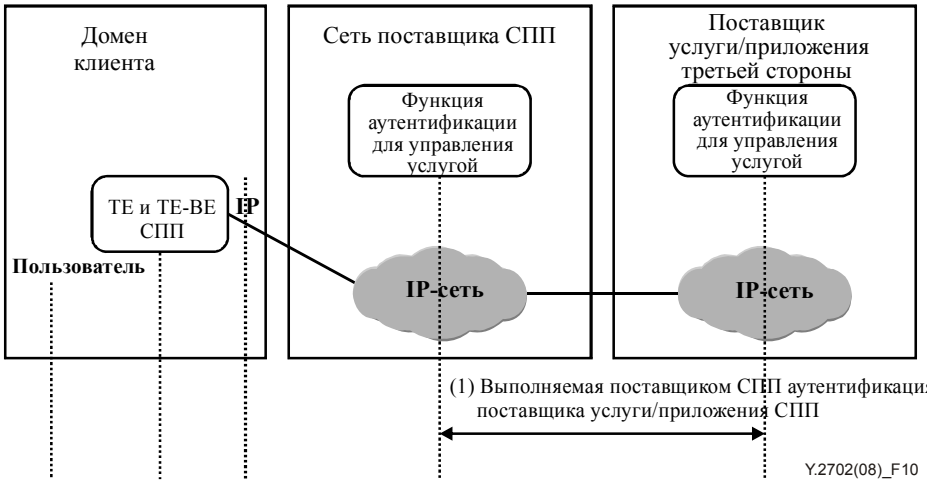


Рисунок 10 – Аутентификация и авторизация для поставщика услуги/ приложения третьей стороны

Следует заметить, что аутентификация пользователя и сети, описанные в предыдущих разделах, выполняются и не показаны на рисунке 10 и в нижеследующем тексте.

12.2 Требования

(R-62) – Необходимо, чтобы поставщик услуг/приложений третьей стороны поддерживал возможности собственной идентификации для поставщика услуг СПП.

(R-63) – Необходимо, чтобы поставщик услуг/приложений третьей стороны поддерживал возможности собственной идентификации для пользователя.

(R-64) – Необходимо, чтобы поставщик СПП поддерживал возможности однозначной идентификации поставщиков услуги/приложения третьей стороны.

(R-65) – Необходимо, чтобы поставщик СПП поддерживал возможности выполнения аутентификации и авторизации поставщиков услуги/приложения третьей стороны.

(R-66) – Необходимо, чтобы поставщики услуги/приложения третьей стороны и СПП, осуществляя идентификацию, аутентификацию и авторизацию (например, используя соглашения SLA и доверительные отношения), обеспечивали соблюдение принятой политики.

(R-67) – Необходимо, чтобы поставщики СПП и услуг/приложений третьей стороны поддерживали возможности защиты против несанкционированного доступа, манипуляции с информацией и повреждения информации аутентификации и авторизации.

(R-68) – Необходимо, чтобы поставщики СПП и услуг/приложений третьей стороны поддерживали возможности защиты от атак (например, атак типа повторная передача перехваченного сообщения и отказ в обслуживании), предпринимаемых в отношении функций и возможностей аутентификации и авторизации.

(R-69) – Необходимо, чтобы поставщики СПП и услуг/приложений третьей стороны обладали возможностью обнаружения и регистрации предпринимаемых со стороны поставщиков услуг/приложений третьей стороны, попыток несанкционированного доступа (например, может быть установлен конфигурируемый порог системы для некоторого числа попыток несанкционированного доступа, при превышении которого генерируется регистрируемый и сообщаемый системе управления сигнал тревоги).

В соответствии с политикой поставщика СПП может потребоваться периодическая аутентификация поставщика услуг/приложений третьей стороны для обеспечения более высокого уровня гарантированности и безопасности.

(R-70) – Исходя из политики поставщика СПП, необходимо обеспечивать возможность периодической повторной аутентификации поставщика услуг/приложений третьей стороны в течение установленного сеанса или транзакции связи.

13 Использование услуги аутентификации и авторизации третьей стороны

13.1 Описание

Поставщики услуг аутентификации и авторизации третьей стороны могут обеспечивать:

– аутентификацию пользователя для поставщика услуг;

– аутентификацию поставщика услуг для пользователя;

– аутентификацию между поставщиками услуг; и

– аутентификацию поставщика услуг/приложений как пользователем, так и поставщиками услуг.

При выполнении этих задач при использовании поставщика услуг аутентификации третьей стороны будут принимать участие не менее трех объектов. Кроме выполнения своих функций по обеспечению аутентификации по запросу, поставщик услуг аутентификации третьей стороны должен аутентифицировать себя как для запрашивающей, так и запрашиваемой сторон.

13.2 Требования

Применимы требования, перечисленные в п. 12.2.

14 Аутентификация и авторизация объектов

14.1 Описание

Кроме аутентификации и авторизации пользователей, устройств пользователей и поставщиков услуг необходимо выполнять аутентификацию объектов в целом. Это включает физические объекты, такие как сетевые элементы и системы, а также виртуальные объекты, такие как:

– приложения;

– прикладные процессы;

– пакеты программного обеспечения;

– сигнализация, управление, а также контент сообщений и данных, передаваемых по каналу связи.

14.2 Требования

(R-71) – Необходимо, чтобы СПП обладали способностью однозначной идентификации объектов на основании политики поставщика СПП.

(R-72) – Необходимо, чтобы СПП поддерживали возможности аутентификации и авторизации объектов на основании политики поставщика СПП.

(R-73) – Необходимо, чтобы СПП поддерживали возможности выполнения верификации и авторизации привилегий объекта (например, разрешение объекту выполнять некое действие при участии в процессе только в случае авторизации его роли и привилегий).

(R-74) – Необходимо, чтобы поставщик СПП, осуществляя идентификацию, аутентификацию и авторизацию объектов, обеспечивал соблюдение принятой политики.

(R-75) – Необходимо, чтобы СПП поддерживали возможности обеспечения конфиденциальности и целостности защиты сообщений и информации, участвующих в обмене в целях аутентификации и авторизации объектов.

(R-76) – Необходимо, чтобы СПП поддерживали возможности защиты против несанкционированного доступа, манипуляции с информацией и повреждения информации аутентификации и авторизации объектов.

(R-77) – Необходимо, чтобы СПП поддерживали возможности защиты от атак (например, атак типа повторная передача перехваченного сообщения и отказ в обслуживании), предпринимаемых в отношении функций и возможностей аутентификации и авторизации объектов.

(R-78) – Необходимо, чтобы СПП обладали возможностью обнаружения и регистрации предпринимаемых объектами попыток несанкционированного доступа СПП (например, может быть установлен конфигурируемый порог системы для некоторого числа попыток несанкционированного доступа, при превышении которого генерируется регистрируемый и сообщаемый системе управления сигнал тревоги).

(R-79) – Необходимо, чтобы СПП обладали возможностью обнаружения и регистрации попыток использования неавторизованных привилегий (например, неразрешенные действия пользователя).

В соответствии с политикой поставщика СПП может потребоваться периодическая аутентификация соседнего поставщика СПП для обеспечения более высокого уровня гарантированности и безопасности.

(R-80) – Исходя из политики поставщика СПП, необходимо обеспечивать возможность периодической повторной аутентификации связанного объекта в течение установленного сеанса или транзакции связи.

Дополнение I

Случай использования SAML

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

I.1 Применение [ITU-T X.1141] "Язык разметки утверждений безопасности" (SAML 2.0)

В настоящем Дополнении представлены практические примеры передачи результатов аутентификации при обеспечении поддержки конфиденциальности с использованием SAML в отношении аутентификации для доступа к услуге/приложению.

I.2 Процедуры аутентификации для доступа к услуге/приложению

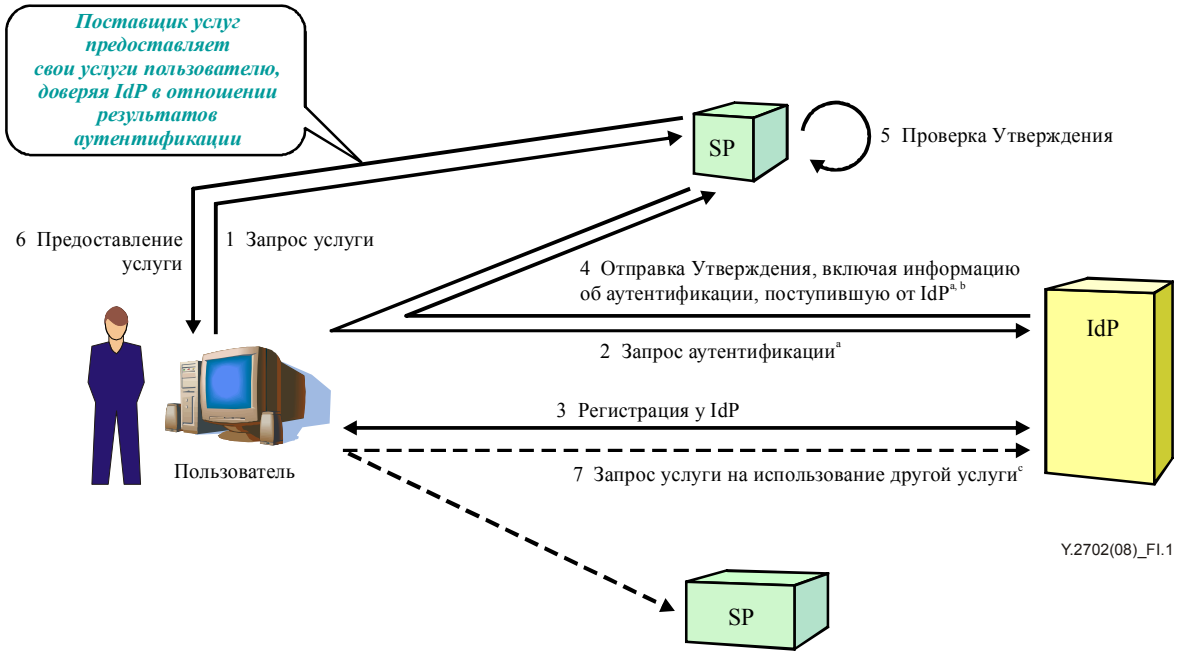
При возникновении необходимости обмена результатами аутентификации между доверенными услугами и/или приложениями, которые могут представляться поставщиками третьей стороны, возможно использование языка разметки утверждений безопасности (SAML 2.0). Язык SAML 2.0 – это открытая спецификация, стандартизованная Организацией по развитию стандартов структурированной информации (OASIS). В частности, SAML может использоваться в следующих случаях:

– однократная регистрация: разные услуги и приложения разрешают своим пользователям – для их удобства – регистрироваться однократно, не осуществляя между собой обмена всей информацией о пользователях;

– объединение счетов: разные услуги и приложения устанавливают связь между своими счетами, относящимися к одному пользователю.

I.3 Аутентификация для доступа к услуге/приложению – Примеры потоков вызовов

На рисунке I.1 представлен характерный пример однократной регистрации с объединением на основе SAML 2.0.



