МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т Y.2704

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(01/2010)

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

Сети последующих поколений – Безопасность

Механизмы и процедуры безопасности для сетей последующих поколений

Рекомендация МСЭ-Т Y.2704

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

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

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

Рекомендация МСЭ-Т Y.2704

Механизмы и процедуры безопасности для сетей последующих поколений

Резюме

В Рекомендации МСЭ-Т Y.2701 "*Требования к безопасности для сетей последующих поколений версии 1*" излагаются требования к безопасности для сетей последующих поколений (СПП) и их интерфейсов, например UNI, NNI и ANI. В Рекомендации МСЭ-Т Y.2704 описываются некоторые механизмы безопасности, которые могут быть использованы для выполнения требований, описанных в Рекомендации МСЭ-Т Y.2701, и конкретно указывается набор возможностей для каждого отобранного механизма. В частности, в данной Рекомендации описываются механизмы идентификации, аутентификации и авторизации; затем обсуждаются вопросы безопасности транспортировки для сигнализации и OAMP, а также безопасности среды передачи. Далее описываются механизмы, относящиеся к данным аудита безопасности, и, наконец, дается описание обеспечения доступа. Механизмы безопасности, описанные в данной Рекомендации, основаны на использовании модели доверия, определение которой приводится в Рекомендации МСЭ-Т Y.2701.

Перечень механизмов безопасности, описанных в данной Рекомендации, не является исчерпывающим. Поставщикам услуг сети СПП предлагается поддерживать использование дополнительных инструментов, возможностей и оперативных мер безопасности тогда, когда они необходимы, помимо тех механизмов безопасности, которые конкретно указаны в данной Рекомендации для обеспечения безопасности СПП.

Хронологическая справка

Версия	Рекомендация	Утверждена	Исследовательская комиссия
1.0	МСЭ-Т Y.2704	29.01.2010 г.	13-я

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

© ITU 2010

Все права сохранены. Никакая часть данной публикации не может быть воспроизведена с помощью каких-либо средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

Стр.

Рекомендация МСЭ-Т Y.2704

Механизмы и процедуры безопасности для сетей последующих поколений

1 Сфера применения

В [ITU-T Y.2701] "*Требования к безопасности для сетей последующих поколений версии 1*" излагаются требования к безопасности для сетей последующих поколений (СПП) и их интерфейсов, например UNI, NNI и ANI, включая модель доверия. Механизмы безопасности, выбранные для реализации этих требований, содержат варианты; использование несовпадающих вариантов нежелательно, поскольку это часто приводит к уязвимости с точки зрения безопасности и затрудняет достижение функциональной совместимости.

В связи с этим в данной Рекомендации особое внимание уделяется ряду важных механизмов безопасности, которые могут быть использованы для выполнения требований, описанных в [ITU-T Y.2701], и определяется набор вариантов для использования в каждом выбранном механизме, с тем, чтобы уменьшить проблемы, связанные с функциональной совместимостью и несовпадением. Перечень механизмов безопасности, описанных в данной Рекомендации, не является исчерпывающим. Поставщикам услуг сети СПП предлагается поддерживать использование других инструментов, возможностей и оперативных мер безопасности тогда, когда они необходимы, помимо тех механизмов безопасности, которые конкретно указаны в данной Рекомендации для обеспечения безопасности СПП.

Данная Рекомендация предназначена для использования совместно с [ITU-T Y.2701] в целях обеспечения основы для безопасности СПП. Данную Рекомендацию следует использовать совместно с другими Рекомендациями по вопросам безопасности и другими техническими спецификациями, в зависимости от случая.

ПРИМЕЧАНИЕ. – Описанные в данной Рекомендации механизмы для идентификации и аутентификации являются частью более широкой темы, общеизвестной как "управление определением идентичности"(IdM).

1.1 Допущения

Данная Рекомендация основана на следующих допущениях:

1) Как определено в [ITU-T Y.2012], группирование функциональных элементов в заданный элемент сети будет меняться в зависимости от поставщика.

2) Каждый поставщик услуг СПП несет конкретную ответственность за безопасность в пределах своего домена, например путем реализации применимых услуг и практических мер в области безопасности, для того чтобы: a) обеспечить собственную защиту; b) не поставить под угрозу сквозную безопасность в пределах своей сети; и c) обеспечить высокую степень готовности и целостности связи с использованием СПП.

3) Каждый домен сети устанавливает политику в отношении соглашений об уровне обслуживания (SLA) и обеспечивает ее выполнение, чтобы гарантировать безопасность своего домена и безопасность сетевых соединений. Предполагается, что в соглашениях SLA определяются услуги, механизмы и практические меры в области безопасности, подлежащие реализации в целях защиты присоединенных сетей и соединений (трафик сигнализации/контроля, трафик канала передачи и трафик управления) в интерфейсах UNI, ANI и NNI.

4) В настоящей Рекомендации рассматриваются вопросы безопасности сети, которая имеет многоуровневую архитектуру, включающую в себя безопасность периметра, ограниченного доверенными доменами, физическую безопасность оборудования поставщика услуг и, возможно, использование шифрования.

1.2 Обзор

Данная Рекомендация имеет следующую структуру:

- Пункт 2 (Справочные документы) – В данном пункте приводятся нормативные спрвочные документы.
- Пункт 3 (Определения) – В данном пункте приводятся определения, используемые в настоящей Рекомендации.
- Пункт 4 (Аббревиатуры и акронимы) – В данном пункте приводится перечень аббревиатур и акронимов, используемых в настоящей Рекомендации.
- Пункт 5 (Условные обозначения) – Данный пункт намеренно оставлен пустым.

- Пункт 6 (Риски и угрозы безопасности) – В данном пункте приводятся справочные документы по вопросам рисков и угроз безопасности, применимые к СПП.
- Пункт 7 (Модель доверия в области безопасности) – В данном пункте представлен краткий обзор модели доверия, определенной в [ITU-T Y.2701].
- Пункт 8 (Идентификация, аутентификация и авторизация) – В данном пункте описываются механизмы и меры безопасности, предназначенные для идентификации, аутентификации и авторизации.
- Пункт 9 (Безопасность транспортировки для сигнализации и OAMP) – В данном пункте описываются механизмы шифрования и защиты целостности данных сигнализации и OAMP.
- Пункт 10 (Безопасность среды передачи) – В данном пункте описываются механизмы защиты среды передачи (т. е. трафика канала передачи).
- Пункт 11 (OAMP) – В данном пункте приводится информация и справочные документы, касающиеся следа аудита, перехвата событий безопасности и их регистрация.
- Пункт 12 (Обеспечение доступа для оборудования в недоверенной зоне) – В данном пункте приводится информация, касающаяся обеспечения доступа для абонентского оборудования в недоверенной зоне.
- Дополнение I – Примеры гарантирования адреса источника и его применения в механизме идентификации и аутентификации абонента.
- Дополнение II – Безопасность при присоединении службы электросвязи в чрезвычайных ситуациях (ETS).
- Дополнение III – Примеры передового опыта в области обеспечения безопасности.
- Библиография.

2 Справочные документы

В нижеследующих Рекомендациях МСЭ-Т и других справочных документах содержатся положения, которые, посредством ссылок в настоящем тексте, составляют положения настоящей Рекомендации. На время публикации указанные здесь издания были действительными. Все Рекомендации и другие справочные документы постоянно пересматриваются, поэтому всем пользователям данной Рекомендации настоятельно рекомендуется изучить возможность использования последних изданий, перечисленных ниже Рекомендаций и других справочных документов. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка в настоящей Рекомендации на какой-либо документ не придает этому отдельному документу статуса Рекомендации.

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

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

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

[ITU-T Y.2703] Recommendation ITU-T Y.2703 (2009), *The application of AAA service in NGN.*

[ITU-T Y.2720] Рекомендация МСЭ-Т Y.2720 (2009 г.), *Структура управления определением идентичности в СПП.*

[ITU-T X.509] Рекомендация МСЭ-Т X.509 (2008 г.) | ISO/IEC 9594-8:2008, *Информационные технологии – Взаимосвязь открытых систем – Справочник: Структуры сертификатов открытых ключей и атрибутов*.

[ITU-T X.660] Recommendation ITU-T X.660 (2008) | ISO/IEC 9834-1:2008, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the International Object Identifier tree.*

[ITU-T X.1035] Recommendation ITU-T X.1035 (2007), *Password-authenticated key exchange (PAK) protocol.*

[IETF RFC4302] IETF RFC 4302 (2005), IP Authentication Header.

[IETF RFC4303] IETF RFC 4303, IP (2005), Encapsulating Security Payload (ESP).

[IETF RFC5246] IETF RFC 5246 (2008), The Transport Layer Security (TLS) Protocol Version 1.2.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 активы (asset) [ITU-T Y.2701]: Все, что имеет ценность для организации, ее бизнеса, функционирования и целостности.

3.1.2 пограничный элемент (border element) [ITU-T Y.2701]: Элемент сети, выполняющий функции соединения различных доменов безопасности и административных доменов.

3.1.3 корпоративная сеть (corporate network) [ITU-T Y.2701]: Частная сеть, которая поддерживает множество пользователей и которая может располагаться во многих местах, например на предприятии, в университетском городке.

3.1.4 пограничный элемент домена (domain border element) [ITU-T Y.2701]: Пограничный элемент, единолично управляемый поставщиком, предоставляющим функции безопасности другим доменам сети.

3.1.5 служба электросвязи в чрезвычайных ситуациях (Emergency telecommunications service, ETS) [b-ITU-T E.107]: Национальная служба, предоставляющая приоритетную связь для авторизованных пользователей ETS в случае стихийных бедствий и чрезвычайных ситуаций.

3.1.6 пограничный элемент сети (network border element) [ITU-T Y.2701]: Пограничный элемент под единоличным контролем поставщика, обеспечивающий выполнение функций безопасности связи с оконечным оборудованием.

3.1.7 домен безопасности (security domain) [ITU-T Y.2701]: Совокупность элементов, политика безопасности, орган безопасности и совокупность действий по обеспечению безопасности, в которых управление элементами осуществляется в соответствии с политикой безопасности. Эта политика будет проводиться органом безопасности. Данный домен безопасности может простираться на несколько зон безопасности.

3.1.8 метка безопасности (security token) [b-ITU-T X.810]: Набор данных, защищаемых с помощью одной или нескольких услуг безопасности, а также информация для обеспечения безопасности, используемая для предоставления этих услуг безопасности, которые передаются между взаимодействующими объектами.

3.1.9 зона безопасности (security zone) [ITU-T Y.2701]: В [ITU-T Y.2701] определены 3 зоны безопасности: 1) доверенная; 2) доверенная, но уязвимая; и 3) недоверенная. Зона безопасности определяется оперативным управлением, местоположением и возможностью соединения с другими устройствами/элементами сети.

3.1.10 пограничный элемент оконечного оборудования [ITU-T Y.2701]: Пограничный элемент, выполняющий функции безопасности между оборудованием в помещении абонента и сетью поставщика услуг.

3.1.11 доверие (trust) [ITU-T Y.2701]: Считается, что объект X доверяет объекту Y относительно некоторой совокупности действий, если и только если объект X надеется, что в отношении данных действий объект Y будет вести себя определенным образом.

3.1.12 доверенная, но уязвимая зона (trusted but vulnerable zone) [ITU-T Y.2701]: С точки зрения поставщика услуг СПП, зона безопасности – это зона, в которой работают (предоставлены и обслуживаются) элементы сети/устройства этого поставщика услуг СПП. Оборудование может управляться либо пользователем/абонентом, либо поставщиком услуг СПП. Кроме того, оборудование может размещаться как в пределах домена поставщика услуг СПП, так и за его границами. Оно связывается как с элементами доверенной зоны, так и с элементами в недоверенной зоне, именно поэтому оно является "уязвимым". Главной функцией безопасности является такая защита элементов сети (NE) от атак безопасности, инициируемых в недоверенной зоне, при которой не возникает неисправностей.

3.1.13 доверенная зона (trusted zone) [ITU-T Y.2701]: С точки зрения поставщика услуг СПП, доверенная зона – это домен безопасности, в котором находятся элементы сети и системы поставщика услуг СПП, которые никогда не связываются непосредственно с абонентским оборудованием. Общие характеристики элементов сети СПП в этом домене заключаются в том, что данные элементы полностью контролируются соответствующим поставщиком услуг СПП, находятся в собственности поставщика услуг СПП, что гарантирует физическую безопасность, и они связаны только с элементами в "доверенной" зоне и с элементами в "доверенной, но уязвимой" зоне.

3.1.14 недоверенная зона (un-trusted zone) [ITU-T Y.2701]: С точки зрения поставщика услуг СПП, недоверенная зона – это зона, в которую включены все элементы сети сетей пользователей или возможно одноранговых сетей, или зоны других поставщиков услуг СПП за пределами исходного домена, которые соединяются с пограничными элементами данного поставщика услуг СПП.

3.1.15 пользователь (user) [b-ITU-T Y.2091]: Понятие "пользователь" включает в себя конечного пользователя, физическое лицо, абонента, систему, оборудование, терминал, например факс, персональный компьютер, (функциональный) объект, процесс, приложение, поставщика или корпоративную сеть.

3.1.16 сеть пользователя (user network) [ITU-T Y.2701]: Частная сеть, состоящая из оконечного оборудования, в которой может быть множество пользователей.

3.2 Термины, определенные в данной Рекомендации

В данной Рекомендации определяются следующий термин:

3.2.1 аутентификатор (authenticator): Аутентификатор – это элемент сети, который содействует идентификации и аутентификации абонентов, устройств и конечных пользователей. Например, пограничные элементы, имеющие функциональную возможность двустороннего агента пользователя (B2BUA) или функционального объекта посредника управления вызовами и сеансами связи (P-CSC-FE) могут являться аутентификаторами абонентов для услуг на базе протокола SIP.