[a] 2 и 4 – осуществляют связь (например, перенаправление HTTP) через агента пользователя (например, веб-браузер).

[b] При необходимости Утверждение может содержать информацию об атрибутах и решение по результатам авторизации.

[c] Тот же поток, что и 1–6, за исключением регистрации у IdP.
(Другими словами, пользователю необходимо однократно зарегистрироваться у IdP для прохождения аутентификации.)

Рисунок I.1 – Пример потоков вызовов SSO с использованием SAML 2.0

В [b-ITU-T X.1141] приведенные на рисунке I.1 термины определены следующим образом:

– Поставщик удостоверений (IdP)

  Тип поставщика услуг, который осуществляет создание, сопровождение информации идентификации и управление этой информацией для администраторов доступа, и обеспечивает аутентификацию администратора доступа для других поставщиков услуг в рамках объединения, например профилей веб-браузеров.

– Поставщик услуг

  Роль, выполняемая системным объектом, когда системный объект предоставляет услуги администраторам доступа или другим системным объектам.

– Утверждение

  Блок данных, созданный органом SAML и относящийся либо к акту аутентификации, выполненной относительно субъекта, или к информации об атрибутах субъекта, либо к данным авторизации, применяемым к субъекту в отношении определенного ресурса.

I.4 Безопасность процедур и механизма аутентификации для доступа к услуге/приложению

Язык SAML 2.0 оснащен средствами, такими как объединение и псевдонимы, предназначенными для защиты безопасности, а также конфиденциальности. Анонимное объединение обеспечивает для поставщика услуги транзитный идентификатор имени nameID. Псевдонимы обеспечивают идентификацию пользователей у поставщика услуг в ходе однократной регистрации, используя парные псевдонимы, которые сохраняют конфиденциальность и позволяют в то же время поддерживать устойчивые отношения с пользователем. Язык SAML 2.0 также позволяет шифровать операторы атрибутов, идентификаторы имени или целые утверждения. Эта функция обеспечивает при необходимости возможность поддержки сквозной конфиденциальности указанных элементов.

Дополнение II

Аутентификация и авторизация для ETS

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

II.1 Обзор

Страны имеют или же разрабатывают свои службы электросвязи в чрезвычайных ситуациях (ETS). Реализация ETS по определению является вопросом национальной компетенции. Однако бедствия/чрезвычайные ситуации могут выходить за пределы географических границ, и поэтому существует вероятность, что страны/администрации будут заключать двусторонние и/или многосторонние соглашения с целью организации связи своих соответствующих систем ETS. В [b-ITU-T E.107] содержатся руководящие принципы, позволяющие обеспечивать связь между одной ETS, реализованной на национальном уровне (ENI), и другой(ими) ENI.

Необходимо, чтобы поставщики СПП разрешали доступ только авторизованным пользователям ETS. Несанкционированный доступ, например нарушитель, выдающий себя за зарегистрированного пользователя, должен предотвращаться. Следовательно, для обеспечения безопасности ETS существенное значение имеют механизмы и возможности аутентификации и авторизации доступа пользователя, устройства пользователя и комбинации пользователя и устройства пользователя ETS в соответствии с принятыми политикой[3] и уровнем гарантированности в отношении конкретных услуг (например, передача речи, данных, видео).

В случае соединения реализованных на национальном ETS поставщики СПП должны будут полагаться друг на друга в отношении аутентификации и авторизации пользователей на основании соглашений об уровне обслуживания. Существует много подходов к аутентификации и авторизациям для ETS. В настоящем Дополнении описаны примеры подходов к аутентификации и авторизации для ETS, а также примеры потоков вызовов.

II.2 Аутентификация и авторизация пользователя ETS

Метод аутентификации и авторизации пользователей ETS является вопросом национальной компетенции. В общем, поставщик СПП осуществляет аутентификацию и авторизацию запроса вызова/сеанса ETS на основании метода зачисления/регистрации и того, как осуществляется вызов услуги. Аутентификация может выполняться для каждого вызова/сеанса, как одноразовая (ограниченная по времени) аутентификация, применимая к текущему сеансу пользователя ETS, или на основании подписки. Поставщики СПП должны быстро проводить аутентификацию зарегистрированных пользователей электросвязи в чрезвычайных ситуациях в самом начале процесса установления вызова/сеанса. Для проведения аутентификации и авторизации на основании применимой политики (например, используя персональный идентификационный номер (PIN) и профили пользователя и подписки) должны использоваться специальные механизмы и методы. После аутентификации и авторизации пользователя, устройства пользователя или комбинации пользователя и устройства пользователя, выполненной на основании применимой политики, вызов/сеанс ETS маркируется и обозначается в прямом направлении к следующим сетям, и факультативно указывается уровень приоритета пользователя ETS. Кроме того, после аутентификации и авторизации все аспекты вызова/сеанса ETS, сигнализация/управление, трафик канала передачи и любые применимые функции управления получают приоритет.

Ниже приведены примеры подходов к выполнению аутентификации и авторизации для ETS.

a) Использование персонального идентификационного номера (PIN): при таком подходе используется аутентификация и авторизация пользователя по номеру PIN. При этом мы идентифицируем пользователя, а не устройство пользователя. Следовательно, этот метод обычно применяется в тех случаях, когда пользователю разрешено вызывать услугу ETS с любого устройства.

b) Использование профиля подписки/обслуживания: при этом подходе для обозначения подписки ETS подготавливается профиль оконечного устройства пользователя. Пользовательский терминал аутентифицируется, и профиль обслуживания пользователя определяется как часть обычной процедуры регистрации поставщика СПП (то есть

[3] ПРИМЕЧАНИЕ. – Политика в данном контексте включает все применимые стратегии, такие как принятые поставщиками СПП, а также регламентарные и государственные правила и нормативы.

поставщика ETS). Если пользователь инициирует запрос, на основании проверки профиля обслуживания пользователя определяется, имеет ли пользователь авторизацию для ETS. Запрос ETS удовлетворяется, если подписка ETS является действительной для пользовательского терминала.

c) Использование сочетания PIN и профиля обслуживания: возможно также сочетание методов с использованием PIN и профиля обслуживания для аутентификации как пользователя, так и устройства пользователя в целях обеспечения более высоких уровней гарантированности.

d) Использование специальных жетонов безопасности и биометрических данных. Кроме описанных выше подходов в целях обеспечения более высоких уровней гарантированности подлинности при выполнении аутентификации и авторизации пользователей ETS могут применяться более сложные подходы на основе использования специальных жетонов безопасности и биометрических данных.

II.3 Аутентификация и авторизация поставщиков СПП для ETS

Аспект аутентификации и авторизации может также приниматься во внимание в отношении передачи и приема трафика ETS между поставщиками СПП с учетом среды со многими поставщиками и разделения управления услугой и транспорта услуги. Существенное значение для обеспечения безопасности ETS имеет также аутентификация и авторизация поставщиков СПП для передачи и приема вызовов/сеансов и трафика ETS на основании соглашений SLA и применимой политики.

II.4 Практические примеры аутентификация и авторизация для ETS

II.4.1 Базовый пример применения аутентификации и авторизации на основании номера PIN

На рисунке II.1 показан базовый пример аутентификации и авторизации ETS с применением персонального идентификационного номера (PIN).

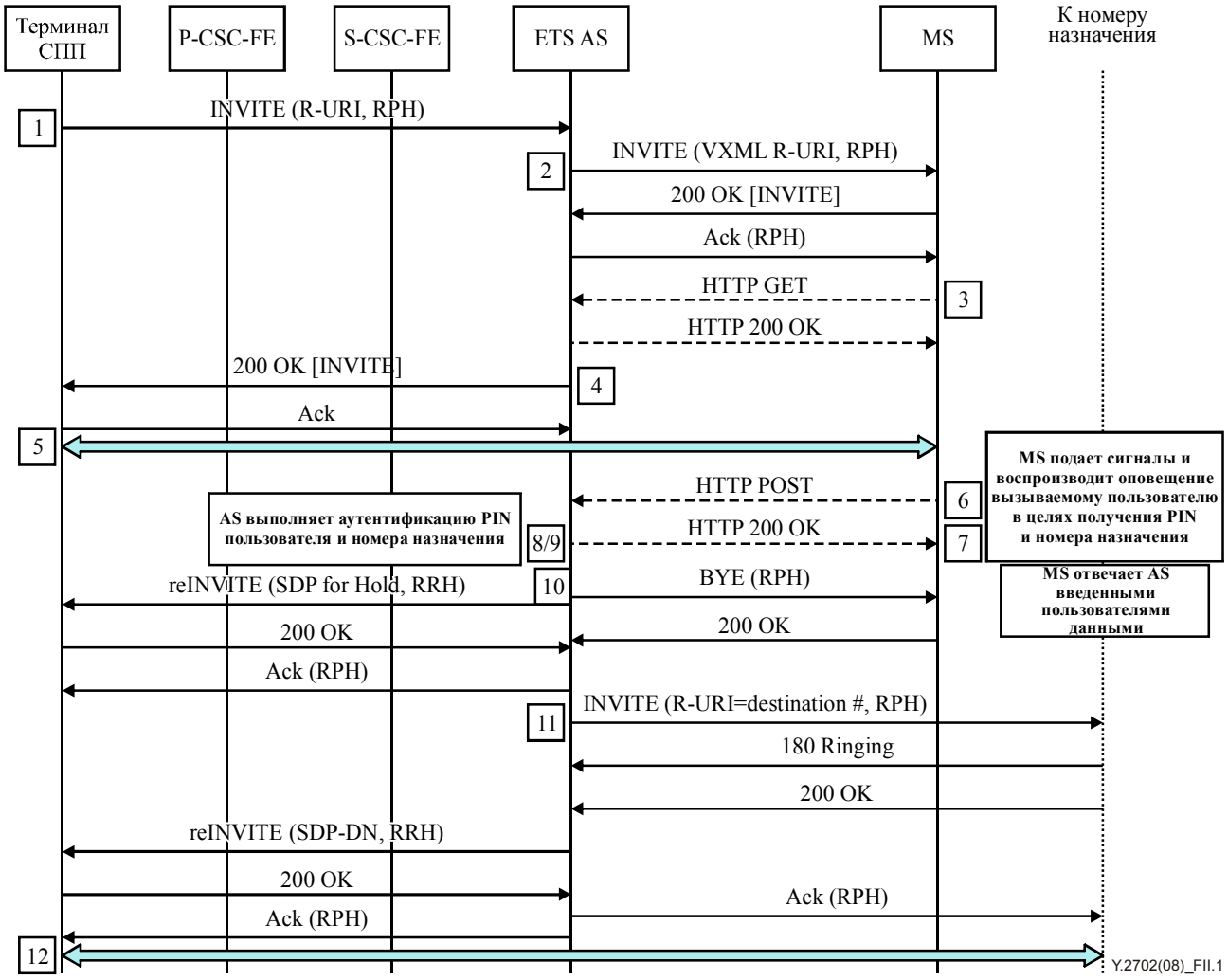


Рисунок II.1 – Аутентификация и авторизация на основании PIN

В данном примере предполагается, что пользователь ETS запрашивает/задействует вызов/сеанс ETS путем запроса вызова/сеанса по номеру ETS. Кроме того, все запросы SIP включают заголовок приоритета использования ресурса (RPH) [b-IETF RFC 4412] для указания того, что требуется приоритетное обслуживание.

1) Вызов/сеанс направляется к серверу приложений ETS (AS), где инициируется обработка аутентификации пользователя.

2) Сервер AS ETS направляет приглашающее сообщение INVITE выбранному медиасерверу (MS) вместе с SDP, связанным с вызывающей стороной. Сообщение INVITE содержит URL сценария VoiceXML, хранящегося на сервере AS ETS. В сценарии описывается порядок взаимодействия MS с вызывающей стороной (какие должны воспроизводиться сообщения, как набирать цифры, сколько цифр набирать, межцифровые таймеры и т. д.).

3) По получении сообщения INVITE сервер MS:

   - может направить сообщение 100 Trying серверу AS ETS;
   - получает сценарий VoiceXML непосредственно от сервера AS ETS, используя HTTP и URL из сообщения INVITE. (MS направляет сообщение HTTP GET серверу AS, а сценарий VoiceXML возвращается от сервера AS ETS AS в сообщении "HTTP 200 OK");
   - проверяет сценарий;
   - составляет и отправляет серверу AS ETS сообщение 200 OK, содержащее его собственный SDP.

4) Сервер AS ETS направляет сообщение 200 OK вызывающей стороне (терминалу СПП), в котором содержится информация о сеансе, полученная им от сервера MS.

5) В этой точке возможно мультимедийное соединение между MS и вызывающей стороной.

6) По получении подтверждения ACK и сценария VXML в сообщении HTTP 200 OK сервер MS выполняет сценарий VoiceXML. Он воспроизводит сигнал и собирает цифры (PIN), введенные вызывающей стороной.

7) Затем MS направляет набранные цифры непосредственно серверу AS ETS, используя для этого сообщение HTTP POST.

8) По получении набранных цифр сервер AS ETS проверяет, действительны ли полученные цифры (PIN).

- Если полученные цифры недействительны (число полученных цифр или неверный номер) сервер AS ETS определяет, что требуется дальнейшее взаимодействие с вызывающей стороной. Сервер AS ETS возвращает серверу MS сообщение HTTP 200 OK, содержащее новый сценарий VoiceXML. Сервер AS ETS передаст инструкцию для окончательного обслуживания обработки.
- Если полученные цифры действительны, сервер AS ETS передаст серверу MS инструкцию на воспроизведение оповещения для набора цифр (номер назначения).

9) Сервер AS ETS определяет, что введенные вызывающей стороной цифры назначения действительны.

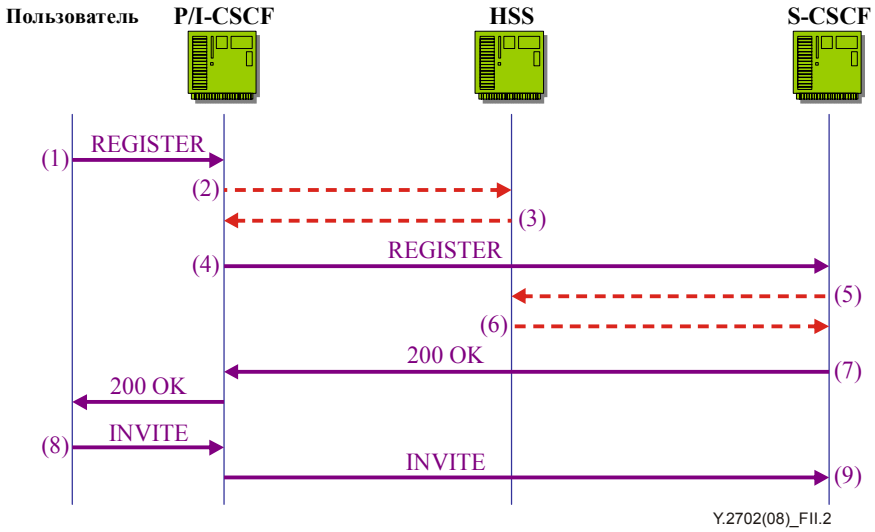
10) Сервер AS ETS освобождает сервер MS от вызова/сеанса с помощью сообщения SIP BYE и направляет вызывающей стороне сообщение reINVITE вместе с SDP для удержания медиаканала.

11) Сервер AS ETS направляет сообщение INVITE стороне назначения. По получении сообщения 200 OK (ответ) AS ETS направляет сообщение reINVITE вместе с SDP, связанным с точкой назначения, вызывающей стороне.

12) Медиатракт устанавливается между вызывающей стороной и номером назначения с аутентификацией AS ETS в тракте управления вызовом.

II.4.2 Пример применения аутентификации и авторизации на основе профиля подписки/обслуживания

На рисунке II.2 представлен пример, в котором для выполняемой ETS аутентификации и авторизации используется профиль подписки/обслуживания.



Примечание. – Для упрощения представления на рисунке не показан весь обмен сообщениями.

Рисунок II.2 – Пример на основе подписки

В основе этого примера лежит использование профиля подписки/обслуживания, связанного с устройством пользователя. Сеть выполняет обычный процесс регистрации и аутентификации устройства пользователя. Когда пользователь задействует вызов/сеанс ETS, выполняется проверка

профиля вызова/сеанса, с тем чтобы определить, прошло ли устройство пользователя авторизацию для вызова/сеанса ETS. При этом существуют следующие потоки вызовов:

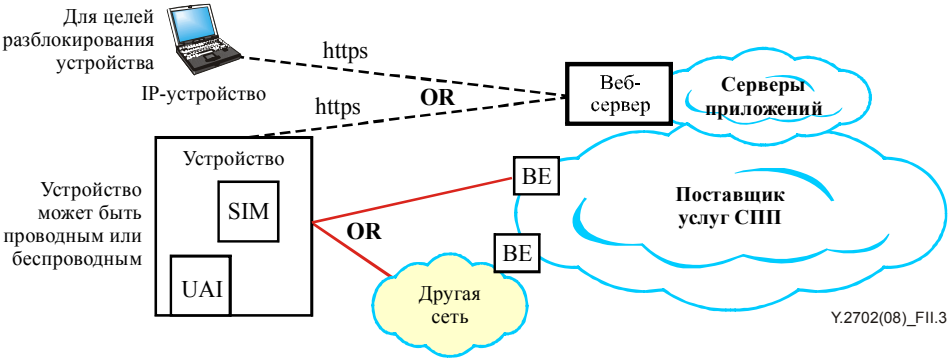
1) инициация регистрации;
2) функция P/I-CSCF запрашивает систему HSS;
3) HSS проверяет подписку пользователя и предоставляет удостоверение функции S-CSCF;
4) функция P/I-CSCF направляет сообщение регистрации функции S-CSCF;
5) функция S-CSCF запрашивает HSS;
6) HSS предоставляет информацию о профиле обслуживания пользователя (может включать взаимодействие с сервером AS);
7) функция S-CSCF направляет сообщение 200 OK;
8) пользователь инициирует сеанс ETS;
9) функция S-CSCF проверяет профиль обслуживания, с тем чтобы определить, является ли разрешенным сеанс ETS.

II.4.3 Пример применения аутентификации и авторизации комбинации пользователя и устройства пользователя

На рисунке II.3 представлен пример, включающий устройство пользователя, имеющее SIM-карту, которое присоединяется к сети с общей аутентификацией начальной загрузки (GBA) стандарта 3GPP.

В данном примере устройство имеет пользовательский интерфейс аутентификации (UAI), с помощью которого пользователь предоставляет аутентификационную информацию через это устройство на прикладной уровень в сети поставщика услуг. Интерфейс UAI может быть либо простейшим, как наборная панель, либо очень сложным, как базирующееся на биометрических данных.

Предполагается, что для сигнализации и медиаданных используется защищенная связь.



SIM – Модуль идентификаци абонента
UAI – Интерфейс аутентификации пользователя

Рисунок II.3 – Аутентификация и авторизация пользователя ETS

Потоки вызовов/сеансов

1) Устройство пользователя включено.
2) Устройство безопасным образом присоединяется к сети, используя архитектуру GBA стандарта 3GPP.
3) Пользователь ETS инициирует местную аутентификацию с SIM-картой в устройстве, используя интерфейс UAI. UAI может быть наборной панелью, с которой вводится PIN, или каким-либо типом устройства обработки биометрических данных.
   a) SIM выполняет аутентификацию пользователя ETS и предоставляет индикатор успеха. SIM информирует сервер приложений ETS о том, что пользователь ETS аутентифицирован.
   b) С другой стороны, информация может быть безопасным образом передана прикладному уровню в сети поставщика услуг.
4) В этот момент "нормальные" пользователь и устройство аутентифицируются для сети. Пользователь в роли пользователя ETS аутентифицирован сервером AS ETS.

Если пользователь не проходит местную аутентификацию после *x* попыток, связь пользователя с устройством должна быть блокирована. Пример разблокирования устройства приведен для пользователя, который осуществляет доступ в GUI через интерфейс AS/WS и который вводит PIN для проверки. Если идентификационные данные пользователя действительны, AS/WS направляет устройству сообщение, содержащее команду разблокирования.

II.4.4 Практический пример применения местоположения предприятия

Вызовы ETS могут инициироваться и завершаться в пунктах местоположения государственных предприятий. Типичное развертывание:

– наличие специализированных средств от местоположения государственного предприятия до поставщика услуг;

– пользователь осуществляет регистрацию с местоположением предприятия, а не с поставщиком услуг;

– местоположение предприятия регистрируется с групповым символом или IWF (например, SBC) на границе сети поставщика услуг и выполняет суррогатную регистрацию от имени предприятия.

Таким образом, если желательна аутентификация сверх аутентификации на основании PIN, потребуется выполнение дополнительных функций. Такие функции включают, в том числе:

– публикацию предприятием информации о присутствии пользователя для поставщика. Этот блок данных будет добавлен в информацию о гарантированности аутентификации;

– передачу жетона безопасности от предприятия поставщику услуг для идентификации в качестве потенциального вызова/сеанса ETS на уровне 2/3 (например, расширение жетона безопасности в RSVP).

Гарантированность аутентификации с данными от нескольких источников требуется в зависимости от типа пользователя.

Дополнение III

Общая архитектура начальной загрузки стандарта 3GPP

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

Общая архитектура начальной загрузки (GBA) определяет процедуру начальной загрузки, не зависимую от доступа. Она обеспечивает основу для взаимной аутентификации конченых пользователей и сетевой прикладной функции (NAF).

GBA – это система аутентификации, состоящая из трех частей:

– конечный пользователь, который пытается получить доступ к услугам сети, используя оборудование пользователя (UE);

– сервер приложений (вызываемая сетевая прикладная функция или NAF);

– доверенный объект (называемый функцией удаленной начальной загрузки сервера или BSF), который участвует в аутентификационном обмене и обмене ключами между двумя другими объектами.