4 Сокращения и акронимы

В данной Рекомендации используются следующие сокращения и акронимы:

3G	3rd Generation	Третье поколение
AGW	Access Gateway	Шлюз доступа
AH	Authentication Header	Заголовок аутентификации
AKA	Authentication and Key Agreement	Соглашение об аутентификации и ключе
ANI	Application-to-Network Interface	Интерфейс приложение-сеть
AS/WS	Application Server/Web Server	Сервер приложения/веб-сервер
AuC	Authentication Center	Центр аутентификации
B2BUA	Back-to-Back User Agent	Двусторонний агент пользователя
BE	Border Element	Пограничный элемент
BSR	Base Station Router	Маршрутизатор базовой станции
CA	Certification Authority	Орган по сертификации
COPS	Common Open Policy Service	Общая открытая служба политики

CRL	Certificate Revocation List		Список аннулированных сертификатов
CSC-FE	Call Session Control Functional Entity		Функциональный объект управления вызовами и сеансами связи
DBE	Domain Border Element		Пограничный элемент домена
DNS	Domain Name System		Система наименований доменов
DoS	Denial of Service		Отказ в обслуживании
DMTF	Dual-Tone Multi-Frequency		Двухтональный многочастотный набор
ECC	Elliptic Curve Cryptography		Криптография на основе эллиптических кривых
ESP	Encapsulating Security Protocol		Протокол безопасного закрытия содержания
ETS	Emergency Telecommunications Service		Служба электросвязи в чрезвычайных ситуациях
FE	Functional Entity		Функциональный объект
GBA	Generic Bootstrapping Architecture		Общая архитектура начальной загрузки
GW	Gateway		Шлюз
HMAC	Hash Message Authentication Code		Хешированный код аутентификации сообщения
HTTP	Hypertext Transfer Protocol		Протокол передачи гипертекста
I-CSC-FE	Interrogating Call Session Control Functional Entity		Запрашивающий функциональный объект управления вызовами и сеансами связи
ID	Identity		Идентичность
IdM	Identity Management		Управление определением идентичности
IDPS	Intrusion Detection and Prevention Systems		Системы обнаружения и предотвращения проникновений
IDS	Intrusion Detection Systems		Системы обнаружения проникновений
IKE	Internet Key Exchange		Обмен ключами в интернете
IMS	IP Multimedia Subsystem		Мультимедийная подсистема IP
IP	Internet Protocol		Протокол Интернет
ISDN	Integrated Services Digital Network	ЦСИС	Цифровая сеть с интеграцией служб
LAN	Local Area Network		Локальная сеть
MD5	Message Digest 5		Профиль сообщения 5
MIB	Management Information Base		База управляющей информации
MPLS	MultiProtocol Label Switching		Многопротокольная коммутация по меткам
MRP-FE	Media Resource Processing Functional Entity		Функциональный объект обработки медиаресурсов
MS	Mobile station		Подвижная станция
NAC-FE	Network Access Control Functional Entity		Функциональный объект управления доступом в сеть
NAPT	Network Address and Port Translation		Трансляция сетевых адресов и портов
NAT	Network Address Translation		Трансляция сетевого адреса
NBE	Network Border Element		Пограничный элемент сети
NE	Network Element		Элемент сети
NGN	Next Generation Network	СПП	Сеть последующего поколения
NNI	Network-to-Network Interface		Межсетевой интерфейс
OAMP	Operations, Administration, Maintenance and Provisioning		Эксплуатация, администрирование, техническое обслуживание и обеспечение доступа

OID	Object Identifier		Идентификатор объекта
ONU	Optical Network Units		Элементы оптической сети
PAK	Password Authenticated Key		Ключ аутентификации на основе пароля
P-CSC-FE	Proxy Call Session Control Functional Entity		Функциональный объект посредника управления вызовами и сеансами связи
POTS	Plain Old Telephone Service		Обычная аналоговая телефонная служба
PSTN	Public Switched Telephone Network	КТСОП	Коммутируемая телефонная сеть общего пользования
QoS	Quality of Service		Качество обслуживания
RAC-FE	Resource and Admission Control Functional Entity		Функциональный объект управления ресурсами и установлением соединений
RADIUS	Remote Authentication Dial In User Service		Услуга удаленной аутентификации вызывающего пользователя
RAN	Radio Access Network		Сеть с радиодоступом
RTSP	Real Time Streaming Protocol		Потоковый протокол реального времени
SAA-FE	Service Authentication and Authorization Functional Entity		Функциональный объект аутентификации и авторизации услуги
SASL	Simple Authentication and Security Layer		Простой уровень аутентификации и безопасности
S-CSC-FE	Serving Call Session Control Functional Entity		Обслуживающий функциональный объект управления вызовами и сеансами связи
SDP	Session Description Protocol		Протокол описания сеанса связи
SIM	Subscriber Identity Module		Модуль идентификации абонента
SIP	Session Initiation Protocol		Протокол инициации сеанса связи
SLA	Service Level Agreement		Соглашение об уровне обслуживания
SL-FE	Subscription Locator Functional Entity		Функциональный объект обнаружения данных о правах подписки
SNMP	Simple Network Management Protocol		Простой протокол управления сетью
SRTP	Secure Real Time Protocol		Защищенный протокол реального времени
TAA-FE	Transport Authentication and Authorization Functional Entity		Функциональный объект аутентификации и авторизации транспортировки
TCP	Transmission Control Protocol		Протокол управления передачей
TE	Terminal Equipment		Оконечное оборудование
TE-BE	Terminal Equipment Border Element		Пограничный элемент оконечного оборудования
TLS	Transport Layer Security		Безопасность на транспортном уровне
TMN	Telecommunications Management Network	СУЭ	Сеть управления электросвязью
TRIP	Telephony Routing over IP		Протокол маршрутизации телефонии по протоколу Интернет
UA	User Agent		Агент пользователя
UDP	User Datagram Protocol		Протокол передачи дейтаграмм пользователя
UE	User Equipment		Оборудование пользователя
UICC	Universal Integrated Circuit Card		Универсальная карта с микропроцессором
UMTS	Universal Mobile Telecommunications System		Универсальная система подвижной связи
UNI	User-to-Network Interface		Интерфейс пользователь-сеть
URL	Uniform Resource Locator		Унифицированный указатель ресурсов
USIM	Universal Subscriber Identity Module		Универсальный модуль идентификации абонента
VLAN	Virtual LAN		Виртуальная локальная сеть

VPN	Virtual Private Network	Виртуальная частная сеть
WLAN	Wireless LAN	Беспроводная локальная сеть доступа
xDSL	x Digital Subscriber Line	Любая цифровая абонентская линия

5 Условные обозначения

Нет.

6 Риски и угрозы безопасности

Информация о рисках и угрозах безопасности, предполагаемых в среде СПП, представлена в пункте 4 [ITU-T Y.2701].

7 Модель доверия безопасности

Выбор поставщиком услуг СПП механизмов безопасности зависит от применяемой модели доверия. В настоящей Рекомендации предполагается использовать модель доверия безопасности, определенную в [ITU-T Y.2701]. В данном пункте приводится краткий обзор модели доверия безопасности СПП, определенной в [ITU-T Y.2701].

В функциональной эталонной архитектуре СПП определяются функциональные объекты (FE). Тем не менее, так как аспекты безопасности сети значительно зависят от способа, при помощи которого FE, физически связаны друг с другом, архитектура безопасности СПП основывается на физических элементах сети (NE), т. е. материальных модулях, содержащих один или несколько FE. Способ группирования данных объектов FE в элементы NE будет меняться в зависимости от поставщика и поставщика услуг СПП.

7.1 Единая сетевая модель доверия

В данном пункте определяются три зоны безопасности:

1) доверенная;

2) доверенная, но уязвимая;

3) недоверенная,

которые зависят от эксплуатационного управления, местоположения и возможности соединения с другими устройствами/элементами сети. Эти три зоны представлены в модели доверия безопасности, показанной на рисунке 1.

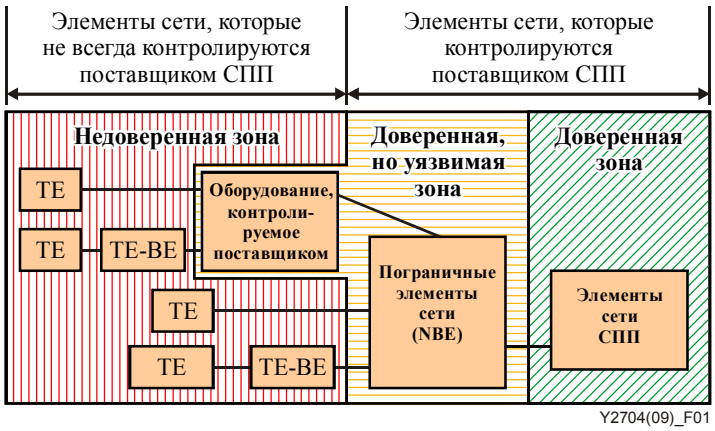


Рисунок 1 – Модель доверия безопасности/[ITU-T Y.2701]

"Доверенная зона безопасности сети" или, для краткости, "доверенная зона" – это зона, где расположены элементы сети и системы поставщика услуг СПП, которые никогда не связываются напрямую с оборудованием пользователя или другими доменами. Общие характеристики элементов сети СПП в данной области заключаются в том, что:

1) они полностью управляются поставщиком услуг СПП (для предоставления услуг, технического обслуживания и оперативного управления);

2) они расположены в домене поставщика услуг СПП; и

3) они связываются с другими элементами только в "доверенной" зоне и в "доверенной, но уязвимой" зоне.

Не следует считать, что раз элемент сети находится в доверенной зоне, то он обязательно в безопасности.

Элементы сети в "доверенной зоне" будут защищаться совокупностью различных методов. В качестве примера можно привести физическую безопасность элементов сети СПП, общее усиление защиты систем, применение защищенной сигнализации, безопасность для сообщений управления и использование отдельной сети VPN в пределах сети MPLS/IP. Ожидается, что для защиты связи в пределах "доверенной" зоны и между элементами сети СПП в "доверенной" и в "доверенной, но уязвимой" зоне будет применяться такая же совокупность методов.

"Доверенная, но уязвимая зона безопасности сети", или, для краткости, "доверенная, но уязвимая зона" – это зона, в которой сетевые элементы/устройства поддерживают связь с элементами в "недоверенной" зоне, которые поэтому являются "уязвимыми". Кроме того, они поддерживают связь с элементами в "доверенной" зоне. Как и элементы сети в "доверенной" зоне, это оборудование управляется поставщиком услуг СПП, хотя оборудование может находиться как в помещениях поставщика услуг СПП, так и в других местах. Его главная функция безопасности заключается в защите элементов NE в доверенной зоне от атак на систему безопасности, инициированных в недоверенной зоне. Совокупность методов, применяемых для защиты связи между элементами сети СПП в "доверенной, но уязвимой" зоне и в "недоверенной" зоне, могут отличаться от применяемых для безопасной связи в "доверенной" зоне.

Элементы, располагающиеся в домене поставщика услуг СПП, имеющие возможность соединения с элементами, находящимися вне доверенной зоны, называются пограничными элементами сети (NBE). Например, такими элементами являются:

- "Пограничные элементы сети (NBE)" на интерфейсе UNI, которые служат средствами связи с управлением услугой или транспортными элементами поставщика услуг СПП в доверенной зоне для обеспечения доступа пользователя/абонента к сети поставщика услуг СПП с целью получения услуг и/или транспортировки данных.
- "Пограничные элементы домена (DBE)", которые аналогичны пограничным элементам сети, за исключением того, что они находится между двумя доменами.
- "Элементы NBE системы конфигурации устройств и начальной загрузки (DCB-NBE)", которые служат интерфейсами с системой конфигурации устройства поставщика услуг СПП в доверенной зоне, для того чтобы конфигурировать устройство пользователя/абонента и оборудование поставщика услуг СПП, относящееся к линейным сооружениям.
- "Элементы OAMP-NBE", которые служат интерфейсами с системами OAMP поставщика услуг СПП в доверенной зоне, для того чтобы обеспечивать доступ и техническое обслуживание для устройств пользователя/абонента и оборудования определенного поставщика услуг СПП, расположенного на внешних линейных сооружениях.
- "Элементы NBE сервера приложения/веб-сервера (AS/WS-NBE)", которые служат интерфейсами с AS/WS-NBE поставщика услуг СПП в доверенной зоне, для того чтобы предоставлять пользователю/абоненту доступ к веб-услугам.

На рисунке 1 показана взаимосвязь между этими элементами NBE и NE, которые требуется защищать.

К примерам устройств/элементов, которые управляются поставщиком услуг СПП, но не располагаются в помещениях поставщика услуг СПП, и могут находиться или не находиться под управлением поставщика услуг СПП, относятся:

- оборудование сети/технологии доступа, относящееся к линейным сооружениям;
- маршрутизатор базовой станции (BSR) – элемент сети, объединяющий базовую станцию, контроллер радиосети и функциональные возможности маршрутизатора для беспроводного доступа;
- элементы оптической сети (ONU) в пределах местонахождения пользователя/абонента.

Для защиты "доверенной, но уязвимой" зоны, состоящей из NBE, используется совокупность различных методов. Некоторыми примерами являются физическая безопасность элементов сети СПП, общее усиление защиты систем, использование безопасной сигнализации для всех сообщений сигнализации, направляемых элементам сети СПП в "доверенной" зоне, безопасность для сообщений OAMP, а также по необходимости модульные фильтры пакетов и брандмауэры. "Недоверенная" зона включает в себя все элементы сети абонентских сетей или, возможно, одноранговых сетей, или доменов других поставщиков услуг СПП, которые связаны с пограничными элементами поставщика услуг СПП. В "недоверенной" зоне, состоящей из оконечного оборудования, оборудование не управляется поставщиком, и может не быть возможности заставить пользователя выполнять политику безопасности поставщика услуг СПП. Тем не менее желательно принимать некоторые меры безопасности, и с этой целью рекомендуется, чтобы сигнализация, среда передачи и OAMP были бы защищены и чтобы был бы укреплен TE-BE, расположенный в "недоверенной" зоне. Однако из-за связи с элементами сети в "недоверенной" зоне, уровень безопасности меньше, чем в "доверенной" зоне.

7.2 Одноранговая сетевая модель доверия

Когда сеть СПП соединена с другой сетью, наличие или отсутствие доверия зависит от:

- физического присоединения, причем присоединение может варьироваться от непосредственной связи в защищенном здании до связи между отдельными (возможно небезопасными) зданиями через совместно используемые устройства;
- одноранговой модели, в которой обмен трафиком может происходить непосредственно между двумя поставщиками услуг СПП или через одного или нескольких поставщиков транспортных сетей СПП;
- деловых отношений между сетями, к которым могут относиться пункты о штрафах в соглашениях SLA и/или доверие к политике безопасности другого поставщика услуг СПП; как правило, поставщики услуг СПП должны считать других поставщиков недоверенными.

На рисунке 2 приведен пример, когда присоединенная сеть считается недоверенной.

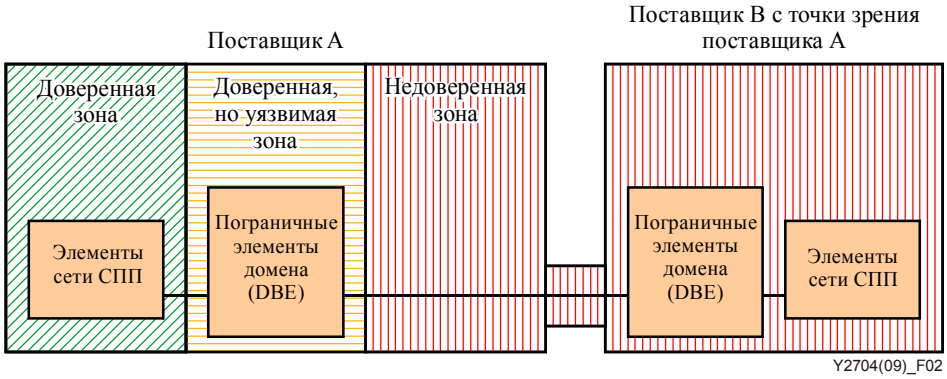


Рисунок 2 – Одноранговая модель доверия/[ITU-T Y.2701]

8 Идентификация, аутентификация и авторизация

Информация, касающаяся идентификации, аутентификации, авторизации и управления определением идентичности (IdM), представлена в [ITU-T Y.2701], [ITU-T Y.2702], [ITU-T Y.2703] и [ITU-T Y.2720].

В данном пункте описываются механизмы идентификации, аутентификации и авторизации, в частности те, которые касаются услуг на основе протокола SIP. Механизмы, касающиеся других услуг, подлежат дальнейшему изучению.

8.1 Абоненты

Запрос какой-либо услуги СПП ставится в соответствие с абонентом. Это соответствие определяется посредством запроса с пользователем. Может потребоваться дополнительная идентификация (и связанная с ней аутентификация) конечного пользователя в зависимости от соглашения об уровне обслуживания (SLA) между поставщиком услуг СПП и абонентом.

Данный процесс может выполняться с использованием функционального элемента, облегчающего идентификацию и аутентификацию абонентов, устройств или оконечных пользователей (называемого аутентификатором). Например, для услуг на базе протокола SIP аутентификаторами абонента могут быть пограничные элементы сети (NBE) с функциями двустороннего агента пользователя (B2BUA) или функциональный объект посредника управления вызовами и сеансами связи (P-CSC-FE). Идентификация и аутентификация обеспечивается путем обмена полномочиями между аутентификатором и оконечным оборудованием (TE).

8.2 Элемент сети

В [ITU-T Y.2701] при осуществлении связи рекомендуется идентифицировать и аутентифицировать элементы сети.

Если пограничный элемент получает запрос от элемента сети СПП из доверенной зоны, то информация для идентификации, содержащаяся в запросе, может считаться точной и не подвергаться дополнительной проверке, в зависимости от политики безопасности, применяемой поставщиком услуг СПП.

Если пограничный элемент получает запрос от элементов сети СПП из недоверенной и доверенной, но уязвимой зон, то рекомендуется осуществлять идентификацию и аутентификацию этих элементов сети и проверять привилегии в отношении связи. Идентификация и аутентификация обеспечивается путем обмена и подтверждения полномочий между аутентификатором и NE.