Базовая схема процесса аутентификации на основании GBA показана с помощью эталонной модели и описана ниже.

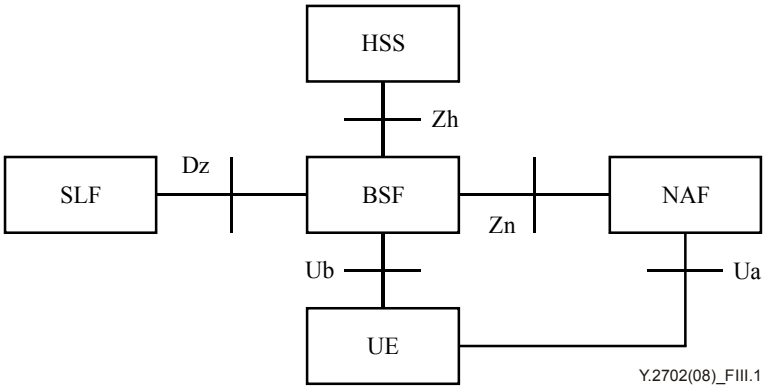


Рисунок III.1 – Простая сетевая модель для начальной загрузки по [b-1 ETSI TS 133 220]

Процедура GBA состоит из следующих основных шагов:

1) Функция NAF запрашивает аутентификацию и согласовывает использование архитектуры GBA через опорную точку Ue.

2) Клиент функции BSF, работающий на UE, инициирует процедуру начальной загрузки через опорную точку Ub. BSF забирает аутентификационную информацию и установки безопасности пользователя GBA из системы HSS через Zh. UE BSF выполняют взаимную аутентификацию, используя протокол HTTP Digest AKA. Результатом процедуры является получение UE идентификатора транзакции начальной загрузки (B-TID) от функции BSF и установление ключа совместного использования (Ks) между оборудованием UE и функцией BSF.

3) Оборудование UE получает Ks_NAF от Ks и направляет функции NAF B-TID (вместе с определяемыми приложением данными).

4) Функция NAF направляет B-TID функции BSF через опорную точку Zn.

5) На основании B-TID функция BSF определяет подлежащий использованию Ks, получает от него Ks_NAF и направляет Ks_NAF функции NAF.

6) Наконец, UE и NAF могут выполнить аутентификацию друг друга, используя ключ совместного использования Ks_NAF. Точная процедура аутентификации зависит от протокола, используемого между UE и NAF. Например, GBA определяет, что приложения на базе HTTP могут использовать либо аутентификацию по протоколу HTTP Digest [b-RFC2617], либо шифронаборы заранее установленных ключей совместного использования TLS [b-RFC4279].

ПРИМЕЧАНИЕ. – Функция BSF обращается с запросом к SLF через опорную точку Dz для получения имени HSS, содержащегося в определяемых абонентами данных. Функция SLF не требуется, если конфигурация BSF обусловливает использование предопределенной HSS.

Отображение объектов GBA в объекты СПП определено в [ITU-T Y.2012].

NAF – соответствует объекту *Applications* (Приложения) на рисунке 3 в [ITU-T Y.2012];

BSF – может включаться в функциональный объект аутентификации и авторизации T-11. Таким образом T-11 может расширяться за счет поддерживаемых возможностей сервера BSF;

HSS – соответствует функциональному элементу профиля пользователя услуги S-5;

SLF – соответствует функциональному элементу указателя подписки S-4;

UE – соответствует функции конечного пользователя.

Дополнение IV

Примеры потоков вызовов управления определением идентичности(IdM)

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

IV.1 Обзор

Примеры потоков в настоящем Дополнении взяты из [b-TR 33.980].

Указанные потоки детально иллюстрируют возможные методы межсетевого взаимодействия между Языком разметки утверждений безопасности версии 2.0, SAML v2.0 (или, в качестве альтернативы, инфраструктуры федеративной безопасности Liberty Alliance, ID-FF), единой платформы идентификации в интернете (ID-WSF), языка разметки утверждений безопасности (SAML) и компонента общей архитектуры аутентификации (GAA), называемого общей архитектурой начальной загрузки (GBA). Настоящее Дополнение носит информационный характер и применимо, только если используются в комбинации ID-WSF и GBA или SAML v2.0 и GBA.

IV.2 Примеры потоков вызовов

Эти потоки существуют, только если используются в комбинации инфраструктура Liberty Alliance и GBA или SAML v2.0 и GBA.

IV.2.1 Сценарий однократной регистрации SSO: ID-FF с передачей запроса аутентификации <lib:AuthnResponse>

IV.2.1.1 Безопасность HTTPS с традиционной TLS

В данном сценарии UE не распознает LAP. Все элементы протокола берутся в пределах инфраструктуры федеративной безопасности [b-ID-FF] и дополняются обусловливаемыми архитектурой GAA данными из [b-TS 33.222]. Вначале описываются шаги, необходимые при использовании HTTPS с традиционной TLS [b-IETF RFC 2246] согласно п. 5.3 [b-2]:

1) UE обращается к SP для получения доступа к предоставляемой этим SP услуге, направляя Запрос HTTP. Этот запрос содержит индикацию поддержки аутентификации на базе GBA (ср. шаг 3), так как это необходимо для перенаправления вызова согласно шагу 3.

2) По получении от UE запроса HTTP SP находит поставщика удостоверений и направляет перенаправленный Запрос HTTP с < lib:AuthnRequest> оборудованию UE. Способы получения адреса поставщика удостоверений зависят от конкретной реализации и являются вопросом компетенции поставщика услуг.

3) В свою очередь UE обращается к IdP, используя содержащийся в поле заголовка местоположения URL, и UE должно осуществить доступ к указателю URL функции NAF/IdP с Запросом HTTP, содержащим информацию <lib:AuthnRequest> information [b-ID-FF bindings].

   UE показывает NAF/IdP, что поддерживается аутентификация на базе GBA путем добавления постоянной строки к заголовку "Пользователь-Агент" HTTP в качестве жетона продукта, согласно описанию в [b-IETF RFC 2616]. Эта постоянная строка устанавливается в соответствии с шагом 2 п. 5.3 технической спецификации [b-TS 33.222].

   Если между UE и IdP существует установленная в процессе начальной загрузки ассоциация безопасности, тогда UE и IdP/NAF совместно используют ключи для защиты опорной точки Ua, и UE располагает всеми необходимыми данными для выполнения аутентификации по протоколу HTTP Digest, которые получены в предыдущих сообщениях. В этом случае шаг 3 комбинируется с запросом шага 5, а шаг 4 пропускается.

4) Поскольку IdP размещается в сборке с функцией NAF, аутентификация на базе протокола HTTP Digest выполняется в соответствии с [b-TS 33.222], и оборудованию UE направляются ответ HTTP, содержащий статус "Не авторизован" и поле заголовка WWW-Authenticate. Метод такой аутентификации и подробная информация о нем содержатся в технической спецификации [TS 33.222], а не в [b-ID-FF].

   Если UE не имеет действительного сеанса начальной загрузки или материал ключа недостаточно обновлен с точки зрения IdP, тогда оборудование UE выполняет новую процедуру начальной загрузки с функцией BSF. Эта операция является прозрачной для SP.

5) UE возвращает данные авторизации IdP, используя в качестве имени пользователя B-TID и в качестве пароля Ks_(ext/int)_NAF. UE может включать дополнительные данные пользователя, относящиеся к протоколу LAP.

Если IdP размещен в сборке с NAF, порядок действий для этого случая определен в технической спецификации [b-TS 33.222]. USS может содержать определяемую Liberty-информацию.

6) Обрабатывается запрос <lib:AuthnRequest>. IdP отвечает вызовом <lib:AuthnResponse> в URL перенаправленного Ответа HTTP [b-ID-FF bindings]. IdP может включать дополнительные данные, относящиеся к протоколу LAP.

7) UE опять обращается к SP, используя этот URL и Запрос HTTP с <lib:AuthnResponse>.

8) SP отвечает, направляя Ответ HTTP.

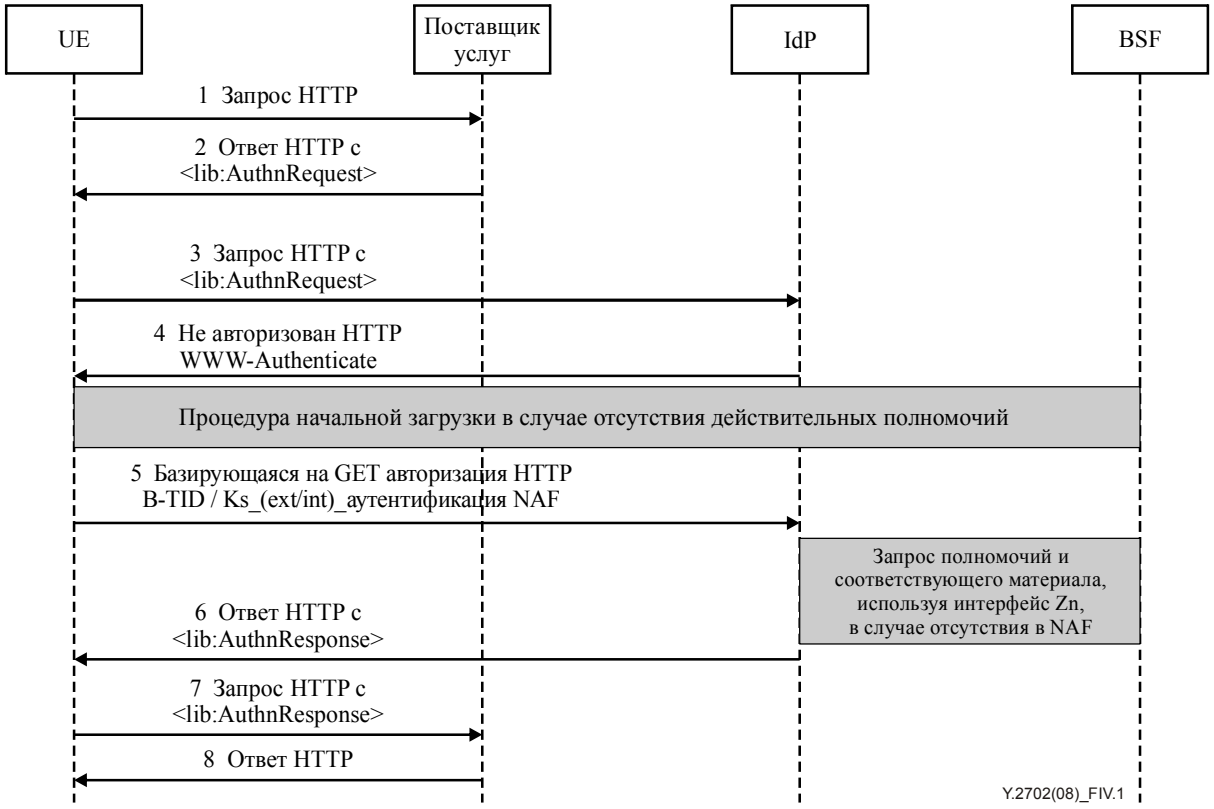


Рисунок IV.1 – Поток сообщений для SSO с <lib:AuthnResponse> и традиционной TLS с GBA

ПРИМЕЧАНИЕ 1. – Поскольку IdP размещается в сборке с NAF, то есть для аутентификации выбирается Ua, как описано в технической спецификации [b-TS 33.222], каждый запрос через Ua аутентифицирует себя сам, поскольку каждый запрос несет полный заголовок аутентификации. Нет разницы между первым запросом и последующими запросами.

ПРИМЕЧАНИЕ 2. – В спецификации функции ID-FF LAP [b-ID-FF] определяется также базирующаяся на POST связь между UE и IdP, помимо базирующегося на GET запроса со строкой запроса. Это соответствует спецификации [b-TS 33.222], так как в ней определяется запрос HTTP без указания какого-либо явного метода.

ПРИМЕЧАНИЕ 3. – Для выбора адреса надлежащего поставщика удостоверений SP может использовать индикацию поддержки аутентификации на базе GBA, полученную на шаге 1.

IV.2.1.2 Безопасность HTTPS с TLS на базе PSK

Если используется безопасность HTTPS с TLS на базе общих ключей (PSK) согласно п. 5.4 технической спецификации [b-TS 33.222], выполняются следующие шаги:

1) UE обращается к SP для получения доступа к предоставляемой этим SP услуге, направляя Запрос HTTP. Этот запрос содержит индикацию поддержки аутентификации на базе GBA (см. шаг 3 п. IV.2.1.1), так как IdP/NAF может вынудить UE использовать традиционную безопасность TLS, даже если UE предлагает использование TLS на базе PSK.

2) По получении от UE запроса HTTP SP находит поставщика удостоверений и направляет перенаправленный Запрос HTTP с < lib:AuthnRequest> в URL оборудованию UE. Способы получения адреса поставщика удостоверений зависят от конкретной реализации и являются вопросом компетенции поставщика услуг.

3) UE начинает устанавливать туннель TLS на базе PSK к IdP/NAF согласно п. 5.4 спецификации [b-TS 33.222]. Это является частью подготовки к отправке перенаправленного запроса к IdP/NAF (ср. шаг 4). Во время установки туннеля TLS оборудование UE показывает возможность использования TLS на базе PSK, и IdP/NAF может выбрать использование TLS на базе PSK с GBA.

   UE по выбранному IdP/NAF шифронабору TLS определяет, будет ли IdP/NAF использовать TLS на базе PSK.

   Если между UE и IdP/NAF существует установленная в процессе начальной загрузки ассоциация безопасности, тогда UE и IdP/NAF совместно используют ключи для защиты опорной точки Ua. Таким образом, UE располагает всеми необходимыми данными для установления туннеля TLS на базе PSK согласно спецификации [b-TS 33.222], и можно сразу переходить к следующему шагу, не выполняя процедуру начальной загрузки.

   Если между UE и IdP/NAF не существует установленной в процессе начальной загрузки ассоциации безопасности, но UE содержит действительный ключ начальной загрузки Ks, тогда UE устанавливает туннель TLS на базе PSK с IdP/NAF на основе соответствующей Ks_(ext)_NAF.

   Если UE не имеет действительного сеанса начальной загрузки или материал ключа недостаточно обновлен с точки зрения IdP/NAF, тогда оборудование UE выполняет новую процедуру начальной загрузки с функцией BSF. Эта операция является прозрачной для SP.

4) В рамках установленного туннеля TLS на базе PSK оборудование UE осуществляет доступ к указателю URL IdP/NAF с Запросом HTTP на базе GET с информацией <lib:AuthnRequest> [b-ID-FF bindings].

5) IdP извлекает <lib:AuthnRequest>, обрабатывает его, использует выполненную в процессе установки туннеля TLS на базе PSK аутентификацию оборудования UE и направляет перенаправленный Ответ HTTP оборудованию UE, который перенаправляет UE обратно к SP. URL может содержать артефакт SAML или <lib:AuthnResponse>.

6) SP извлекает артефакт SAML или <lib:AuthnResponse>, выполняет обработку и отвечает, направляя Ответ HTTP.

7) SP отвечает, направляя Ответ HTTP.

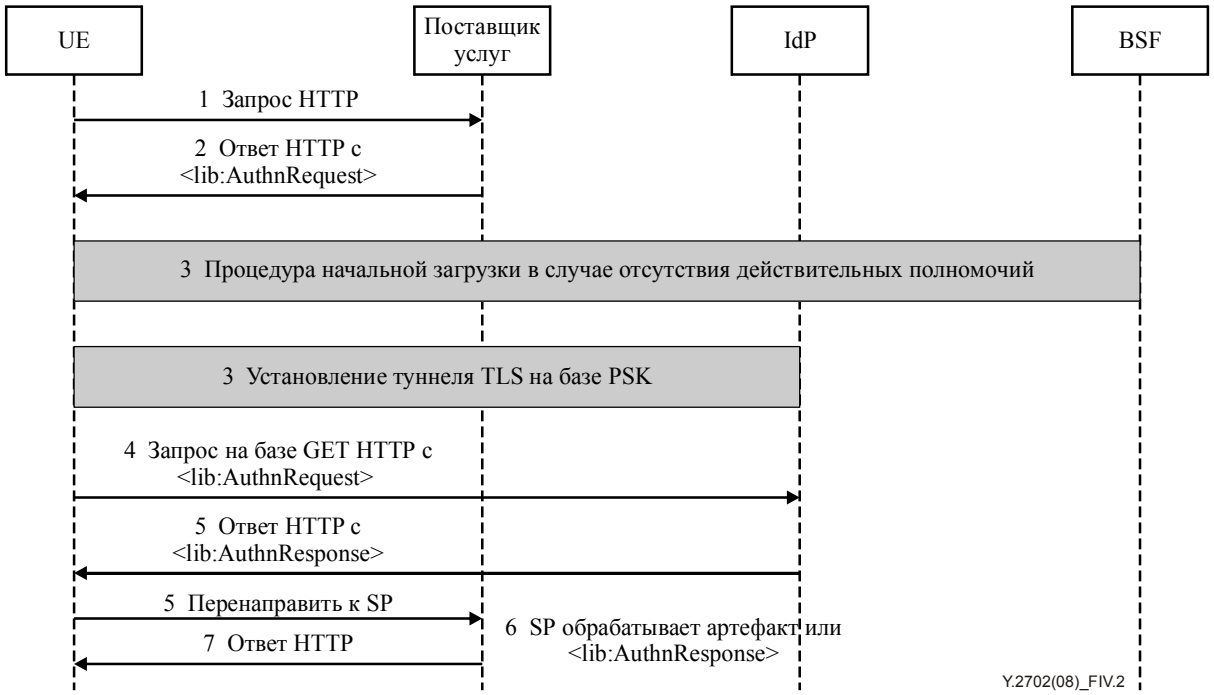


Рисунок IV.2 – Поток сообщений для SSO с <lib:AuthnResponse> и использования TLS на базе PSK с GBA

ПРИМЕЧАНИЕ. – Примечания в п. IV.2.1.1 применимы также к использования TLS на базе PSK, определенного в данном подразделе.

IV.2.2 Сценарий однократной регистрации SSO: ID-FF с передачей артефакта

Данный сценарий аналогичен сценарию, описанному в п. IV.2.1, за исключением того, что поставщик услуг обладает возможностью непосредственно обращаться к IdP.

ПРИМЕЧАНИЕ. – Поскольку базовый поток сообщений аналогичен для случаев использования артефакта и <lib:AuthnResponse>, в данном разделе применимы те же различия между использованием традиционной TLS и TLS на базе PSK, которые указаны в п. IV.2.1. Потоки сообщений, представленные в данном разделе, относятся к традиционной TLS. Также возможно аналогичное использование TLS на базе PSK.

Поставщик IdP должен поддерживать дополнительный интерфейс с SP, с тем чтобы обеспечить SP возможность получения утверждений аутентификации. Этот интерфейс не является полностью отдельным от GBA, так как данная аутентификационная информация может включать связанную с GBA информацию, например идентификационные данные пользователя, псевдоним и дополнительную информацию от GUSS, ограничения, обусловливаемые GBA, и т. д.

1) UE обращается к SP для получения доступа к предоставляемой этим SP услуге, направляя Запрос HTTP. Этот запрос содержит индикацию поддержки аутентификации на базе GBA (см. шаг 3), так как это необходимо для перенаправления вызова согласно шагу 3.

2) По получении от UE запроса HTTP SP находит поставщика удостоверений и направляет перенаправленный Запрос HTTP с < lib:AuthnRequest> оборудованию UE. Способы получения адреса поставщика удостоверений зависят от конкретной реализации и являются вопросом компетенции поставщика услуг.

3) В свою очередь UE обращается к IdP, используя содержащийся в поле заголовка местоположения URL, и UE должно осуществить доступ к указателю URL функции NAF/IdP с Запросом HTTP, содержащим информацию <lib:AuthnRequest> [b-ID-FF bindings].

   UE показывает NAF/IdP, что поддерживается аутентификация на базе GBA путем добавления постоянной строки к заголовку "Пользователь-Агент" HTTP в качестве жетона продукта, согласно описанию в [b-IETF RFC 2616]. Эта постоянная строка устанавливается в соответствии с шагом 2 п. 5.3 технической спецификации [b-TS 33.222].

Если между UE и IdP существует установленная в процессе начальной загрузки ассоциация безопасности, тогда UE и IdP/NAF совместно используют ключи для защиты опорной точки Ua, и UE располагает всеми необходимыми данными для выполнения аутентификации по протоколу HTTP Digest, которые получены в предыдущих сообщениях. В этом случае шаг 3 комбинируется с запросом шага 5, а шаг 4 пропускается.

4) Поскольку UE еще не аутентифицировано поставщиком IdP, аутентификация должна быть выполнена в данный момент, как описано в технической спецификации [b-TS 33.222]. Метод этой аутентификации и подробная информация о нем не определены в [b-ID-FF] Liberty Alliance. IdP направляет оборудованию UE ответ HTTP, содержащий статус "Не авторизован", как описано в спецификации [b-TS 33.222].

   Если в NAF отсутствует действительный материал ключа, обусловливаемый NAF, или материал ключа не удовлетворителен с точки зрения NAF или IdP, тогда должна быть выполнена процедура начальной загрузки согласно спецификации [b-TS33.220]. Эта операция является прозрачной для SP.

5) UE отвечает запросом на базе HTTP GET с полем заголовка аутентификации, содержащим в качестве имени пользователя B-TID и в качестве пароля Ks_(ext/int)_NAF. UE может включать дополнительные данные пользователя, относящиеся к протоколу LAP.

   IdP/NAF может запросить представление полномочий и соответствующего материала, в случае если они еще не были сохранены. Полученная USS может содержать дополнительную Liberty-информацию.

6) IdP отвечает содержащим артефакт SAML указателем URL перенаправленного Ответа HTTP [b-ID-FF bindings]. IdP может включать дополнительные данные, относящиеся к протоколу LAP.

7) UE опять обращается к SP, используя этот URL и Запрос HTTP с артефактом SAML.