8.3 Использование полномочий при обеспечении безопасности СПП

В системе безопасности СПП полномочия используются для идентификации и аутентификации устройства, абонента и/или конечного пользователя. Типы полномочий для идентификации и аутентификации устройства, абонента и/или конечного пользователя описаны в пункте 8.3.1. Полномочия могут быть двух разных видов: либо сертификаты открытого ключа X.509 (описаны в пункте 8.3.2), либо совместно используемый ключ (описан в пункте 8.3.3). Сертификаты X.509 могут использоваться для установления безопасного транспортного соединения между оконечным оборудованием (TE) и аутентификатором (описано в пункте 8.3.1) на основе политики, применяемой поставщиком услуг СПП. Совместно используемый ключ может применяться либо для установления безопасного транспортного соединения, либо при создании/проверке отклика на вызов, инициированный аутентификатором (описано в пункте 8.3.1) на основе политики, применяемой поставщиком услуг СПП.

8.3.1 Полномочия устройства, абонента и конечного пользователя

В СПП используются три различных типа полномочий:

1) полномочия устройства;
2) полномочия абонента; и
3) полномочия конечного пользователя.

Полномочия устройства могут поставляться производителем вместе с устройством. Например, при производстве устройства производителем могут быть прошиты полномочия, включающие в себя такую информацию, как серийный номер или название компании-производителя. Полномочия устройства идентифицируют это устройства. Любой поставщик услуг СПП может поставить полномочия устройства в соответствие с услугой конкретного абонента, с тем чтобы уменьшить

необходимость в полномочиях абонента. В таких случаях запросы от устройства могут быть поставлены в соответствие с конкретной учетной записью, согласно политике поставщика услуг СПП.

Полномочия абонента используются для установления соответствия между отправителем запроса СПП и конкретной учетной записью. Полномочия абонента вводятся (например, с помощью загрузки, SIM-карты и т. д.) в устройство, способное принимать такие полномочия. Полномочия абонента, установленные в устройство, обеспечивают соответствие абонента этому устройству. Все вызовы, совершаемые с какого-либо устройства, будут ставиться в соответствие с абонентом, полномочия которого установлены в этом устройстве. В одном устройстве может быть установлено много наборов полномочий. В этом случае устройство предоставляет средства для проведения различия между запросами, относящимися к каждому абоненту.

ПРИМЕЧАНИЕ. – Абонент СПП может иметь одну или несколько подписок на услуги СПП, не относящихся к какому-либо устройству или относящихся к одному или нескольким устройствам. Кроме того, подписки СПП могут быть связаны с одним или несколькими конечными пользователями (т. е. конечный пользователь не обязательно является абонентом), которые могут использовать различные устройства или совместно использовать одно и то же устройство, согласно политике поставщика услуг СПП.

Полномочия конечного пользователя используются для идентификации и аутентификации конкретных конечных пользователей в сети. Например, с помощью SIM-карты можно идентифицировать конечного пользователя применительно к услуге; когда конечный пользователь помещает в телефон свою SIM-карту, между телефоном и этим конечным пользователем устанавливается соответствие и все вызовы идентифицируются как вызовы, исходящие от этого пользователя. Еще одним примером является метка безопасности, представляющая собой аппаратную метку (физическое устройство) или программную метку (программу, установленную на универсальном устройстве, например персональном компьютере). Данная метка предоставляется авторизованному пользователю, чтобы расширить возможности процесса аутентификации. В метке безопасности могут храниться криптографические ключи, например цифровая подпись, или биометрические данные, например отпечатки пальцев. Запрос, создаваемый устройством СПП, будет идентифицирован и аутентифицирован как запрос, поступивший от конечного пользователя, которому соответствует данная метка безопасности. В определенных сценариях, например как в вышеописанном случае с SIM-картой, имеется возможность того, чтобы много конечных пользователей пользовалось услугой, которая соответствует одному абоненту (т. е. учетной записи абонента), и стоимость вызовов, инициируемых конечным пользователем, относится на учетную запись абонента. Абонент и конечный пользователь могут совпадать, либо же на одного абонента может приходиться много конечных пользователей. Конечные пользователи могут идентифицироваться или аутентифицироваться в сети, чтобы воспользоваться персональными услугами. С использованием полномочий конечного пользователя между оконечным оборудованием и сетью СПП (аутентификатором) могут устанавливаться индивидуальные ассоциации безопасности на транспортном уровне. Для целей выставления счетов поставщик услуг СПП ставит полномочия конечного пользователя в соответствие с конкретной услугой пользователя.

8.3.2 Сертификаты открытого ключа X.509 в роли полномочий

Сертификат открытого ключа X.509 – это цифровой документ, который включает в себя идентификатор объекта, его атрибуты, открытый ключ, который принадлежит объекту, а также другую информацию аутентификации (например, информацию об органе, выдающем сертификат, список аннулированных сертификатов (CRL), даты и время начала и окончания действия сертификата и т. д.). Описание некоторых основных полей и некоторых полей расширения сертификата X.509 представлено в таблице 1. Более подробное описание полей сертификата открытого ключа X.509 представлено в [ITU-T X.509]. Сертификат открытого ключа подписывается в цифровом виде доверенной третьей стороной, которая обычно называется органом по сертификации (CA) для сертификата открытого ключа. CA вычисляет хеш-значение, например с использованием алгоритма SHA-1, для всех полей за исключением поля *Signature Value,* шифрует его со своим собственным закрытым ключом, и затем добавляет подпись вместе с алгоритмом подписи, применяемым в сертификату (в поле *Signature Value*).

Таблица 1 – Некоторые основные поля и поля расширения сертификата открытого ключа X.509

Название поля	Описание
Subject	Идентифицирует объект, относящийся к сертификату открытого ключа (известное имя из справочника субъекта сертификации)
Serial number	Уникальный идентификатор сертификата
Issuer	Идентифицирует объект, который подписал и выдал сертификат (известное имя справочника CA)
Valid From	Дата и время начала срока действия сертификата
Valid To	Дата и время окончания срока действия сертификата
Public Key	Открытый ключ держателя сертификата
Version	Версия зашифрованного сертификата открытого ключа X.509
Subject Alternative Name	Другой идентификатор держателя сертификата
CRL Distribution Points	Имя или адрес распределительного пункта CRL
Authority Information Access	Имя или адрес для доступа к информации об органе по сертификации (CA)
Enhanced Key Usage	Описание целей, для которых может использоваться сертификат (список идентификаторов объектов (OID), определенный в МСЭ-Т | ИСО/МЭК) [ITU-T X.660]
Application policies	Приложения и услуги, для которых может использоваться сертификат (определяются с помощью OID)
Certificate Policies	Политика и механизмы, используемые органом по сертификации для получения запроса на обработку, авторизацию, выпуск сертификатов и управление их использованием
Signature Algorithm	Идентификатор алгоритма для алгоритма и хеш-функции, используемый CA при подписании сертификата (например, SHA-1 с RSA)
Signature Value	Действительная подпись сертификата

Сертификаты открытого ключа, определенные в [ITU-T X.509], могут использоваться элементами сети СПП при установлении ассоциаций безопасности с другими элементами сети, а также обеспечивают основу для взаимной идентификации и аутентификации. Они могут также использоваться между оконечным оборудованием и аутентификатором для тех же целей.

Применительно к сертификату абонента или конечного пользователя поле <Subscriber Account Identifier> (см. пункт 8.4.2), представляющее собой идентификатор для извлечения информации об учетной записи абонента, используется аутентификатором для получения дополнительной информации посредством функциональных объектов SAA/TAA. Применительно к сертификату устройства, название производителя устройства и серийный номер устройства используются аутентификатором для определения соответствующего поля <Subscriber Account Identifier> (применимо только если устройство поставлено в соответствие абоненту), и далее поле <Subscriber Account Identifier> используется, как описано для получения дальнейшей информации о полномочиях посредством SAA/TAA-FE.

Сертификаты конечного пользователя, услуги и устройства могут использоваться при создании соединений TLS между устройством и аутентификатором (пункт 9.1.2) или могут использоваться при создании соединений IPsec посредством аутентификации методом IKE (пункт 9.2.4.3).

8.3.3 Разделенные ключи в роли полномочий

Разделенный ключ может использоваться для улучшения безопасности доступа в СПП. В этом случае одна из копий разделенного ключа передается абоненту или конечному пользователю, а другая копия хранится в соответствующих функциональных объектах, например функциональных объектах профиля пользователя услуги (SUP-FE) или функциональных объектах профиля пользователя транспорта (TUP-FE). Требуется, чтобы каждый ключ имел уникальное название, и это название используется аутентификатором для получения дополнительной информации о полномочиях.

При использовании предварительно разделенных ключей надежность системы зависит от надежности разделенного секрета. Цель состоит в том, чтобы не допустить того, чтобы разделенный секрет стал слабым звеном в цепочке безопасности. Это означает, что энтропия (случайность) разделенного секрета должна быть такой же высокой, как и энтропия используемого шифра. Другими словами, рекомендуется, чтобы энтропия разделенного секрета составляла не менее 128–160 бит.

Следует заметить, что подход с симметричными ключами имеет определенные отличия от подхода с ассиметричными ключами, описанными в пункте 8.3.2, и следует иметь в виду, что:

– объект должен иметь отдельный набор симметричных ключей для каждого партнера по связи;

– ключи должны предоставляться, создаваться и храниться безопасным способом;

– объект должен доверять своему партнеру в сохранении секрета разделенного ключа.

8.3.4 Информация, предоставляемая в функциональных объектах SUP/TUP для каждого набора полномочий

Функциональные объекты SUP/TUP являются хранилищами для всех полномочий устройств, абонентов и конечных пользователей, которые должны использоваться для доступа к инфраструктуре СПП. Они, как правило, реализуются в виде неотъемлемой части аутентификатора, с тем чтобы оптимизировать процесс обработки запросов аутентификации. Однако для обеспечения мобильности, аутентификатору может понадобиться обратиться за консультацией к удаленному серверу функциональных объектов SAA/TAA, чтобы получить информацию о полномочиях. Идентификатор учетной записи абонента или название ключа используются для извлечения и информации посредством функциональных объектов SAA/TAA.

Следующая информация, относящаяся к безопасности, связанная с каждым набором полномочий, необходима для предоставления в функциональны объектах, например SUP/TUP, в которых хранятся полномочия:

1) идентификатор учетной записи или название ключа;

2) требуется ли для данного абонента идентификация и аутентификация конечного пользователя;

3) описывают ли полномочия абонента или конечного пользователя; и

4) допустимые значения заголовка "From" в запросах.

Ниже приводится несколько примеров информации, содержащейся в хранилищах полномочий, например в функциональных объектах SUP/TUP.

Для сертификата устройства, относящегося к оконечному оборудованию СПП, которое использует четыре линии POTS с номерами 212-555-1111-1113 и 1151:

Учетная запись абонента:	123-456789
Заголовки "From":	sip:212-555-111[1-3]@NGN .ngn.com
	| sip:212-555-1151@NGN .ngn.com
Последовательность, подтверждающая идентичность:	sip:212-555-1111@NGN .ngn.com
Тип полномочий:	subscriber
Требуются идентификатор конечного пользователя:	no

Для сертификата абонента, присвоенного семье Джона Доу:

Учетная запись абонента:	Doe-family
Заголовки "From":	sip:*Doe@NGN .ngn.com
Последовательность, подтверждающая идентичность:	sip:Doe@NGN .ngn.com
Тип полномочий:	subscriber
Требуются идентификатор конечного пользователя:	no

Для предварительно разделенного ключа, присвоенного семье Джона Доу:

Название ключа:	JohnDoe
Ключ:	dfe56131d1958046689d83306477ecc
Заголовки "From":	sip:*Doe@NGN .ngn.com
Последовательность, подтверждающая идентичность:	sip: Doe@NGN .ngn.com
Тип полномочий:	subscriber
Требуются идентификатор конечного пользователя:	no

Для пограничного элемента оконечного оборудования, обслуживающего компанию Acme Widget:

Учетная запись абонента:	Acme Widget Company
Заголовки "From":	sip:*@acme.com
Последовательность, подтверждающая идентичность:	sip:acme.com
Тип полномочий:	subscriber
Требуются идентификатор конечного пользователя:	no

Для конечного пользователя в компании Acme Widget:

Учетная запись абонента:	Acme Widget Company
Заголовки "From":	sip:bob@acme.com
Последовательность, подтверждающая идентичность:	sip:bob@acme.com
Тип полномочий:	end-user

8.4 Идентификация и аутентификация абонентов

8.4.1 Общая стратегия

Идентичность отправителя в протоколе SIP обычно содержится в заголовке "From". Однако процесс идентификации абонента путем использования заголовка "From" в запросе SIP подвержен спуфинг-атакам и, таким образом, не используется при необходимости обеспечения более высокого уровня гарантии идентичности абонента. Вместо этого значение поля "From" сравнивается в идентичностью абонента, полученной другими способами.

Для того чтобы свести к минимуму задержку при установлении вызова, идентификация и аутентификация абонента осуществляются на основе сетевого адреса источника (адреса источника в заголовке пакета IP) или ассоциации безопасности транспортировки (ассоциации, устанавливаемые, например, по протоколам IPsec или TLS между вызывающим устройством и аутентификатором), когда это возможно. Если при использовании этих методов не происходит идентификации, соответствующей заголовку "From" в запросе SIP, то отправителю направляется вызов; если в ответе содержатся надлежащие полномочия, то запрос обрабатывается. Более подробная информация об этих процедурах описывается в следующих пунктах.

Процедуры, указанные в пункте 8.4.2, описывают то, каким образом аутентификтор определяет на основе сетевого адреса источника, что либо:

1) абонента невозможно определить с помощью данного метода;

2) абонент определен и он соответствует заголовку "From" в запросе;

3) абонент определен, однако он отличается от абонента, указанного в заголовке "From" в запросе.

Процедуры, указанные в пункте 8.4.3, описывают то, каким образом аутентификатор определяет на основе ассоциации безопасности транспортировки, что либо:

1) абонента невозможно определить с помощью данного метода;

2) абонент определен и он соответствует заголовку "From" в запросе;

3) абонент определен, однако он отличается от абонента, указанного в заголовке "From" в запросе.

Действия, которые далее осуществляются аутентификатором, описаны в таблице 2.

Таблица 2 – Действия, осуществляемые аутентификатором по каждому результату аутентификации

Определение абонента на основе адреса	**Определение абонента на основе безопасности транспортировки**	**Действия аутентификатора**
н/п	н/п	Использование вызова/ответа
н/п	Совпадает	OK
н/п	Отличается	Использование вызова/ответа
Совпадает	н/п	OK
Совпадает	Совпадает	OK
Совпадает	Отличается	Использование идентичности абонента, содержащейся в сетевом адресе источника
Отличается	н/п	Использование вызова/ответа
Отличается	Совпадает	Использование идентичности абонента из ассоциации безопасности транспортировки
Отличается	Отличается	Использование вызова/ответа
н/п: Не применимо.		

Если действие по результатам заключается в использовании вызова/ответа, то следуют процедуре, описанной в пункте 8.4.4.

Помимо стратегий, описанных в пунктах 8.4.2–8.4.4, для идентификации и аутентификации абонентов может также использоваться общая архитектура начальной загрузки (GBA), описание которой приводится в пункте 8.4.5.

Стратегии аутентификации, описанные в этой Рекомендации, являются типовыми примерами, и каждый поставщик услуг СПП может выбирать, какие из этих стратегий использовать (например, использовать только одну процедуру, описанную в следующих пунктах).

8.4.2 Идентификация абонента с помощью сетевого адреса источника

Данная форма идентификации абонента является самой простой. Она основывается только на адресе источника, поставляемом в пакетах IP. Аутентификатор обращается к предварительно распределенным диапазонам адресов IP для поиска поля < Subscriber Account Identifier >, и если адрес источника запроса находится в пределах одного из этих диапазонов, то аутентификатор считает, что исходящий запрос направлен от абонента. Далее поле < Subscriber Account Identifier > используется для получения полномочий абонента через функциональные объекты SAA/TAA и проверки на соответствие значению заголовка "From".

Если значение заголовка "From" соответствует абоненту, то считается, что имеет место "совпадение"; если значение заголовка "From" не соответствует абоненту, то считается, что имеет место "отличие"; если источник IP-адреса не содержится ни в одном из предварительно установленных соответствий для диапазонов адресов, то считается, что источник "не установлен".

Надежность этого метода идентификации абонента зависит от обеспечения гарантии адреса источника. Гарантирование адреса источника означает, что IP-адрес может использоваться только законным абонентом, которому присвоен адрес. Для достижения этого функциональным объектам транспортной обработки или транспортного управления необходимы следующие два механизма, которые должны координироваться надлежащим образом: 1) строгое управление установлением соответствия между абонентом и присвоенными ему/ей адресами; и 2) предотвращение имитации адреса на основе этой управляемой информации. Примеры указанных выше механизмов и их координации представлены в Дополнении I.

8.4.3 Идентификация абонента с помощью ассоциации безопасности TLS/IPsec

Если для передачи трафика сигнализации между вызывающим устройством и аутентификатором было установлено безопасное транспортное соединение TLS и данное транспортное соединение было аутентифицировано с помощью сертификата TE-BE X.509 (см. пункт 8.3.2), то аутентификатор проверяет, чтобы заголовок "From" соответствовал разрешенным значениям для абонента, определенным в поле <Subscriber Account Identifier>.

Если для передачи трафика сигнализации между вызывающим устройством и аутентификатором было установлено безопасное транспортное соединение (IPsec или TLS) и данное транспортное соединение было аутентифицировано с помощью сертификата устройства X.509, предназначенного для оконечного устройства СПП (см. пункты 8.3.1 и 8.3.2), то аутентификатор использует название производителя устройства и серийный номер устройства для определения соответствующего поля <Subscriber Account Identifier> (применимо только если устройство поставлено в соответствие абоненту). Поле <Subscriber Account Identifier> используется для получения полномочий абонента, и эти полномочия проверяются на соответствие значению в заголовке "From".

Если для передачи трафика сигнализации между вызывающим устройством и аутентификатором было установлено безопасное транспортное соединение (или IPsec, или TLS) и данное транспортное соединение было аутентифицировано с помощью сертификата абонента СПП X.509 (см. пункты 8.3.1 и 8.3.2), то аутентификатор использует поле <Subscriber Account Identifier> для получения полномочий абонента через функциональные объекты SAA/TAA. Далее аутентификатор проверяет полномочия абонента на соответствие значению в заголовке "From".

Если для передачи трафика сигнализации между вызывающим устройством и аутентификатором было установлено безопасное транспортное соединение (или IPsec, или TLS) и данное транспортное соединение было аутентифицировано с помощью предварительно разделенного ключа (см. пункт 9.2.4.3.1), то аутентификатор использует название ключа для получения полномочий абонента через функциональные объекты SAA/TAA. Далее аутентификатор проверяет полномочия абонента на соответствие значению в заголовке "From".

Если между вызывающим устройством и аутентификатором не использовалось безопасное транспортное соединение или использовалось соединение TLS типа "анонимный клиент", то данный метод будет "не установлен".

8.4.4 Идентификация абонента с помощью вызова/ответа

Механизм вызов/ответ является более безопасной версией устаревшей схемы идентификатор пользователя/пароль (т. е. отправка идентификатора пользователя и пароля в рамках запроса о предоставлении услуги и наличие проблемы, заключавшейся в том, что эту информацию было легко воспроизвести для получения в дальнейшем услуги мошенническим образом). В схеме вызов/ответ сервер направляет клиенту вызов, в котором содержится просьба о том, чтобы клиент выполнил некоторую операцию по шифрованию с использованием разделенного ключа. Результат данного вычисления включается в ответ, который затем проверяется сервером. Если данные обмена будут перехвачены другими лицами, то эти данные будет нельзя воспроизвести, поскольку сервер никогда не использует старый вызов повторно.

Существует один важный вид методов "вызов-ответ", который сочетает в себе удобство аутентификации, основанной на использовании пароля, и безопасности метода, который основан на схеме "вызов-ответ". Данный вид представлен протоколом обмена ключами, аутентифицированными с помощью пароля (PAK). Протокол PAK обеспечивает взаимную аутентификацию обеих сторон при создании симметричного криптографического ключа путем обмена по алгоритму Диффи-Хеллмана. Использование обмена по алгоритму Диффи-Хеллмана обеспечивает *совершенную прямую секретность* – свойство протокола по созданию ключей, которое гарантирует, что раскрытие сеансового ключа или долговременного закрытого ключа после заданного сеанса не приведет к раскрытию какого либо более раннего сеанса. Кроме того, при аутентификации методом PAK обеспечивается защита обмена от атак типа "незаконный посредник". При аутентификации создается ответ на предварительно разделенный секрет, который защищен от прослушивания и офлайновых словарных атак (т. е. остается нераскрытым). Таким образом, этот протокол может использоваться для широкого диапазона приложений, где существуют предварительно распределенные секреты, базирующиеся на, возможно, ненадежном пароле. Протокол PAK указан в [ITU-T X.1035] и [b-TIA 683-D].

Метод вызов/ответ предусматривает обмен дополнительными сообщениями между аутентификатором и вызывающим оконечным пунктом. В связи с этим он может влиять на задержку, воспринимаемую пользователем. Задача обеспечения безопасности в СПП заключается в использовании метода запрос/ответ только там, где это совершенно необходимо для достижения требуемого уровня идентификации и аутентификации.

Если для передачи трафика сигнализации между вызывающим устройством и аутентификатором было установлено безопасное транспортное соединение (или IPsec, или TLS) и предыдущий запрос в пределах настраиваемого временного интервала с тем же самым содержимым заголовка "From" был успешно аутентифицирован аутентификатором, то аутентификация считается успешной и запрос принимается. В связи с тем, что в случае сигнализации для установления связи, типовым первоочередным запросом о новом соединении является запрос "Register" (регистрация), то данный вызов/ответ будет осуществляться в течение времени, которое не влияет на задержку при установлении связи.

Поскольку для обработки запросов об аутентификации требуется большой объем вычислений, важно, чтобы аутентификатор ограничивал частоту запросов, поступающих на функциональные объекты SAA/TAA. Ограничения, определенные в настоящем пункте, могут соблюдаться независимо от того являются ли функциональные объекты SAA/TAA составной частью аутентификатора или отдельным элементом. Простая атака типа отказа в обслуживании заключается в том, что оконечный пункт просто перегружает аутентификатор неверными запросами: если для каждого запроса требуется производить криптографические вычисления в SAA/TAA-FE, то произойдет фактическое прекращение обслуживания всех запросов – и правильных, и неправильных. Для противодействия таким атакам аутентификатор может на месте отклонить запрос, если в ожидании авторизации находится запрос от того же самого оконечного пункта. Несколько более сложный вариант данного метода заключается в том, чтобы аутентификатор на месте отклонял запросы, если в общей сложности не менее XXX запросов поступило в течение YYY секунд (значения XXX и YYY должны настраиваться в аутентификаторе). Кроме того, аутентификатор может специально подождать в течение настраиваемого периода времени, прежде чем отвечать на запрос, не прошедший авторизацию. Данный способ также предотвращает различные виды атак с раскрытием пароля.

8.4.4.1 Метод вызов/ответ при использовании в вызывающем устройстве протокола сигнализации SIP

Если в вызывающем устройстве используется протокол сигнализации SIP, то для реализации вызова/ответа может использоваться по выбору механизм аутентификации посредника, определенный в [b-IETF RFC 3261]. См. пункт 22.2 [b-IETF RFC 3261], пункт 3 [b-IETF RFC 2617] и пункт 3 [b-IETF RFC 3310].

На запрос SIP аутентификатор дает ответ 407 (требуется аутентификация посредника). В этот ответ аутентификатор включает заголовок Proxy-Authenticate со следующими параметрами: схема аутентификации – "Digest", Realm – "NGN .ngn.net", qop – "auth", параметр "Nonce" – криптографическое случайное 16-октетное значение (шестнадцатеричное), факультативное значение параметра "Opaque", и алгоритм шифрования – "MD5" или "AKAv1-MD5", в зависимости от соглашения об обслуживании с абонентом.

Пример заголовка Proxy-Authenticate в ответе 407:

```
Proxy-Authenticate: Digest realm="NGN .ngn.com", qop="auth",
nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", stale=FALSE, algorithm=MD5
```

Вызывающее устройство в ответ на 407 генерирует запрос, содержащий заголовок Proxy-Authentication. Данный заголовок проверяется на предмет содержания следующей информации: схема аутентификации – "Digest", параметр "Realm" идентичен параметру, содержащемуся в ответе 407, параметр "Nonce" идентичен параметру, содержащемуся в ответе 407, и параметр "Opaque" идентичен параметру в ответе 407. Кроме того, заголовок Proxy-Authentication содержит параметр "Username", в котором содержится название ключа, параметр "Uri", совпадающий с параметром "Request-URI" в запросе, и параметр "Response", являющийся хеш-значением, указанным в [b-IETF RFC 2617] или [b-IETF RFC 3310].

Пример заголовка Proxy-Authorization в повторно направляемом запросе:

```
Proxy-Authorization: Digest username="bob", realm="NGN .ngn.com",
nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", uri="sip:5551212@ngn.com",
response="dfe56131d1958046689d83306477ecc"
```

Для реализации схемы вызов/ответ могут также использоваться механизмы "межпользовательской аутентификации", определенные в [b-IETF RFC 3261]. Более подробную информацию можно найти в пункте 22.2 [b-IETF RFC 3261], пункте 3 [b-IETF RFC 2617] и пункте 3 [b-IETF RFC 3310].

Если запрос разветвляется, то различные элементы сети СПП (например, MGC-FE) и/или оконечное оборудование могут пожелать направить вызов вызывающему устройству. Разветвляющий элемент сети (например, S-CSC-FE) объединяет эти вызовы и помещает их в единый ответ, который данный элемент направляет вызывающему устройству. При приеме ответа, который содержит много вызовов, вызывающее устройство предоставляет в запросе много полномочий и повторно представляет его.

8.4.4.2 Метод вызов/ответ при использовании в вызывающем устройстве протокола сигнализации, отличного от SIP

Если ожидается, что вызывающее устройство должно использовать SIP, однако оно выдает свой запрос с использованием протокола сигнализации, отличного от протокола SIP, то вызов/ответ считается неудачным, и запрос отклоняется.

8.4.5 Общая архитектура начальной загрузки

В общей архитектуре начальной загрузки (GBA) указывается процедура начальной загрузки, независимая от метода доступа. В этой процедуре обеспечивается основа для взаимной аутентификации конечных пользователей и функцией сетевого приложения (NAF), которая может использоваться для идентификации и аутентификации абонентов в СПП. Для получения информации о GBA см. [b-ETSI TS 133 220].

8.5 Идентификация и аутентификация конечных пользователей

8.5.1 Общая стратегия

Наряду с безусловным требованием об идентификации абонента, предъявляемым инфраструктурой СПП, идентификация конечного пользователя является услугой по выбору, которую может запрашивать абонент или этого требует услуга. Как правило, это осуществляется с целью предоставления дополнительных услуг, например персональных мобильности и присутствия, когда для обеспечения возможности подключения услуги требуется проверить идентичность запрашивающего пользователя. Если абонент желает применять данный дополнительный уровень идентификации, необходимо, чтобы все устройства на оконечных пунктах поддерживали возможность ввода дополнительных полномочий конечного пользователя или использования сертификата конечного пользователя вместо сертификата абонента.

Существуют два метода, позволяющие аутентификатору осуществлять идентификацию и аутентификацию конечного пользователя. Первый метод реализуется через ассоциацию безопасности на транспортном уровне, используемую для обмена сигнализацией. Если данная ассоциация безопасности была установлена с использованием сертификата конечного пользователя (или предварительно разделенного ключа, соответствующего единственному конечному пользователю), то идентификация конечного пользователя завершается. Второй метод осуществляется по схеме вызов/ответ, при которой название ключа, данное в ответе, ставится в соответствие с конечным пользователем. Эти два метода описаны в нижеследующих пунктах.

Усовершенствованные устройства СПП могут иметь много идентичностей, например сертификат абонента, а также один или несколько сертификатов конечных пользователей для лица (лиц), которое(ые) в настоящее время использует(ют) это устройство. Такое устройство будет создавать много соединений TLS с аутентификатором – по одному отдельному соединению на каждый сертификат. Далее это устройство будет направлять запросы аутентификатору по соответствующему соединению сигнализации, основанному на желаемой идентичности связи.

Имеется обеспокоенность в отношении того, что полномочия для одиночного пользователя продолжают действовать долгое время после того, как лицо перестало являться пользователем. Если ассоциация безопасности транспортировки была основана на сертификате конечного пользователя, то может потребоваться, чтобы абонент осуществлял непрерывную деятельность по поддержанию срока действия аутентификации. Если такая деятельность не осуществляется, аутентификатор закрывает безопасное транспортное соединение и требует, чтобы вызывающее устройство повторно установило соединение с использованием действующего сертификата конечного пользователя (либо сертификата абонента, либо сертификата устройства, если не имеется ни одного сертификата конечного пользователя). Подробные требования к характеристикам аутентификатора приведены в пунктах 9.1.2 и 9.2.4.3.1, и они основаны на двух таймерах: один таймер, который ограничивает абсолютное количество времени, в течение которого могут действовать полномочия конечного пользователя для ассоциации безопасности, и второй таймер, который ограничивает перерыв между двумя последовательными запросами. Значения перерывов могут предоставляться в расчете на абонента или конечного пользователя, однако они должны ограничиваться максимальными значениями, устанавливаемыми поставщиком услуг СПП.

8.5.2 Идентификация конечного пользователя с помощью ассоциации безопасности TLS/IPsec

Если для передачи трафика сигнализации между вызывающим устройством и аутентификатором было установлено безопасное транспортное соединение TLS и данное транспортное соединение было аутентифицировано с помощью сертификата TE-BE X.509 (см. пункт 8.6), то аутентификатор проверяет, чтобы заголовок "From" соответствовал разрешенным значениям для абонента, определенным в поле <Subscriber Account Identifier> , которое содержится в этом сертификате.

Если для передачи трафика сигнализации между вызывающим устройством и аутентификатором было установлено безопасное транспортное соединение (или IPsec, или TLS) и данное транспортное соединение было аутентифицировано с помощью сертификата конечного пользователя X.509, предназначенного для оконечного устройства СПП (см. пункт 8.6), то аутентификатор использует поле <Subscriber Account Identifier> для получения полномочий абонента через функциональные объекты SAA/TAA. Далее аутентификатор проверяет полномочия абонента на соответствие значению в заголовке "From". Если для передачи трафика сигнализации между вызывающим устройством и аутентификатором было установлено безопасное транспортное соединение (пункт 8.4.4) и данное транспортное соединение было аутентифицировано с помощью предварительно разделенного ключа (см. пункт ,(9.2.4.3.1то аутентификатор использует название ключа для получения полномочий абонента через функциональные объекты SAA/TAA. Далее аутентификатор проверяет полномочия абонента на соответствие значению в заголовке "From".

8.5.3 Идентификация конечного пользователя методом вызова/ответа

Процедуры идентификации методом вызова/ответа для идентификации конечного пользователя является такими же, как и процедуры, используемые для идентификации абонента, которые указаны в пункте 8.4.4.

Единственное расширение заключается в том, что аутентификатор проверяет информацию относительно названия ключа, извлекаемую через функциональные элементы SAA/TAA, на предмет указания на то, что ключ соответствует конечному пользователю. Если это так, то идентификация конечного пользователя является успешной.

Если аутентификатор уже выполнил процедуру вызов/ответ для идентификации абонента и полученное в ответном сообщении название ключа не идентифицирует конечного пользователя, то в этом случае идентификация конечного пользователя является неуспешной. Если процедура вызова/ответа не требовалась для идентификации абонента, то теперь вызов направляется.

8.6 Идентификация и аутентификация с помощью пограничного элемента оконечного оборудования

Процедуры идентификации и аутентификации, выполняемые TE-BE, идентичны процедурам, выполняемым аутентификатором, при этом имеются два отличия:

1) TE-BE может обеспечиваться всеми полномочиями, необходимыми для идентификации и аутентификации абонента(ов) и конечных пользователей, которым он служит, поскольку у него нет доступа к распределенной функции, обеспечиваемой функциональными элементами SAA/TAA, которая была бы доступна аутентификатору.

2) При повторном направлении запроса в ответ на вызов от аутентификатора, содержащего заголовок "Proxy-Authorization", этот запрос передается аутентификатору, а не обрабатывается в TE-BE.