8) SP направляет поставщику IdP Запрос HTTP с артефактом SAML. Этот запрос содержит сообщение Запрос SOAP <samlp:Request> к конечной точке SOAP поставщика удостоверений, запрашивающее утверждение путем предоставления артефакта утверждения SAML в элементе < samlp:AssertionArtefact> согласно описанию в [b-ID-FF bindings].

9) Теперь IdP может создать или найти запрошенное утверждение и ответить сообщением Запрос SOAP <samlp:Response>, содержащим запрошенное утверждение <saml:Assertion> или код статуса согласно определению в [b-OASIS]. IdP направляет утверждение аутентификации, соответствующее артефакту.

10) SP обрабатывает сообщение SOAP с <saml:Assertion>, которое было возвращено в ответе <samlp:Response>, проверяет подпись в <saml:Assertion> и обрабатывает сообщение согласно определению в [b-ID-FF bindings], после чего отвечает, направляя Ответ HTTP.

Срок жизни утверждения аутентификации SAML должен быть равным или меньше B-TID.

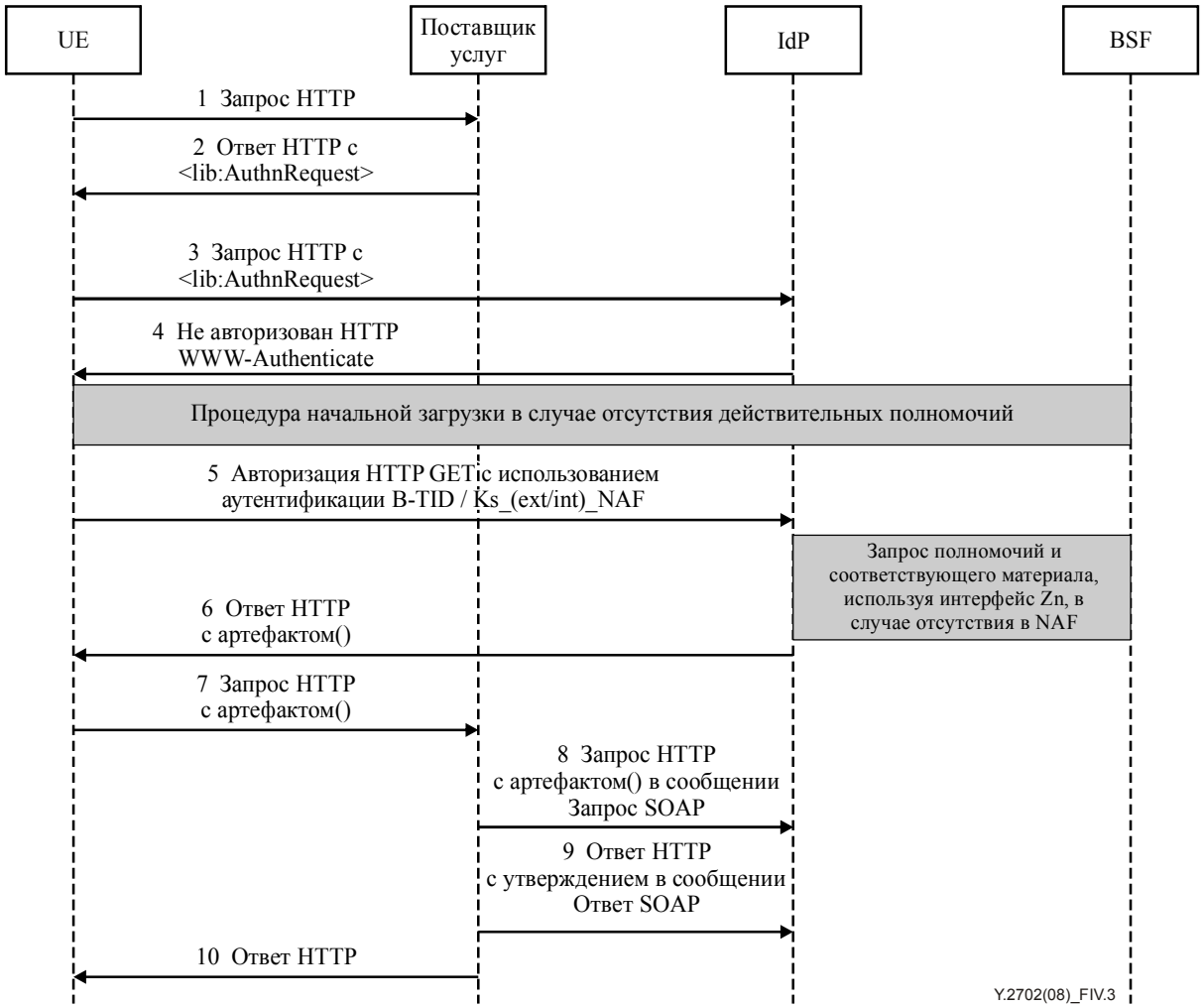


Рисунок IV.3 – Поток сообщений для SSO с передачей артефакта и использованием GBA

IV.2.3 Сценарий однократной регистрации SSO: услуга аутентификации на базе ID-WSF

В этом сценарии оборудование UE поддерживает LAP, то есть является LUAD (поддерживающим Liberty-агентом или устройством пользователя согласно описанию в спецификации профилей Liberty-ID-WSF для поддерживающих Liberty-агентов и устройств пользователя [b-ID-WSF profiles]). Используемые элементы протокола поступают от услуги аутентификации ID–WSF [b-ID-WSF service], и взаимодействие UE с IdP состоит из двух последовательных запусков протокола. Активный LUAD клиент в первый раз обращается к NAF/IdP до осуществления доступа к услуге, предоставляемой данным SP.

1) UE выполняет аутентификацию с услугой аутентификации (AS) поставщика IdP и получает жетон безопасности, который предоставляет UE полномочия вызывать некоторые услуги.

2) UE вызывает услугу однократной регистрации (SSOS) поставщика IdP, используя для этого жетон безопасности. На этом шаге UE получает утверждение аутентификации (информация аутентификации и авторизации), которое должно использоваться для SP.

3) UE представляет поставщику SP утверждение аутентификации, действуя в качестве WSP для доступа к веб-услуге.

В случае если WSP, предоставляющий пользователю веб-услугу, является частью домена оператора IdP, клиент LUAD может также обратиться с этим жетоном безопасности напрямую к WSP. В этом случае можно пропустить обращение к SSOS.

Отображение трех шагов в архитектуре GBA выполняется следующим образом:

– Первый шаг отображается в процессе связи между пользователем (LUAD) и AS, как определено в LAP [b-ID-WSF service]. Протокол аутентификации встроен в протокол SASL. При необходимости оборудованием UE должен выполняться прогон Ub. Это не базируется на протоколах LAP [b-ID-WSF security], [b-ID-FF] или [b-ID-WSF service], а лишь на протоколах GBA [b-TS 33 220].

– Второй и третий шаги абсолютно такие же, как определенные в LAP (без связи с GBA). Единственная зависимость от GBA заключается в содержимом утверждения аутентификации SAML, которое частично определяется результатами на базе GBA (параметры протокола, например время выполнения; и определяемые пользователем параметры, например взятые из USS).

Ниже описан поток сообщений для сценария SSO услуги аутентификации на базе ID-WSF с передачей ответа. Это описание также применимо, если SSOS также предоставляет услугу аутентификации ID-WSF, в каковом случае SSOS размещается в сборке с AS.

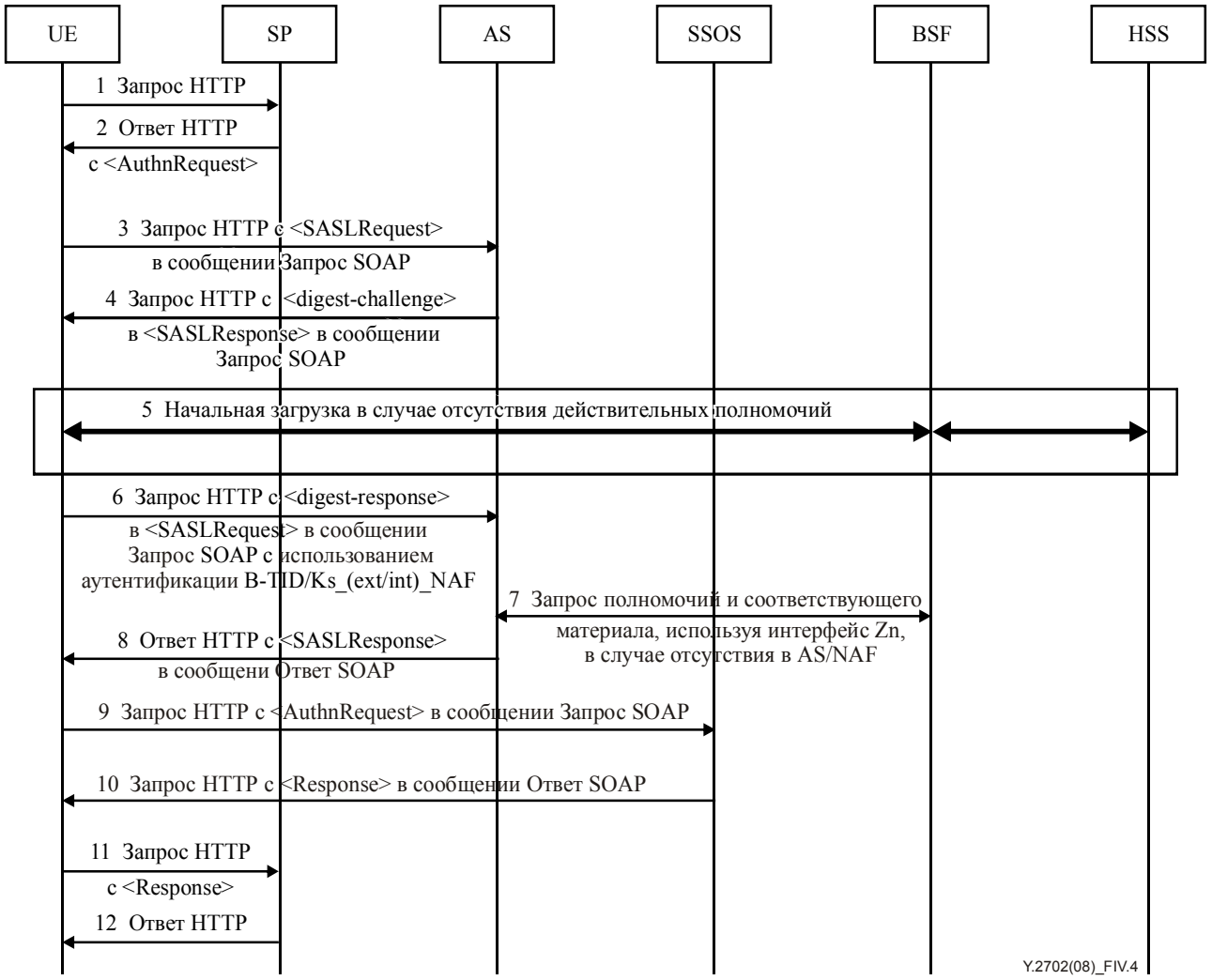


Рисунок IV.4 – Поток сообщений для AS на базе ID-WSF и SSO с передачей ответа и использованием GBA

1) UE обращается к SP для получения доступа к предоставляемой этим SP услуге, направляя Запрос HTTP.

2) По получении от UE запроса HTTP SP находит адрес AS направляет перенаправленный запрос HTTP оборудованию UE. Ответ HTTP может содержать или не содержать заголовок <lib:AuthnRequest> в зависимости от приложения или модели развертывания. Способы получения адреса AS зависят от конкретной реализации.

3) UE (LUAD-WSC) направляет серверу AS запрос HTTP. Этот запрос содержит связанный с SOAP заголовок <SASLRequest>, в который вставлен параметр "механизм" со списком, содержащим одно или несколько имен механизмов SASL поддерживающих клиентов.

UE показывает NAF/IdP, что поддерживается аутентификация на базе GBA путем добавления постоянной строки к заголовку "Пользователь-Агент" HTTP в качестве жетона продукта, согласно описанию в [b-IETF RFC 2616]. Эта постоянная строка устанавливается в соответствии с шагом 2 п. 5.3 технической спецификации [b-TS 33.222].

Если между UE и NAF/AS существует установленная в процессе начальной загрузки ассоциация безопасности, тогда UE и NAF/AS совместно используют ключи для защиты опорной точки Ua, и UE может выполнять последующую процедуру аутентификации, если разрешено профилем SASL. В этом случае шаг 3 комбинируется с запросом шага 6, а шаги 4 и 5 пропускаются.

4) AS направляет оборудованию UE ответ HTTP. Ответ содержит связанный с SOAP заголовок <SASLResponse>, в который вставлен параметр "serverMechanism" с именем выбранного механизма SASL (то есть аутентификация на базе DIGEST) из списка поддерживающих клиентскую технологию механизмов SASL, и в этом случае заголовок <SASLResponse> также содержит параметр <digest-challenge>. Метод и подробные данные, связанные с этим параметром, соответствуют [b-IETF RFC 2831].

5) Если UE не имеет действительного сеанса начальной загрузки или материал ключа неудовлетворителен с точки зрения AS, тогда оборудование UE выполняет новую процедуру начальной загрузки с функцией BSF и получает общий ключ Ks_(ext/int)_NAF. Эта операция является прозрачной для SP.

6) UE повторно направляет серверу AS запрос HTTP. Этот запрос содержит связанный с SOAP заголовок <SASLRequest>, в который вставлен параметр "механизм", содержащий возвращенный на шаге 4 механизм SASL, и в этом случае заголовок <SASLRequest> также содержит параметр <digest-response>, в котором рассчитываются данные авторизации с использованием в качестве имени пользователя B-TID и в качестве пароля Ks_(ext/int)_NAF. Метод и подробные данные, связанные с этим параметром, соответствуют [b-IETF RFC 2831]. UE может включать дополнительные данные пользователя, относящиеся к протоколу LAP.

7) Поскольку AS размещается в сборке с NAF, AS запрашивает Ks_(ext/int)_NAF и другие материалы от BSF, используя интерфейс Zn, если они еще не доступны.

8) AS обрабатывает параметр <digest-response> в заголовке <SASLRequest>. Затем AS отвечает, направляя в ответе HTTP связанный с SOAP заголовок <SASLResponse>. Заголовок <SASLResponse> содержит параметр ID-WSF EPR (EndpointReference), который относится к экземпляру SSOS, и устанавливается URI типа услуги согласно [b-ID-WSF service] для идентификации SSOS на базе ID-WSF. Заголовок <SASLResponse> также содержит некоторые полномочия, необходимые оборудованию UE для вызова SSOS. AS может включать дополнительные связанные с LAP данные.

9) UE направляет SSOS запрос HTTP. Этот запрос содержит связанный с SOAP заголовок <samlp2:AuthnRequest>, в котором установлен атрибут ProtocolBinding согласно [b-ID-WSF service] для идентификации связывания протоколов SAML, которое должно использоваться. Этот запрос содержит также заголовок <wsse:security>, который включает возвращенные на шаге 8 полномочия. Оборудованию UE может потребоваться самому создать заголовок <samlp2:AuthnRequest>, если оно не получило такого заголовка на этапе шага 2 в соответствии с приложением или моделью развертывания.

10) Обрабатывается запрос <samlp2:AuthnRequest>. SSOS отвечает заголовком <samlp2: Response>, содержащимся в URL перенаправленного ответа HTTP [b-ID-FF binding]. Заголовок <samlp2: Response> содержит параметр <saml2:Assertion>. SSOS может включать дополнительные данные, относящиеся к протоколу LAP.

11) UE опять обращается к SP, используя этот URL и Запрос HTTP с <samlp2: Response>.

12) SP отвечает, направляя Ответ HTTP.

ПРИМЕЧАНИЕ. – Если IdP управляется совместно с BSF, тогда первый шаг может быть отображен в опорной точке Ub архитектуры GBA [b-TS 24.109]. Второй шаг может быть отображен в интерфейсе Ua архитектуры GBA.

Несмотря на формальную аналогию выполнения двух последовательных прогонов протоколов, требуемых обеими протокольными областями, более простое отображение, как представляется, невозможно. Синтаксис и семантика информационных элементов, передаваемых между протоколами GBA и LAP, значительно различаются.

IV.2.4 Сценарий однократной регистрации SSO: SAML v2.0 с передачей <samlp:Response>

IV.2.4.1 Безопасность HTTPS с TLS

Данный сценарий является вариантом сценария, описанного в п. IV.2.1.1, при том отличии, что все протокольные элементы берутся в пределах [b-SAML v2.0], реализуя профиль SSO веб-браузера по [b-OASIS]. Следовательно, все описанные шаги применимы для данного сценария после замены <lib:AuthnRequest> на <samlp:AuthnRequest> и <lib:AuthnResponse> на <samlp:Response>. Описание шагов повторно не приводится, включена только обновленная версия рисунка IV.1.

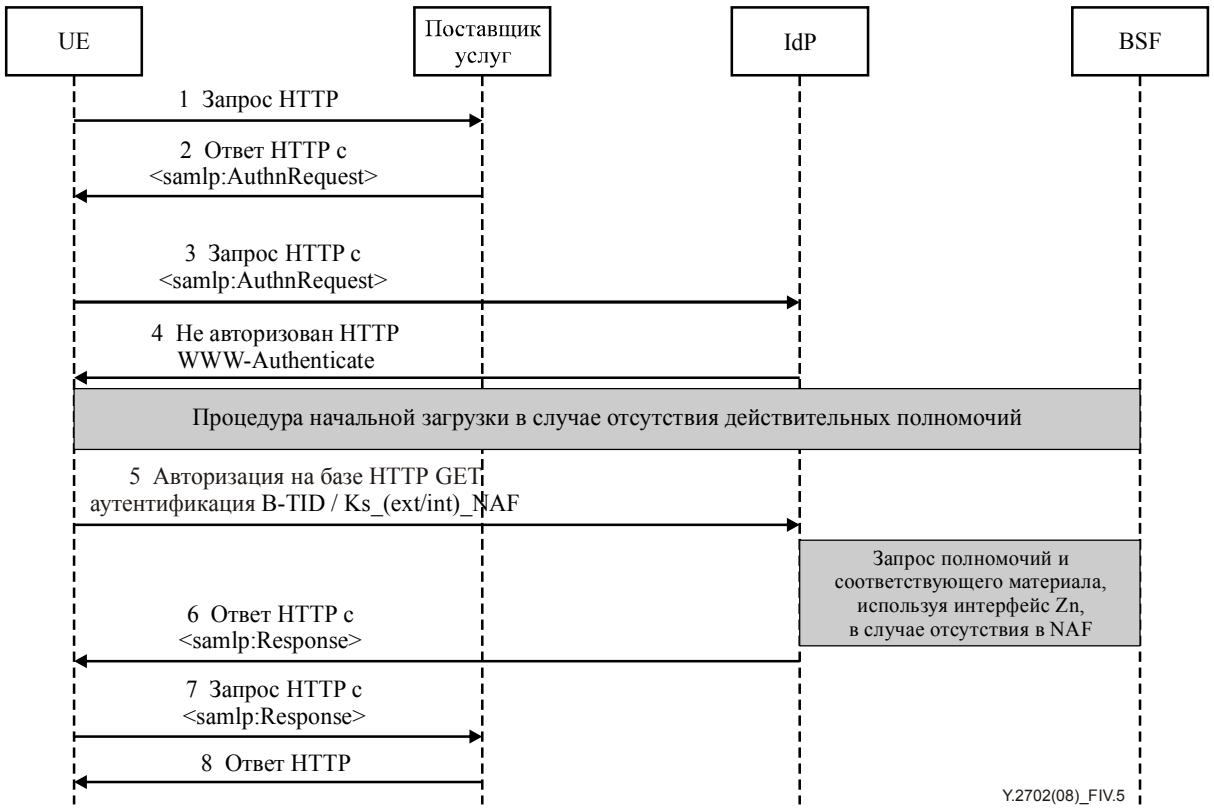


Рисунок IV.5 – Поток сообщений для SSO с <samlp:Response> и TLS с GBA

IV.2.4.2 Безопасность HTTPS с TLS на базе PSK

Данный сценарий является вариантом сценария, описанного в п. IV.2.1.2 при том отличии, что все протокольные элементы берутся в пределах [b-SAML v2.0], реализуя профиль SSO веб-браузера по [b-OASIS]. Следовательно, все описанные шаги применимы для данного сценария после замены <lib:AuthnRequest> на <samlp:AuthnRequest> и <lib:AuthnResponse> на <samlp:Response>. Описание шагов повторно не приводится, включена только обновленная версия рисунка IV.2.