8.6.1 Использование сертификатов X.509

Между каждым элементом TE-BE и по меньшей мере одним из элементов NBE существует ассоциация безопасности, установленная вместе с выданным TE-BE сертификатом X.509. Запросы, полученные на NBE, сопровождаются процедурами идентификации и аутентификации, указанными в пункте Э .8.4.3то сводит к минимуму проверку идентичности, осуществляемую TE-BE. В случае если необходим вызов/ответ (например, для пользователя роуминга), обмен будет осуществляться между вызывающим оконечным пунктом и элементом NBE, и данные будут прозрачно предаваться через элемент TE-BE.

Безопасное транспортное соединение между оконечным пунктом и TE-BE является факультативным. Предполагается, что сетевой адрес источника позволит адекватно идентифицировать большинство запросов.

Оконечные пункты регистрируются на NBE через TE-BE.

8.7 Интерфейс между аутентификатором и функциональными объектами SAA/TAA

8.7.1 Использование протокола RADIUS и его расширений

Функциональные объекты SAA/TAA содержат точку принятия решения, а функциональные объекты SUP/TUP являются хранилищами для всех полномочий конечных пользователей и устройств в инфраструктуре СПП. Ряд функций SAA/TAA-FE, таких как аутентификация, может быть распределен, чтобы оптимизировать качественные характеристики запросов аутентификации.

Для связи между аутентификатором и функциональными объектами SAA/TAA в качестве протокола обычно используются два конкурирующих варианта: RADIUS [b-IETF RFC 2865] (широко известный и пользующийся большой поддержкой) и Diameter [b-IETF RFC 3588] (определенный для устранения ряда недостатков, присущих протоколу RADIUS). Окончательной целью для инфраструктуры СПП является переход к протоколу Diameter; однако признается, что существующие реализации серверов базируются на протоколе RADIUS и что были разработаны многочисленные специальные расширения базового протокола RADIUS, призванные удовлетворить требования этой функции аутентификации. Несмотря на то что данная версия Рекомендации основана на протоколе RADIUS совместно с расширением, описанным в [b-IETF RFC 5090], в будущей версии этой Рекомендации данный интерфейс будет вероятно изменен на интерфейс на базе протокола Diameter совместно с расширением, описанным в [b-IETF RFC 4740].

Аутентификатор становится клиентом RADIUS, а сервер функциональных элементов SAA/TAA становится сервером RADIUS, определенным в [b-IETF RFC 2865]. И клиент, и сервер, могут реализовывать расширения для аутентификации SIP Digest, как указано в [b-IETF RFC 5090]. Связь между аутентификатором и сервером функциональных элементов SAA/TAA может быть защищена путем взаимной аутентификации с использованием протокола IPsec.

Используя расширения [b-IETF RFC 4590], аутентификатор делает запрос RADIUS с параметрами из заголовка Proxy-Authentication; сервер RADIUS вычисляет ожидаемый ответ и направляет его обратно аутентификатору. Далее аутентификатор проверяет запрос путем сравнения фактического ответа от оконечного пункта с ожидаемым ответом.

Пример сообщения, направляемого аутентификатором серверу функционального элемента SAA/TAA, является следующим:

```
Code = 1 (Access-Request)
      Identifier = 1
      Length = 164
      Authenticator = 56 7b e6 9a 8e 43 cf b6 fb a6 c0 f0 9a 92 6f 0e
      Attributes:
      NAS-IP-Address = d5 89 45 26 (213.137.69.38)
      NAS-Port-Type = 5 (Virtual)
      User-Name = "bob"
      Digest-Response (206) = "2ae133421cda65d67dc50d13ba0eb9bc"
      Digest-Attributes (207) = [Realm (1) = "NGN .ngn.com"]
      Digest-Attributes (207) = [Nonce (2) = " ea9c8e88df84f1cec4341ae6cbe5a359
"]
      Digest-Attributes (207) = [Method (3) = "INVITE"]
      Digest-Attributes (207) = [URI (4) = " sip:5551212@ngn.com "]
      Digest-Attributes (207) = [Algorithm (5) = "md5"]
      Digest-Attributes (207) = [User-Name (10) = "bob"]
An example of the response sent from the SAA/TAA-FEs server to the Authenticator
is:
Code = 2 (Access-Accept)
      Identifier = 1
      Length = 20
      Authenticator = 6d 76 53 ce aa 07 9a f7 ac b4 b0 e2 96 2f c4 0d
      Attributes:
      Digest-Response (206) = "dfe56131d1958046689d83306477ecc"
```

8.7.2 Ассоциация безопасности транспортировки для сигнализации

При использовании сертификата X.509 для установления ассоциации безопасности транспортировки для сигнализации, функциональные объекты SUP/TUP хранят (индексированный по полю <Subscriber Account Identifier>) набор применимых заголовков "From", которые могут встретиться в запросах от этого источника. Этот набор будет сравниваться с заголовком "From", содержащимся в этом запросе.

Если предварительно совместно используемый ключ используется для установления ассоциации безопасности для транспортной сигнализации (например, одноранговым поставщиком услуги), то функциональные объекты SUP/TUP хранят набор применимых заголовков "From" (индексированный по названию ключа), которые могут встретиться в запросах от этого источника. Этот набор будет сравниваться с заголовком "From", содержащимся в запросе.

8.8 Идентификация и аутентификация трафика канала передачи

Бывают ситуации, когда желательно идентифицировать трафик отдельного канала передачи в целях совершенствования безопасности. Например, чтобы противодействовать мошенническим атакам, таким как спуфинг или внедрение ложных пакетов RTP. В СПП трафик канала передачи может быть идентифицирован с использованием пяти элементов, в число которых входят:

- IP-адрес источника;
- IP-адрес получателя;
- порт источника;
- порт получателя; и
- номер протокола.

Механизм идентификации, описанный в данном пункте, использует этот идентификатор для аутентификации каждого пакета. Этот механизм основан на разделенном секрете и использовании криптографической хеш-функции – хешированного кода аутентификации сообщения (HMAC) с ключом. Более подробная информация представлена в [b-NIST FIPS 198-1].

К объектам, участвующим в процессе аутентификации, относятся функция конечного пользователя и функциональный объект узла доступа, которые описаны в [ITU-T Y.2701] и изображены на рисунке 3 с использованием в качестве примера интерфейса UNI.

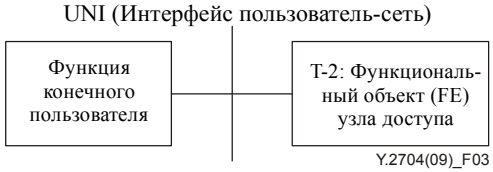


Рисунок 3 – Объекты СПП, участвующие в процедуре аутентификации – пример с интерфейсом UNI

При описании этого механизма используются следующие соглашения о терминах:

- *F* – идентификатор (из пяти элементов) трафика канала передачи;
- *K* – разделенный секрет, которым владеют как функция конечного пользователя, так и функциональный объект узла доступа;
- *P* – пакет, который функция конечного пользователя намеревается направить функциональному объекту узла доступа;
- *i* – порядковый номер пакета, который увеличивается на обеих сторонах, осуществляющих связь, и являющийся 64-битной величиной;
- *t* – отметка времени, являющаяся 64-битной величиной, которая указывает время в секундах. В качестве варианта может представлять собой случайную величину "nonce";
- (*P′*, *Q*) – пакет, который получил функциональный объект узла доступа.

Когда функция конечного пользователя намеревается направить пакет *P* функциональному объекту узла доступа, то она сначала вычисляет величину *H(F, t+i, K)*, являющуюся значением хеш-функции от конкатенации *F*, *t+i* и *K*, а затем добавляет эту величину к пакету *P*. Таким образом, полный пакет, направляемый функцией конечного пользователя функциональному объекту узла доступа, равен *[P, H(F, t+i, K)]*. Когда функциональный объект узла доступа принимает пакет *(P′, Q)*, он вычисляет величину *H(F, t+i, K)*. Если используется метка времени, то функциональный объект узла доступа вычисляет хеши для всех значений времени *t* , находящихся в согласованном интервале для разницы между временами функции конечного пользователя и функционального объекта узла доступа (эту процедуру необходимо выполнить только один раз в начале сеанса). В этом случае функциональный объект узла доступа ищет соответствие между значением *Q* и любым из вычисленных значений хешей. Если соответствие найдено, то этот пакет аутентифицируется. Соответствующее значение времени *t* будет использоваться для пакетов в потоке.

Если используется случайная величина "nonce", то функциональный объект узла доступа просто проверяет равенство вычисленного значения хеша *Q*. Если имеется равенство, пакет аутентифицируется.

В условиях, когда может произойти потеря пакета, простого увеличения значения *i* от пакета к пакету не достаточно. В этом случае функциональный объект узла доступа может осуществить поиск в интервале от *i* до *i+d* (где *d* – какое-либо малое число) для повторной синхронизации *i*.

Использование данного механизма аутентификации способствует противодействию мошенническим атакам, например спуфингу или внедрению ложных пакетов RTP.

Для реализации данного механизма предлагается, чтобы функция конечного пользователя и функциональный объект узла доступа согласовали формат идентификатора *F*, разделенный секрет *K*, хеш-функцию *H*, точное синхронизированное время для начала отметки времени *t*, место и способ добавления хешированной величины к пакету *P*, значение *d*, а также условия, при которых начинается повторная синхронизация *i*.

Использование данного механизма является предметом политики безопасности операторов сети. Существуют другие механизмы, которые могут использоваться для аутентификации потоков, например протокол IPsec. Преимущество данного механизма по сравнению с протоколом IPsec состоит в тот, что в то время как для IPsec требуется шифрование всего пакета IP (в туннельном режиме) или информационного содержания (в транспортном режиме), данный механизм требует вычисления лишь хеша *H(F, t+i, K)*, что может быть сделано быстрее и с использованием меньших вычислительных ресурсах.

9 Безопасность транспортировки для сигнализации и OAMP

Безопасность на транспортном уровне используется в инфраструктуре СПП для гарантии конфиденциальности и целостности данных сигнализации и сообщений OAMP. В данном пункте определяется профиль протокола TLS и IPsec, используемого элементами сети инфраструктуры СПП, в качестве двух важных механизмов безопасности. Перечни механизмов не являются исчерпывающими, и могут приниматься другие реализации, в зависимости от политики поставщика услуг СПП.

В пределах "доверенной" зоны и "доверенной, но уязвимой" зоны, для обеспечения защиты сообщений OAMP требуется туннель VPN, например IPsec или TLS. В пункте 9.1 приводится профиль для случаев использования TLS, а в пункте 9.2 приводится профиль для случаев использования протокола IPsec. IPsec используется между TE-BE и OAMP-NBE, т. е. между недоверенной зоной и доверенной, но уязвимой зоной, для создания туннеля VPN. В пункте 9.3 приводится применяемый профиль IPsec.

Несмотря на то что внутри СПП обеспечение безопасности среды передачи не требуется, на некоторых пограничных элементах для услуг, предоставляемых в конкретных оконечных пунктах, реализуются протоколы безопасности среды передачи. Для этих элементов в пункте 10 приводится профиль протоколов безопасности среды передачи.

9.1 Протокол TLS

В инфраструктуре СПП протокол TLS часто используется для защиты различных типов трафика сигнализации, например SIP, COPS, TRIP, HTTP, между элементами сети в пределах доверенной зоны. Этот протокол также поддерживается пограничными элементами, которые могут получать зашифрованные сообщения сигнализации от оконечных пунктов абонентов, и элементами TE-BE для связи с NBE. Конкретные требования для каждого типа элемента сети представлены в [ITU-T Y.2701].

Протокол TLS определен в [b-IETF RFC 5246]. Этот протокол обеспечивает конфиденциальность и целостность данных и используется поверх надежного протокола транспортного уровня, например TCP или SCTP.

Если иное не указано в настоящем пункте, желательно чтобы элементы сети инфраструктуры СПП, для которых требуется TLS, соответствовали спецификации TLS [b-IETF RFC 5246] и любым требованиям, указанным в [b-IETF RFC 3261], которые относятся к его использованию в SIP. Несмотря на то что в TLS поддерживается возможность согласования, а также используются методы сжатия, в рамках инфраструктуры СПП сжатие не может использоваться в связи с ухудшением качественных характеристик.

9.1.1 Наборы параметров шифрования

Набор параметров шифрования включает используемый при установлении соединения TLS метод соглашения об аутентифицированном ключе, а также шифры для шифрования и аутентификации, используемые для защиты уровня записи. Наборы параметров шифрования согласовываются с клиентом TLS путем представления перечня поддерживаемых наборов шифрования в сообщении Client Hello, в ответ сервер указывает выбранный набор шифрования в сообщении Server Hello.

На выбор параметров шифрования влияют многие факторы. Далее приведены примеры общих факторов, определяющих выбор алгоритма шифрования:

1) Требуемая безопасность
   - Ценность данных (для организации и/или для других объектов – чем выше ценность информации, тем более криптостойкое шифрование требуется).
   - Временная ценность данных (если данные являются ценными, но в течение лишь короткого периода времени (например, в течение несколько дней в противоположность нескольким годам), может использоваться менее криптостойкий алгоритм шифрования).
   - Угроза данным (чем выше уровень угрозы, тем более криптостойкое шифрование требуется).
   - Другие меры, которые уже применяются и могут обусловливать применение менее криптостойкого шифрования, например использование методов защищенной связи, таких как работа по выделенным линиям, а не в общедоступном интернете.
2) Требуемая производительность (более жесткие требования к производительности могут потребовать приобретения дополнительных системных ресурсов, таких как аппаратный криптографический усилитель, или применения менее криптостойкого шифрования).

3) Системные ресурсы (меньший объем ресурсов, например обработка, память, может обусловливать применение менее криптостойкого шифрования).

4) Импорт, экспорт или ограничения использования.

5) Схемы шифрования, поддерживаемые сетевыми элементами.

6) Схемы шифрования, поддерживаемые устройствами пользователя.

В таблице 3 представлен перечень возможных наборов параметров шифрования, пригодных для использования в СПП, однако данный перечень не является исчерпывающим.

Таблица 3 – Наборы параметров шифрования, пригодные для СПП

Название набора шифрования	Справочный документ	Обмен ключами	Шифр	Хеш-функция
TLS_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	RSA	AES-128 в режиме CBC	SHA-1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	Режим временного ключа Диффи-Хеллмана с подписями RSA	AES-128 в режиме CBC	SHA-1
TLS_RSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 2246]	RSA	3DES в режиме CBC	SHA-1
TLS_DHE_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 5246]	Режим временного ключа Диффи-Хеллмана с подписями RSA	3DES в режиме CBC	SHA-1
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	RSA	Camellia-128 в режиме CBC	SHA-1
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	Режим временного ключа Диффи-Хеллмана с подписями RSA	Camellia-128 в режиме CBC	SHA-1

Наборы параметров шифрования, приведенные в таблице, которые описаны в [b-IETF RFC 5246], [b-IETF RFC 4132] и [b-IETF RFC 4492], также могут использоваться любым NE по выбору.

Таблица 4 – Наборы параметров шифрования (по выбору), пригодные для СПП

Название набора шифрования	Справочный документ	Обмен ключами	Шифр	Хеш-функция
TLS_DH_DSS_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	Алгоритм Диффи-Хеллмана с подписью DSS	AES-128 в режиме CBC	SHA-1
TLS_DH_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	Алгоритм Диффи-Хеллмана с подписью RSA	AES-128 в режиме CBC	SHA-1
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	Режим временного ключа Диффи-Хеллмана с подписями DSS	AES-128 в режиме CBC	SHA-1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	Режим временного ключа Диффи-Хеллмана с подписями RSA	AES-128 в режиме CBC	SHA-1

Таблица 4 – Наборы параметров шифрования (по выбору), пригодные для СПП

Название набора шифрования	Справочный документ	Обмен ключами	Шифр	Хеш-функция
TLS_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	RSA	AES-256 в режиме CBC	SHA-1
TLS_DH_DSS_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	Алгоритм Диффи-Хеллмана с подписью DSS	AES-256 в режиме CBC	SHA-1
TLS_DH_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	Алгоритм Диффи-Хеллмана с подписью RSA	AES-256 в режиме CBC	SHA-1
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	Режим временного ключа Диффи-Хеллмана с подписями DSS	AES-256 в режиме CBC	SHA-1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4132]	Режим временного ключа Диффи-Хеллмана с подписями RSA	AES-256 в режиме CBC	SHA-1
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	Алгоритм Диффи-Хеллмана с подписью DSS	Camellia-128 в режиме CBC	SHA-1
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	Алгоритм Диффи-Хеллмана с подписью RSA	Camellia-128 в режиме CBC	SHA-1
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	Режим временного ключа Диффи-Хеллмана с подписями DSS	Camellia-128 в режиме CBC	SHA-1
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	RSA	Camellia-256 в режиме CBC	SHA-1
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	Алгоритм Диффи-Хеллмана с подписью DSS	Camellia-256 в режиме CBC	SHA-1
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	Алгоритм Диффи-Хеллмана с подписью RSA	Camellia-256 в режиме CBC	SHA-1
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	Режим временного ключа Диффи-Хеллмана с подписями DSS	Camellia-256 в режиме CBC	SHA-1
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	Режим временного ключа Диффи-Хеллмана с подписями RSA	Camellia-256 в режиме CBC	SHA-1
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	Алгоритм Диффи-Хеллмана на эллиптических кривых с подписью ECDSA	3DES в режиме CBC	SHA-1

Таблица 4 – Наборы параметров шифрования (по выбору), пригодные для СПП

Название набора шифрования	Справочный документ	Обмен ключами	Шифр	Хеш-функция
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	Алгоритм Диффи-Хеллмана на эллиптических кривых с подписью ECDSA	AES-128 в режиме CBC	SHA-1
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	Алгоритм Диффи-Хеллмана на эллиптических кривых с подписью ECDSA	AES-256 в режиме CBC	SHA-1
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	Режим временного ключа Диффи-Хеллмана на эллиптических кривых с подписью ECDSA	3DES в режиме CBC	SHA-1
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	Режим временного ключа Диффи-Хеллмана на эллиптических кривых с подписью ECDSA	AES-128 в режиме CBC	SHA-1
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	Режим временного ключа Диффи-Хеллмана на эллиптических кривых с подписью ECDSA	AES-256 в режиме CBC	SHA-1
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	Алгоритм Диффи-Хеллмана на эллиптических кривых с подписью RSA	3DES в режиме CBC	SHA-1
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	Алгоритм Диффи-Хеллмана на эллиптических кривых с подписью RSA	AES-128 в режиме CBC	SHA-1
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	Алгоритм Диффи-Хеллмана на эллиптических кривых с подписью RSA	AES-256 в режиме CBC	SHA-1
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	Режим временного ключа Диффи-Хеллмана на эллиптических кривых с подписью RSA	3DES в режиме CBC	SHA-1
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	Режим временного ключа Диффи-Хеллмана на эллиптических кривых с подписью RSA	AES-128 в режиме CBC	SHA-1

Таблица 4 – Наборы параметров шифрования (по выбору), пригодные для СПП

Название набора шифрования	Справочный документ	Обмен ключами	Шифр	Хеш-функция
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	Режим временного ключа Диффи-Хеллмана на эллиптических кривых с подписью RSA	AES-256 в режиме CBC	SHA-1

ПРИМЕЧАНИЕ 1. – Общепринятым и широко используемым шифром является RC-4. Тем не менее он не включен в вышеприведенный перечень, поскольку он не является открытым стандартом.

ПРИМЕЧАНИЕ 2. – Криптография на основе эллиптических кривых (ECC) – это криптографическая система с открытым ключом, использование которой может быть целесообразным для определенных приложений в СПП. В частности, ECC будет требоваться для определенных приложений в силу ее преимуществ в аспекте эффективности. По сравнению с другими распространенными криптосистемами, такими как RSA, ECC обеспечивает тот же уровень безопасности при существенно меньших размерах ключей. Кроме того, ECC характеризуется вычислительной эффективностью и преимуществами по сравнению с некоторыми иными методами, использующими открытые ключи, которые обеспечивают тот же уровень защиты.

9.1.2 Использование TLS для сертификатов

TLS – это протокол типа "клиент-сервер" с факультативной функцией аутентификации клиента. Вместе с тем в пределах доверенной зоны инфраструктуры СПП или между доверенной зоной и доверенной, но уязвимой зоной может выполняться взаимная аутентификация с использование TLS. В этом случае сервер TLS посылает клиенту запрос сертификата. Если клиент в доверенной зоне или в доверенной, но уязвимой зоне не предоставляет сертификат клиента, то сервер может отклонить запрос на установление соединения. Оба сертификата – клиента и сервера TLS – должны соответствовать спецификации сертификации инфраструктуры СПП, представленной в пункте 8.3. Проверка сертификатов может осуществляться согласно пункту 8.3. Прежде чем продолжить установление соединения TLS, сервер или клиент TLS могут проверить соответствие удаленной системы своему сертификату.

Между доверенной, но уязвимой зоной и недоверенной зоной сервер TLS может направлять клиенту запрос сертификата. Если клиент не имеет сертификата, он отвечает пустым сообщением "Сертификат клиента" и продолжает сеанс как анонимный клиент.

Если NBE принимает аутентифицированное соединение с оконечным пунктом на основании сертификата конечного пользователя СПП (см. пункт 8.5.2) NBE может реализовать для данного соединения два таймера. Первый таймер, T1, начинает работать при установлении соединения. Второй таймер, T2, начинает работать при установлении соединения и обнуляется каждый раз при получении на NBE запроса по этому соединению. При достижении таймерами своих предельных значений (которые могут зависеть от значений, содержащихся в сертификате) соединение сбрасывается элементом NBE и повторно устанавливается оконечным пунктом для обновления сертификата конечного пользователя СПП.

9.1.3 Управление сеансовыми ключами

Предполагается, что сеансы TLS, устанавливаемые между сетевыми элементами инфраструктуры СПП, будут продолжительными. Следовательно, важно периодически менять сеансовые ключи. Сеансовые ключи для сеансов TLS могут меняться по истечении задаваемого периода времени.

9.2 IPsec в доверенной и доверенной, но уязвимой зонах

IPsec инфраструктуры СПП может использоваться для защиты трафика разных типов (например, SNMP, RADIUS) между элементами сети в пределах доверенной зоны. Конкретные требования для каждого типа элемента сети представлены в [ITU-T Y.2701].

Как указано в общем описании [b-IETF RFC 4301], IPsec состоит из ряда разных компонентов. Они могут использоваться для обеспечения конфиденциальности, целостности и защиты от повторной передачи. Некоторые из них могут конфигурироваться вручную, но, как правило, используется компонент управления ключами. Кроме того, принятием решения об использовании IPsec обычно управляет база данных политики. В данном пункте описывается обязательный для реализации поднабор компонентов IPsec.

В сетевых элементах, которые используют IPsec, рекомендуется обеспечивать, чтобы соединения, защищенные TLS, не осуществлялись с применением IPsec.

ПРИМЕЧАНИЕ. – Элементы сети, которые используют IPsec, должны обеспечивать, чтобы потоки медиаданных, защищенные с помощью SRTP или RC4, не передавались с использованием IPsec. Это делается во избежание двойного шифрования, которое непроизводительно использовало бы ресурсы СПП. Следует отметить, что туннелирование шифрования может происходить со стороны конечного пользователя.

9.2.1 Протоколы AH и ESP

Заголовок аутентификации (AH), описание которого содержится в [IETF RFC 4302] и [b-IETF RFC 4835], и протокол безопасного закрытия содержания (ESP), описание которого содержится в [IETF RFC 4303], являются двумя вариантами протоколов шифрования сетевого трафика. Оба факультативно обеспечивают защиту от повторной передачи. ESP обычно используется для обеспечения конфиденциальности, целостности и аутентификации трафика. ESP также может обеспечивать целостность и аутентификацию без конфиденциальности. Кроме того, ESP может использоваться только для обеспечения конфиденциальности. AH защищает участки предшествующего заголовка IP, включая адрес источника и адрес назначения. AH может также защищать те функции IP, которые необходимы промежуточным маршрутизаторам, но которые требуется доставить адресату неповрежденными и аутентичными, хотя такие функции IP используются крайне редко.

Элементы сети инфраструктуры СПП могут поддерживать протокол безопасного закрытия содержания (ESP), который описан в [IETF RFC 4303]. В режиме сцепления шифрованных блоков (CBC) могут поддерживаться ESP_DES (как длиной 40, так и 56 битов), ESP_3DES, ESP_AES [b-IETF RFC 3602] и ESP_CAMELLIA [b-IETF RFC 4312]. Элементы сети, которые поддерживают ESP_NULL, могут НЕ использовать ESP_NULL, если они осуществляют связь с другим сетевым элементом инфраструктуры СПП. Фактические алгоритм шифрования в ESP согласовывается в процессе управления ключами.

Все реализации ESP требуются в [b-IETF RFC 4301] для поддержки концепции ассоциации безопасности (SA), а в [b-IETF RFC 4301] представлена общая модель обработки трафика IP, относящегося к SA. Несмотря на то что для определенных реализаций IPsec не требуется соответствие всем параметрам этой общей модели, внешние режимы любой реализации IPsec могут соответствовать внешним режимам этой общей модели. Таким образом, обеспечивается то, что компоненты не будут принимать трафик, поступающий из неизвестных адресов и не будут передавать трафик без применения мер безопасности (когда требуется безопасность). Элементы сети инфраструктуры СПП, реализующие IPsec, могут обеспечивать режим, соответствующий общей модели, описанной в [b-IETF RFC 4301].

9.2.2 Режим транспортировки и туннелирования

Оба протокола – AH и ESP – могут использоваться либо в режиме транспортировки, либо в режиме туннелирования. В режиме туннелирования после заголовка IPsec следует внутренний заголовок IP. Это обычно используется для виртуальных частных сетей (VPN) и, как правило, требуется, если ни один из концов защищенного с помощью IPsec маршрута не является конечным пунктом назначения, например если IPsec реализуется в брандмауэре или в маршрутизаторе. Режим транспортировки более предпочтителен для связи типа пункт-пункт.

Элементы сети инфраструктуры СПП могут поддерживать IPsec в режиме транспортировки.

9.2.3 Защита от повторной передачи

Элементы сети инфраструктуры СПП могут использовать факультативную услугу защиты от повторной передачи (услугу антиповтора). В рамках элементов сети инфраструктуры СПП услуга антиповтора может быть включена в любое время. Порядковый номер IPsec, выходящий за пределы текущего окна антиповтора, помечается как повтор и пакет отклоняется. Если услуга антиповтора включена, порядковый номер IPsec не может выходить за пределы и обнуляется. До того как это произойдет, должна быть создана новая ассоциация безопасности согласно [IETF RFC 4303].

9.2.4 Управление ключами

Для всех криптографических систем необходимо управление ключами. Несмотря на то что IPsec обеспечивает ручные и автоматические схемы управления ключами, ручные схемы не обеспечивает масштабируемость, характерную для автоматических схем, и не предоставляют защиты от повторной передачи. Все схемы управления ключами обеспечивают аутентификацию. В элементах сети инфраструктуры СПП должен быть реализован один из описанных в данном пункте механизмов автоматического обмена ключами.

Если для управления ключами IKE не используется, альтернативному протоколу управления ключами необходим интерфейс с уровнем IPsec для создания/обновления/удаления ассоциации безопасности. Ассоциации безопасности IPsec могут автоматически устанавливаться и при необходимости повторно устанавливаться. Это означает, что для уровня IPsec также необходим способ для сообщения приложению управления ключами о том, когда необходимо установить новую ассоциацию безопасности (например, оканчивается срок прежней SA или в конкретном интерфейсе отсутствует SA). Кроме того, некоторые пограничные элементы могут требовать использования нескольких протоколов управления ключами (например, IKE для защищенных соединений для OAMP и PKINIT для защищенных соединений). В этих случаях рекомендуется использование интерфейса PF_KEY [b-IETF RFC 2367].

9.2.4.1 Идентификаторы преобразования

Идентификатор преобразования IPsec используется процедурами управления ключами для согласования алгоритма шифрования, который используется ESP в IPsec. Идентификатор преобразования используется также IKE для защиты своих сообщений этапа-1 и этапа-2. Перечень имеющихся идентификаторов преобразования IPsec приведен в [b-IETF RFC 5282]. В инфраструктуре СПП могут поддерживаться идентификаторы ESP_3DES (значение 0x03, размер ключа 192 битов, режим CBC) и ESP_CAMELLIA (значение 0x16, размер ключа 128 битов, режим CBC) [b-IETF RFC 4312]. Рекомендуется поддержка идентификатора ESP_AES (значение 0x0C, размер ключа 128 битов, режим CBC). IKE разрешает согласование размера ключа шифрования, поэтому если в будущем потребуется увеличить размер ключа для одного из указанных выше алгоритмов, IKE будет использовать эту встроенную функцию.

Для всех этих преобразований в информационном содержании каждого пакета ESP в незашифрованном виде переносится вектор инициализации CBC (IV) [b-IETF RFC 2451]. В режиме CBC может использоваться ключ AES-128, определенный в [b-NIST FIPS 197] и [b-IETF RFC 3602], с блоками размером 128 битов и произвольно генерируемым вектором инициализации. AES-128 требует выполнения 10 циклов криптографических операций [b-IETF RFC 3602]. В режиме CBC может использоваться ключ Camellia-128, определенный в [b-IETF RFC 3713 и [b-IETF RFC 4312], с блоками размером 128 битов и произвольно генерируемым вектором инициализации. Он требует выполнения 18 циклов криптографических операций [b-IETF RFC 3713].

9.2.4.2 Алгоритмы аутентификации

Алгоритм аутентификации IPsec используется процедурами управления ключами для согласования алгоритма аутентификации пакетов. Перечень доступных алгоритмов аутентификации IPsec представлен в [b-IETF RFC 5282]. В инфраструктуре СПП могут поддерживаться алгоритмы аутентификации HMAC-MD5-96 (значение 0x01, размер ключа 128 битов, определен в [b-IETF RFC 2403]) и HMAC-SHA-1-96 (значение 0x02, размер ключа 160 битов, определен в [b-IETF RFC 4835]).

9.2.4.3 Обмен ключами по интернету (IKE)

Один из механизмов автоматического обмена ключами описан в [b-IETF RFC 2409] и называется IKE. Управление ключами IKE является полностью асинхронными относительно сообщений и не вносит задержки в процессе установления связи. Единственное исключение составляет непредвиденная ошибка, когда один из оконечных пунктов неожиданно утрачивает ассоциацию безопасности.

IKE – это одноранговый протокол управления ключами. Он выполняется в два этапа. На первом этапе согласовывается разделенный секрет в процессе обмена ключами Диффи-Хеллмана. Далее этот секрет используется для аутентификации второго этапа IKE. На втором этапе согласовывается другой секрет, используемый в целях получения ключей для протокола ESP IPsec.

9.2.4.3.1 Первый этап IKE

Для аутентификации на первом этапе IKE определяются три разных режима. В инфраструктуре СПП НЕ ДОЛЖНА использоваться аутентификация IKE на основе шифрования с открытым ключом, поскольку для этого требуется, чтобы инициатор уже знал открытый ключ отвечающей стороны. Может поддерживаться аутентификация IKE с подписями и аутентификация IKE с предварительно разделенными ключами.

IKE определяет конкретные наборы параметров Диффи-Хеллмана (например, простое число и генератор), которые могут использоваться для первого этапа обмена IKE. В элементах сети инфраструктуры СПП может использоваться первая группа, и рекомендуется поддержка остальных групп.

Если используется аутентификация IKE с подписями, и клиент, и сервер могут обмениваться сертификатами X.509 (см. пункт 8.3.2). Проверка сертификатов может выполняться согласно пункту 8.3.

Если пограничный элемент сети принимает аутентифицированное соединение с оконечным пунктом на основании сертификата конечного пользователя СПП, NBE может реализовать для данного соединения два таймера. Первый таймер, T1, начинает работать при установлении соединения. Второй таймер, T2, начинает работать при установлении соединения и обнуляется каждый раз при получении на NBE запроса по этому соединению. При достижении таймерами своих предельных значений (которые могут зависеть от значений, содержащихся в сертификате), соединение сбрасывается элементом NBE и повторно устанавливается оконечным пунктом для обновления сертификата конечного пользователя СПП.