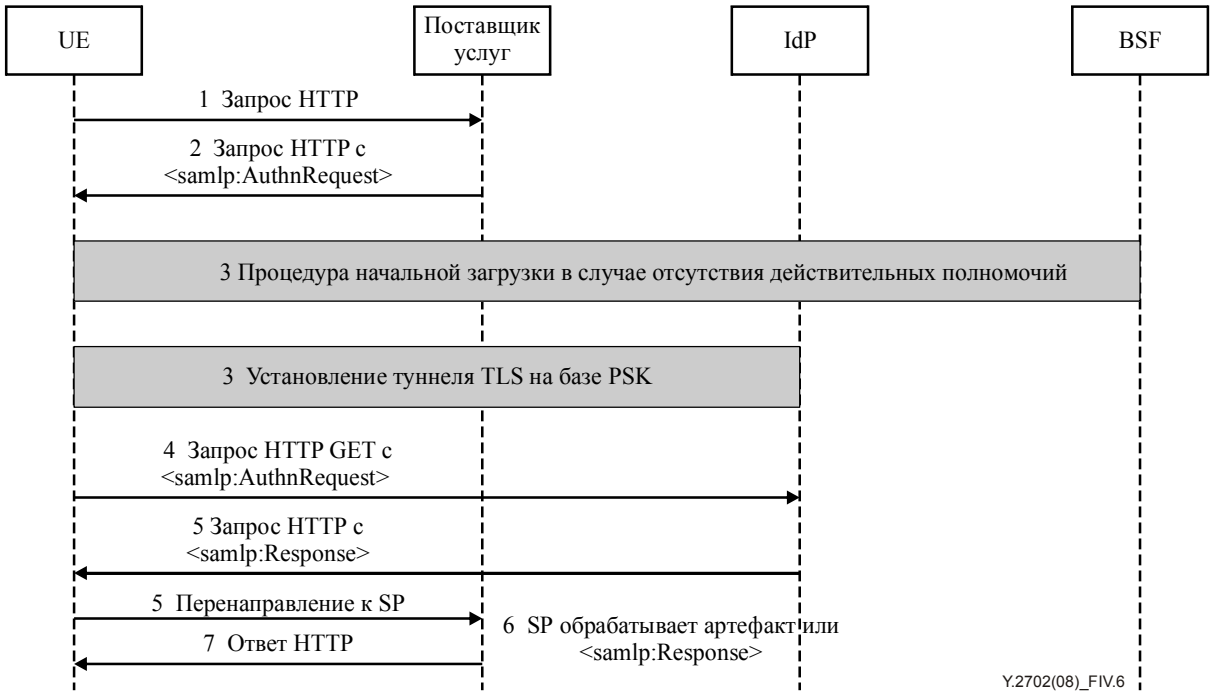


Рисунок IV.6 – Поток сообщений для SSO с <samlp:Response> и использования TLS на базе PSK с GBA

IV.2.5 Сценарий однократной загрузки SSO: SAML v2.0 с передачей артефакта (решение)

Данный сценарий является вариантом сценария, описанного в п. IV.2.2 при том отличии, что все протокольные элементы берутся в пределах [b-SAML v2.0], реализуя профиль SSO веб-браузера по [b-OASIS]. Следовательно, все описанные шаги применимы для данного сценария после замены <lib:AuthnRequest> на <samlp:AuthnRequest>. Описание шагов повторно не приводится, включена только обновленная версия рисунка IV.3.

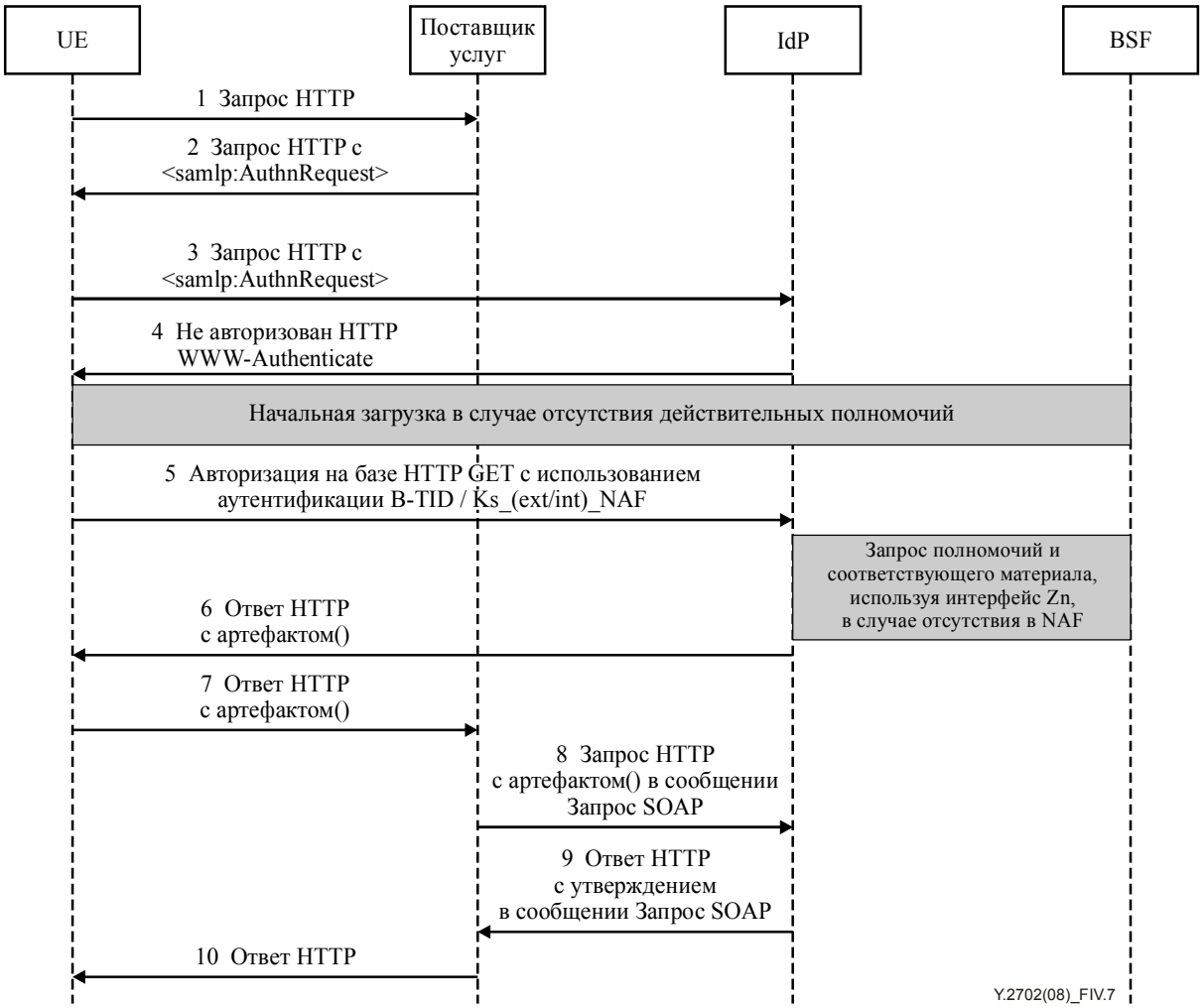


Рисунок IV.7 – Поток сообщений для SSO с разрешением артефакта (SAML v2.0) и использованием GBA

Библиография

[b-ITU-T E.107] Рекомендация МСЭ-Т E.107 (2007 г.), *Служба электросвязи в чрезвычайных ситуациях (ETS) и основа для взаимодействия реализованных на национальном уровне ETS*.

[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.1141] Рекомендация МСЭ-Т X.1141 (2006 г.), *Язык разметки, предусматривающий защиту данных (SAML 2.0)*.

[b-Alliance] Liberty Alliance Project, ID-SIS: *Liberty Alliance ID-SIS 1.0 Specifications*. <http://www.projectliberty.org/liberty/specifications__1>

[b-ID-FF] Liberty Alliance Project, ID-FF v1.2: *Liberty ID-FF Architecture Overview*. <http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications>

[b-ID-FF bindings] Liberty Alliance Project, *ID-FF v1.2: Liberty ID-FF Bindings and Profiles Specification*. <http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications>

[b-ID-FF protocols] Liberty Alliance Project, ID-FF v1.2: *Liberty ID-FF Protocols and Schema Specification*. <http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications>

[b-ID-WSF binding] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF SOAP Binding Specification*. <http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID WSF discovery] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF Discovery Service Specification*. <http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID-WSF profiles] Liberty Alliance Project, ID-WSF: *Profiles for Liberty enabled User Agents and Devices*. <http://projectliberty.org/liberty/content/download/3447/22967/file/liberty-idwsf-client-profiles-v2.0-original.pdf>

[b-ID-WSF security] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF Security Mechanisms*. <http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID-WSF service] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF Authentication Service Specification and Single Sign-On Service*. <http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID-WSF v1.2] Liberty Alliance Project, ID-WSF v1.2: *Security Mechanisms*. <http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_1_1_specifications>

[b-LAP] Liberty Alliance Project Support Documents: *Authentication Context Specification v2.0*.

<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_specifications_support_documents_and_utility_schema_files>

[b-M-04-04] M-04-04: *E-Authentication Guidance for Federal Agencies*. <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

[b-NIST 800-63] NIST Special Publication 800-63 (2006), *Electronic Authentication Guidelines*. <http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>

[b-OASIS] OASIS, *Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0*. <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>

[b-OASIS auth] OASIS, *Authentication Contexts for the OASIS Security Assertion Markup Language (SAML) V2.0*. <http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf>

[b-Reverse] Liberty Alliance Project Support Documents: *Liberty Reverse HTTP Binding for SOAP Specification v1.1*. <http://www.projectliberty.org/resource_center/specifications/liberty_alliance_specifications_support_documents_and_utility_schema_files>

[b-SAML assertions] OASIS, SAML v2 Core, *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

[b-SAML v2.0] OASIS, SAML v2 Core, *Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0*. <http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf>

[b-TR 21.905] 3GPP TR 21.905 (in force), *Vocabulary for 3GPP Specifications*. <http://www.3gpp.org/ftp/Specs/html-info/21905.htm>

[b-TR 33.980] 3GPP TR 33.980 (in force), *Liberty Alliance and 3GPP security interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA) (Release 7)*. <http://www.3gpp.org/ftp/Specs/html-info/33980.htm>

[b-TS 24.109] 3GPP TS 24.109 (in force), *Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details*. <http://www.3gpp.org/ftp/Specs/html-info/24109.htm>

[b-TS 29.109] 3GPP TS 29.109 (in force), *Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3*. <http://www.3gpp.org/ftp/Specs/html-info/29109.htm>

[b-TS 33.220] 3GPP TS 33.220 (in force), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture*. <http://www.3gpp.org/ftp/Specs/html-info/33220.htm>

[b-TS 33.221] 3GPP TS 33.221 (in force), *Generic Authentication Architecture (GAA); Support for subscriber certificates*. <http://www.3gpp.org/ftp/Specs/html-info/33221.htm>

[b-TS 33.222] 3GPP TS 33.222 (in force), *Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)*. <http://www.3gpp.org/ftp/Specs/html-info/33222.htm>

[b-IETF RFC 2222] IETF RFC 2222 (1997), *Simple Authentication and Security Layer (SASL)*. <http://www.ietf.org/rfc/rfc2222.txt?number=2222>

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*. <http://www.ietf.org/rfc/rfc2246.txt?number=2246>

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol-HTTP/1.1*. <http://www.ietf.org/rfc/rfc2616.txt?number=2616>

[b-IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*. <http://www.ietf.org/rfc/rfc2617.txt?number=2617>

[b-IETF RFC 2831] IETF RFC 2831 (2000), *Using Digest Authentication as a SASL Mechanism*. <http://www.ietf.org/rfc/rfc2831.txt?number=2831>

[b-IETF RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*. <http://www.ietf.org/rfc/rfc3546.txt?number=3546>

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*. <http://www.ietf.org/rfc/rfc4279.txt?number=4279>

[b-IETF RFC 4412] IETF RFC 4412 (2006), *Communication Resource Priority for the Session Initiation Protocol*. <http://www.ietf.org/rfc/rfc4412.txt?number=4412>

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 межсетевого протокола и сети последующих поколений**
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2009 г.