Если используется аутентификация IKE с предварительно разделенными ключами, то для аутентификации обмена используется ключ, полученный каким-либо способом по внешнему каналу (например, вручную). Реализации могут допускать предварительно разделенные ключи размером не менее 128 октетов. В сетевых элементах не требуется проверки требований для предварительно разделенных ключей. Реализации могут поддерживать агрессивный метод, определенный в пункте 5.4 [b-IETF RFC 2409], и использовать наименование ключа в качестве идентификационных данных инициатора/отвечающей стороны. Известно, что агрессивный режим IKE v1 [b-IETF RFC 2409] в сочетании ключом, который был заранее разделен, небезопасен. В этом режиме хеширование секрета передается по сети открытым способом; если атакующий перехватывает IP-трафик, то он может вскрыть ключ в режиме оф-лайн с применением метода решения "в лоб". Для предотвращения вычислений PSK с применением метода решения "в лоб" на основе данных его хеширования, рекомендуется использовать PSK с длиной не менее 128 бит.

При использовании предварительно разделенных ключей устойчивость системы зависит от устойчивости разделенного секрета. Целью является недопущение того, чтобы разделенный секрет стал слабым звеном в цепочке обеспечения безопасности. Это означает, что необходимо поддерживать энтропию (произвольность) разделенного секрета, соответствующую используемому шифру. Другими словами, рекомендуется, чтобы разделенный секрет содержал не менее 128–160 битов энтропии.

9.2.4.3.2 Второй этап IKE

На втором этапе IKE устанавливается ассоциация безопасности IPsec ESP, включая ключи и наборы параметров шифрования ESP. Сначала устанавливается разделенный секрет второго этапа, а затем из него выводится весь материал ключа, используя одностороннюю функцию, определенную в [b-IETF RFC 2409]. Секрет второго этапа строится на основании зашифрованных случайных величин

"nonce", которыми обмениваются обе стороны. Кроме использования зашифрованных величин "nonce" в [b-IETF RFC 2409] допускается другой алгоритм обмена Диффи-Хеллмана, но он не может использоваться в элементах сети инфраструктуры СПП. Это позволяет избежать связанного с его применением ухудшения производительности.

9.3 Протоколы соглашения о ключе между недоверенной и доверенной, но уязвимой зоной

Кроме того, по желанию можно использовать протокол соглашений о ключе (AKA), определенный для сетей IMS. Аутентификация универсальной системы подвижной связи (UMTS) и протокол соглашений о ключе (AKA) поддерживают взаимную аутентификацию подвижной станции (MS) и сети. Протокол UMTS AKA является запросно-ответным протоколом, в котором применяется долгосрочный ключ, *K*, который используется совместно универсальным модулем идентификатора абонента (USIM) и центром аутентификации (AuC). Эти объекты находятся на универсальной смарт-карте (UICC) MS и в домашней сети подвижной станции соответственно. Протокол AKA определен в [b-3GPP TS 33.102], Архитектура безопасности.

Хотя механизм AKA обычно используется для аутентификации беспроводных устройств, оборудованных смарт-картами, например UICC, в технических условиях AKA нет ничего, что могло бы помешать применению этого механизма для аутентификации фиксированных устройств, способных работать с приложениями USIM.

9.4 IPsec между недоверенной и доверенной, но уязвимой зоной

TE-BE – это элемент сети СПП, который находится в недоверенной зоне. Вместе с тем он по-прежнему управляется оператором СПП и ему необходим доступ к системам OAMP, находящимся в доверенной зоне. Следовательно, существует элемент OAMP-SE, который находится в доверенной, но уязвимой зоне и который функционирует как пункт ответа для сообщений OAMP.

TE-BE может обеспечивать, что соединения, защищенные TLS, не проходят через туннель IPsec VPN. TE-BE может обеспечивать, что медиапотоки, защищенные с помощью SRTP, не проходят через туннель IPsec VPN.

Туннель IPsec VPN может использоваться протоколом IPsec ESP [IETF RFC 4303] в режиме туннелирования [b-IETF RFC 4301].

Услуга антиповтора IPsec может быть включена в любое время.

Туннель IPsec VPN может поддерживать идентификаторы преобразования ESP_3DES (размер ключа 192 бита в режиме CBC) и ESP_CAMELLIA (размер ключа 128 битов в режиме CBC) [b-IETF RFC 4312]. Рекомендуется, чтобы туннель IPsec VPN поддерживал идентификатор преобразования ESP_AES (размер ключа 128 битов в режиме CBC).

Туннель IPsec VPN может поддерживать алгоритмы аутентификации HMAC-MD5-96 (размер ключа 128 битов) и HMAC-SHA-1-96 (размер ключа 160 битов).

Генерация ключей и управление ключами для туннеля IPsec VPN может выполняться с помощью IKE [b-IETF RFC 2409], используя аутентификацию IKE с цифровыми подписями или аутентификацию IKE с предварительно разделенным ключом. Если используется аутентификация IKE с цифровыми подписями, и клиент, и сервер могут обмениваться сертификатами X.509, а сертификаты могут проверяться.

10 Безопасность среды передачи

В инфраструктуре СПП шифрование медиаполотоков не требуется, но может возникнуть необходимость его поддержки, если пользователь запрашивает такое шифрование. Эта поддержка может включать поддержку протоколов шифрования медиапотоков SRTP [b-IETF RFC 3711]. В дальнейшей части данного пункта предполагается, что пограничные элементы сети (например, граница домена поставщика сети) реализуют шифрование/дешифрование, хотя это возможно осуществлять на отдельной платформе, совместно используемой элементами NBE. В любом случае шифрование и дешифрование должно быть совмещено с другими возможностями обработки медиапотока, такими как обнаружение и транскодирование двухтонального многочастотного набора (DTMF).

В случае требования соединения абонентов, запрашивающих выполнение шифрования медиапотока в их линии доступа, с абонентами, которые не запрашивают (или не поддерживают) этого, существуют пять случаев, которые необходимо рассматривать и иллюстрации которых представлены на рисунке 4.

Первый и самый простой случай возникает, если ни один из оконечных пунктов не запрашивает выполнения шифрования. Медиапоток поступает от источника в пункт назначения через пограничные элементы без шифрования в какой-либо из линий. Ни пограничный элемент сети NBE 1 (выступающий как отправитель), ни пограничный элемент сети NBE 2 (выступающий как получатель) не выполняют какого-либо шифрования или дешифрования.

Второй случай возникает, если отправитель запрашивает шифрование медиапотока, а получатель не запрашивает шифрование. Элемент NBE 1 функционирует как пункт шифрования/дешифрования ответа. NBE 1 получает зашифрованный медиапоток от отправителя, дешифрует его и пропускает его по инфраструктуре СПП к элементу NBE 2, который направляет его (по-прежнему незашифрованным) к получателю. В обратном направлении элемент NBE 1 принимает незашифрованный медиапоток, поступающий по инфраструктуре СПП, и шифрует его до направления к отправителю. Таким образом, медиапоток на участке 1 (от отправителя до элемента NBE 1) является зашифрованным, на участке 2 (между NBE 1 и NBE 2) – незашифрованным и на участке 3 (между NBE 2 и получателем) – незашифрованным.

Третий случай возникает, если получатель запрашивает шифрование медиапотока, а отправитель – не запрашивает. Элемент NBE 2 функционирует как пункт шифрования/дешифрования ответа. Элемент NBE 1 принимает незашифрованный медиапоток от отправителя и пропускает его (по-прежнему незашифрованным) по инфраструктуре СПП к элементу NBE 2. NBE 2 шифрует его и пропускает к получателю. В обратном направлении NBE 2 принимает зашифрованный медиапоток от оконечного пункта – получателя и дешифрует его до направления по инфраструктуре СПП. Элемент NBE 1 пропускает незашифрованный медиапоток к отправителю. Таким образом, медиапоток на участках 1 и 2 является незашифрованным, а на участке 3 – зашифрованным.

Четвертый случай возникает, если отправитель и получатель – оба – запрашивают шифрование медиапотока, но ни один из них не поддерживает совместимых схем шифрования или инфраструктура СПП обеспечивает какую-либо расширенную услугу (такую, как обнаружение двухтонального многочастотного набора (DTMF) для приложений телефонной карты). Оба элемента – NBE 1 и NBE 2 – функционируют как точки шифрования/дешифрования ответа. NBE 1 принимает зашифрованный поток от отправителя, дешифрует его и пропускает по инфраструктуре СПП к элементу NBE 2. NBE 2 зашифровывает его и пропускает к получателю. В обратном направлении элемент NBE 2 принимает зашифрованный медиапоток от оконечного пункта – получателя и дешифрует его до направления по инфраструктуре СПП. Элемент NBE 1 принимает незашифрованный медиапоток и зашифровывает его перед отправкой к отправителю. Таким образом, медиапоток на участках 1 и 3 является зашифрованным, а медиапоток, следующий по инфраструктуре СПП (участок 2) – незашифрованным.

Пятый случай возникает, если отправитель и получатель – оба – запрашивают шифрование медиапотока, поддерживают совместимые схемы шифрования, а в инфраструктуре СПП не обеспечиваются расширенные услуги. Элемент NBE 1 принимает зашифрованный медиапоток от отправителя и пропускает его без изменения по инфраструктуре СПП к элементу NBE 2, который пропускает его без изменения к получателю. В обратном направлении NBE 2 принимает зашифрованный медиапоток от получателя и пропускает его без изменения по инфраструктуре СПП к элементу NBE 1, который пропускает его без изменения к отправителю. Таким образом, медиапоток на всех трех участках является зашифрованным. Сигнализация, необходимая для обеспечения данного случая не входит в сферу применения данной Рекомендации.

Шифрование медиапотока, описанное в данном пункте, обеспечивает аутентификацию, конфиденциальность и целостность сообщения.

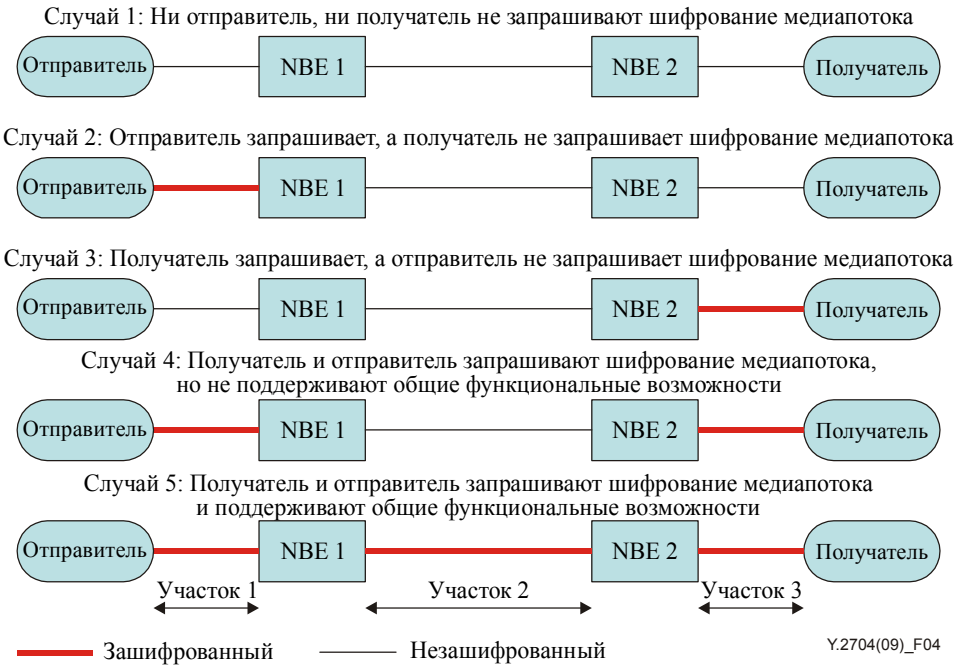


Рисунок 4 – Взаимосвязь шифрования медиапотока, возможностей пограничных элементов и запроса отправителя/получателя

10.1 Протокол SRTP

Защищенный протокол RTP описан в [b-IETF RFC 3711] и определен как профиль RTP [b-IETF RFC 3550]. Он предназначен для реализации между уровнем приложения RTP и транспортным уровнем в наборе протоколов – для осуществления перехвата пакета RTP, пересылки эквивалентного пакета SRTP и передачи эквивалентного пакета RTP сверху набора протоколов на приемной стороне. Он в основном осуществляет шифрование информационной части пакета RTP и добавляет аутентификационный признак в конец пакета на передающей стороне, а также проверяет аутентификационный признак и дешифрует информационную часть пакета на приемной стороне.

10.1.1 Алгоритмы шифрования и аутентификации

Элемент NBE, поддерживающий SRTP, может поддерживать AES в режиме счетчика [b-IETF RFC 3711]. Более подробная информация представлена в [b-NIST FIPS SP 800-38a]. NBE может поддерживать HMAC-SHA1 для генерации проверки целостности сообщений, длина признака составляет 80 битов.

10.1.2 Согласование набора параметров шифрования и генерация ключа

Генерация ключей для SRTP может выполняться несколькими способами:

1) путем обеспечения доступа (через элемент обеспечения доступа TE);

2) путем использования материала ключа, сгенерированного устройством – оконечным пунктом и включенного в протокол описания сеанса (SDP) [b-IETF RFC 4566] в запросах INVITE;

3) путем обмена материалом ключа с использованием отдельного протокола управления ключами и вложения его с SDP.

Для каждого абонента элемент NBE может получить от элементов SAA/TAA-FE главный ключ SRTP и из него получить предварительные ключи шифрования и аутентификации сеанса. Может поддерживаться главный ключ SRTP длиной 128 байтов. Может поддерживаться алгоритм вывода ключа, описанный в [b-IETF RFC 3711]. Длина предварительного ключа шифрования может составлять 128 битов, длина предварительного добавляемого сеансового ключа может составлять 112 битов, а предварительный ключ аутентификации может составлять 160 битов. После выдачи абоненту нового главного ключа SRTP NBE может немедленно начать его использовать.

Если SDP в запросе INVITE содержит "RTP/SAVP" в качестве значения медиапротокола в строке "m=", не содержит значение ключа в строке "k=" и не содержит атрибут "a=crypto", то элемент NBE может использовать предварительные ключи из системы обеспечения в качестве реальных ключей для данного сеанса. В этом случае набор параметров шифрования не согласовывается.

Если SDP в запросе INVITE содержит "RTP/SAVP" в качестве значения медиапротокола в строке "m=", не содержит значение ключа в строке "k=" и содержит значение ключа в строке "k=", то элемент NBE может использовать ключ, содержащийся в строке "k=", в качестве главного ключа SRTP и генерировать из него сеансовый и аутентификационный ключи. В этом случае набор параметров шифрования не согласовывается.

Если SDP в запросе INVITE содержит "RTP/SAVP" в качестве значения медиапротокола в строке "m=" и атрибут "a=crypto", то элемент NBE может генерировать сеансовый и аутентификационный ключи согласно требованиям [b-IETF RFC 4568]. Например, запись SDP "a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4" означает, что набором шифрования является AES_CM_128_HMAC_SHA1_80, а key_param определяется текстом, начинающимся с "inline:". Первое поле в key_param является главным ключом с добавляемым главным ключом, сцепленным и затем кодированным в формат base64. Перечень имеющихся наборов шифрования представлен в пункте 5.2 [b-IETF RFC 4568], из которого выбирается один в ходе обмена "предложение/ответ".

Если SDP в запросе INVITE содержит "RTP/SAVP" в качестве значения медиапротокола в строке "m=" и атрибут "a=key-mgmt", то элемент NBE может генерировать ключи и параметры безопасности в соответствии с требованиями [b-IETF RFC 4567]. Например, "a=key-mgmt:mikey AQAFgM0XflABAAAAAAAAAAAAA..." означает, что протоколом управления ключами является mikey [b-IETF RFC 3830], а оставшийся текст является данными управления ключами, кодированными в формат base64 [b-IETF RFC 4648].

10.1.3 Интерфейс аутентификации между элементом сети СПП и сервером жетонов безопасности

Элемент сети СПП может осуществлять реализацию SASL [b-IETF RFC 4422] для защиты своих функций OAMP. Уровень SASL может включать аутентификационную проверку по жетону безопасности, как это описано в [b-IETF RFC 2808]. Это связывается с "жетоном безопасности" ключа SASL. Пользователь, запрашивающий доступ к OAMP обеспечивает:

1 идентификационные данные для авторизации (что позволяет системным администраторам выполнить регистрацию с другими идентификационными данными пользователя; если поле пусто, по умолчанию происходит переход к идентификационным данным для аутентификации);

2 идентификационные данные для аутентификации (идентичность, чей код-пароль будет использоваться);

3 пин-значение пользователя и 6-значный код-пароль в жетоне безопасности.

Элемент сети СПП может осуществлять реализацию согласованного с SAA/TAA-FE клиента как часть выполняемой SASL обработки жетона безопасности. Элемент сети СПП собирает представленные полномочия пользователя и затем передает их на сервер жетонов безопасности. Собираемые поля включают имя пользователя, пин-код и отражаемое в текущий момент значение жетона безопасности. Элемент сети принимает обратно сообщение статуса Прием/Отказ/Повтор. Если результат успешный, SASL открывает пользователю доступ к функциям OAMP исходя из уровня доступа, связанного с именем этого пользователя.

11 OAMP

По всем случаям попыток доступа к OAMP (успешным и неуспешным), изменения OAMP и завершения OAMP должен фиксироваться след аудита. Кроме того, должны регистрироваться события, считающиеся важными согласно политике поставщика СПП.

В данном пункте содержится описание некоторых механизмов выполнения важных функций. Оно не является исчерпывающим и, исходя из политики поставщика СПП, могут быть приняты другие реализации.

ПРИМЕЧАНИЕ. – Необходимо обеспечить безопасность регистрации событий. Дополнительная информация содержится в [ITU-T Y.2701] и [b-ITU-T M.3016.0].

11.1 Интерфейс элемента сети и систем регистрации

Рекомендуется, чтобы элементы сети отправляли свою информацию для регистрации на удаленную хост-машину регистрации. Те элементы, которые для выполнения этой функции используют протокол Syslog [b-IETF RFC 5424], могут следовать требованиям данного пункта.

Элементы сети, которые используют протокол Syslog, могут включать отметку времени, указывающую время на основании значения, полученного из доверенного источника времени через SNTP/NTP, и могут передавать время в формате UTC. Элементы могут включать название их хост-машины (если информация о ней была обеспечена) или свой IP-адрес в заголовке сообщения syslog.

11.2 Использование SNMP элементами сети

Важно, чтобы элементы сети СПП могли быть управляемыми с удаленной платформы. Реализует это механизм SNMP, который является отраслевым стандартом. Все большее распространение получает SNMPv3 [b-IETF RFC 3413], [b-IETF RFC 3414] и [b-IETF RFC 3415], в котором разрешены многие проблемы безопасности, свойственные SNMPv2.

Рекомендуется, чтобы элементы сети отправляли свою информацию для регистрации на удаленную хост-машину регистрации. Для выполнения этой функции такие элементы могут использовать протокол SNMP, принимая во внимание оговорки, сделанные в настоящей Рекомендации в отношении SNMPv3.

SNMP определяется общей архитектурой [b-IETF RFC 3411], механизмом именования объектов и событий (MIB) [b-IETF RFC 1155], [b-IETF RFC 1212], [b-IETF RFC 1215], [b-IETF RFC 2578], [b-IETF RFC 2579] и [b-IETF RFC 2580] и протокольными функциями [b-IETF RFC 3416] и [b-IETF RFC 3417]. Более подробный обзор документов, в которых описана современная стандартная схема сетевого управления, содержится в пункте 7 [b-IETF RFC 3410].

Каждый элемент сети СПП может осуществлять реализацию клиента SNMP. Если используются SNMPv1 или v2 и если этого требует политика безопасности поставщика СПП, то в качестве транспорта Элементы сети должны использовать UDP по IPSec. Каждый экземпляр сообщения может кодироваться с использованием базовых правил кодирования ASN.1 [b-ITU-T X.690] в единую дейтаграмму UDP. Клиент может использовать порт 161 для приложений ответчика на запросы и может использовать порт 162 для приложений приемника уведомлений.

Требуется, чтобы элементы сети СПП выполняли реализацию всех необходимых MIB для отчета по событиям безопасности и следам аудита.

11.3 Управление обновлениями для безопасности

Регулярное проведение технического обслуживания и установка обновлений для безопасности на элементах сети и серверах СПП сводит к минимуму их уязвимость для атак и неумышленных отказов. Необходимо разработать комплексную стратегию управления обновлениями, включая процессы и платформы для выполнения установки и проверки.

11.4 Управление версиями

Конфигурации и изменения элементов сети должны архивироваться. Основной целью архивирования системы является возможность восстановления системы в случае сбоев аппаратного и программного оборудования, которые ведут к повреждению данных загрузки программного обеспечения и/или связанных с этим системных данных. В состав архивируемых системных данных для загрузки могут входить следующие:

- данные и логические правила, касающиеся клиентов;
- возможности соединения сетевого трафика, такие как устройства и магистрали;
- оператор СПП и прикладное программное обеспечение поставщиков;
- операционная система;
- конфигурация аппаратного оборудования.

Требуется вести непрерывную регистрацию работы по обеспечению, с тем чтобы можно было осуществить обновление любого элемента сети (NE) с помощью действий по обеспечению, которые были выполнены с момента, когда было сделано архивирование образа системы.

Платформа обеспечения может выполнять следующие функции:

- Журнал регистрации действий для каждого элемента сети (NE), осуществляющего непосредственное предоставление.
- Состояние действий по предоставлению для каждого NE, как минимум, за одну неделю.

Платформа обеспечения может предоставить пользователям возможность просмотра в ручном режиме сохраненных действий по обеспечению для каждого NE. Предоставляемое пользователю описание действий необходимо для составления сводки по размеру, количеству и типу транзакций, выполненных в течение данного интервала времени.

Платформа обеспечения может предоставлять служебную программу, которая позволяет провести повторное обеспечение доступа NE путем повторного ввода данных в определенный NE. Эта служебная программа должна допускать выбор даты/времени начала и окончания для данных, которые должны быть представлены повторно. Исходя из определенных значений даты/времени начала и окончания, платформа обеспечения должна автоматически выполнять повторный ввод всех промежуточных данных в конкретный NE.

11.5 След аудита, перехват, регистрация в TE-BE

Все требования в отношении следа аудита, перехвата и регистрации, относящиеся к сетевым элементам СПП, применяются к TE-BE.

TE-BE подсоединяется к системам OAMP через туннель VPN. Следовательно, он направляет свои сообщения регистрации, принимает запросы SNMP и направляет ответы SNMP через эту VPN. Не рекомендуется, чтобы TE-BE принимал какие-либо запросы OAMP по какому-либо иному интерфейсу.

Требования к туннелю VPN представлены в пункте 9.4.

12 Обеспечение для оборудования в недоверенной зоне

Конфигурирование всего оконечного абонентского оборудования выполняется элементом обеспечения TE. Элемент обеспечения TE размещается в доверенной зоне и может осуществлять связь с TE только через пограничные элементы сети (NBE), как показано на рисунке 2. TE или TE-BE могут осуществлять аутентификацию и устанавливать ассоциацию безопасности с NBE до того, как он сможет получить файл конфигурации от элемента обеспечения TE. Для установления ассоциации безопасности с оконечным оборудованием (включая TE-BE) NBE может поддерживать и TLS и IPsec. Более подробно это описано в пунктах 9.1 и 9.2.

В этом контексте управляемое поставщиком оборудование может трактоваться как часть NBE.

Элемент обеспечения TE указывает адрес NBE в данных конфигурации, загружаемых для аутентифицированного устройства. Элемент обеспечения TE также может включать сертификат, используемый для аутентификации абонента с NBE, как описано в пункте 8.4.

Устройство TE запрашивает обеспечение от поставщика услуг СПП. Элемент NBE принимает этот запрос и проводит аутентификацию TE с помощью SAA/TAA-FE. После выполнения аутентификации устройства пограничный элемент направляет запрос обеспечения элементу обеспечения TE. Элемент обеспечения TE затем загружает конфигурацию и/или программный модуль в TE. Если аутентификация TE невозможна, регистрируется отказ.

Дополнение I

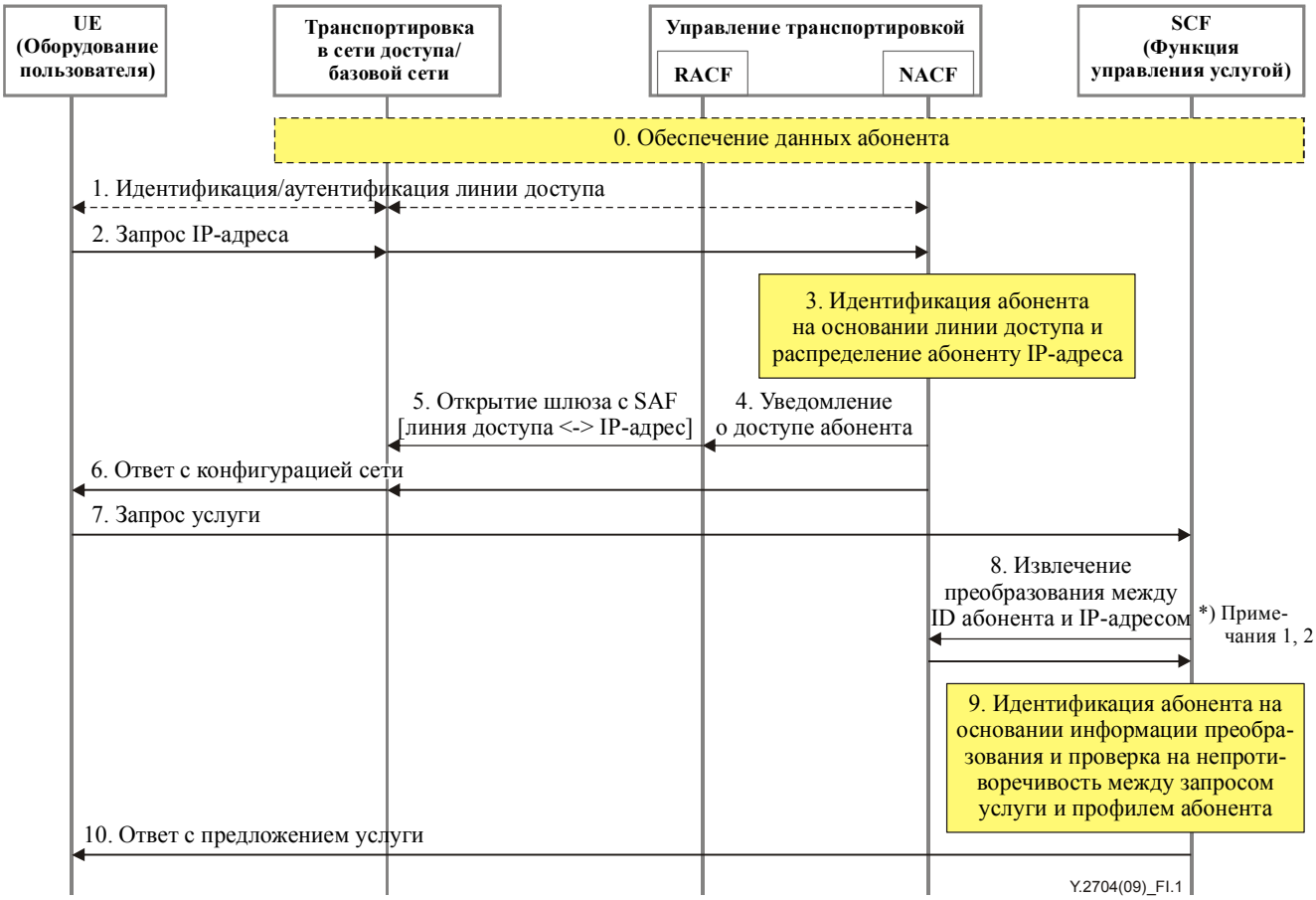
Примеры гарантирования адреса источника и его применения в механизме идентификации и аутентификации абонента

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

В настоящем Дополнении представлены конкретные примеры механизмов гарантирования адреса источника и его применения к идентификации и аутентификации абонента по сетевому адресу источника, как это описано в пункте 8.4.2.

I.1 Идентификация и аутентификация абонента, связанные с аутентификацией линии доступа

В данном пункте представлен пример идентификации и аутентификации абонента, в котором IP-адрес присваивается как результат аутентификации линии доступа. В примере каждый абонент статически связан со своей линией доступа. Вследствие этого, описанный в данном примере механизм применим только к некочевым (т. е. фиксированным) услугам.



ПРИМЕЧАНИЕ 1. – Информация преобразования между IP-адресом и ID абонента может предоставляться от функции управления доступом к сети (NACF) в функцию управления услугой (SCF) в момент распределения адресов функцией NACF.

ПРИМЕЧАНИЕ 2. – Функция NACF может обеспечивать преобразование между IP-адресом и информацией о местоположении (например, идентификатор линии) вместо преобразования между IP-адресом и ID абонента. В этом случае требуется, чтобы SCF осуществляла преобразование между идентификатором и местоположением абонентов и выводила ID абонента из информации о местоположении, переданной от NACF.

Рисунок I.1 – Потоки сообщений высокого уровня в примере 1

Описание

0 Профили абонентов имеют предварительно установленную конфигурацию с соответствующими FE (например, TUP-FE, SUP-FE) в функции NACF или SCF.

В данном сценарии наиболее важными являются следующие установки:

1) NACF (обычно TUP-FE) поддерживает преобразование между идентификаторами абонентов (идентификатор счета абонента) и идентификаторами логических/физических линий доступа (например, ID сети VLAN или порт доступа).

2) SCF (обычно SUP-FE) поддерживает преобразование между идентификаторами абонентов и атрибутами или профилями соответствующих абонентов (например, значения заголовка "From" в случае услуг на базе SIP). В случае если пространство имен ID абонента в функции SCF отличается от пространства имен ID абонента в функции NACF, рекомендуется, чтобы функция SCF также поддерживала преобразование между этими идентификаторами.

   В ином случае, функция NACF не должна поддерживать преобразование между идентификаторами абонента и линии доступа. Для таких сценариев рекомендуется, чтобы функция SCF поддерживала преобразование между идентификаторами абонента и линии доступа, так чтобы функция SCF могла извлечь ID соответствующего абонента из ID линии доступа.

   В шлюзах транспортировки в сети доступа/базовой сети в соответствии с начальной конфигурацией все проходы для линий доступа абонента закрыты, так что отбрасываются все входящие IP-пакеты, кроме пакетов, необходимых UE для присоединения к сети (например, передача запроса адреса или запроса аутентификации).

1 UE присоединяется к сети доступа по своей линии доступа, с тем чтобы получить IP-соединение с СПП. В этом примере предполагается неявная аутентификация доступа функцией NACF, которая выполняется на шаге 3. Вместе с тем функция NACF может альтернативно использовать метод явной аутентификации доступа (например, IEEE 802.1X). В этом случае на данном этапе выполняется аутентификация доступа к сети, т. е. до присвоения IP-адреса.

2 UE запрашивает распределение IP-адреса. Это, как правило, выполняется путем направления сообщения об обнаружении и запросе DHCP; эти сообщения ретранслируются шлюзами к функции NACF.

3 В данном примере сеть доступа выполняет аутентификацию линии доступа и обеспечивает ID аутентифицированной линии доступа (например, ID сети VLAN или порт доступа) для функции NACF. Следовательно, NACF может идентифицировать ID абонента UE на основании ID линии доступа, по которой направляется запрос на IP-адрес. Далее, функция NACF распределяет IP-адрес запрашивающему UE и сохраняет преобразование между ID абонента и распределенным IP-адресом.

Эта информация преобразования может быть передана от функции NACF к функции SCF и сохранена (кэширована) в SCF. В этом случае шаг 8, ниже, может быть пропущен.

4 Функция NACF уведомляет функцию RACF о том, что абонент подсоединен. Это уведомление включает ID абонента, ID линии доступа (физической/логической), распределенный IP-адрес и профили QoS.

5 Функция RACF принимает определяемое политикой решение о распределении сетевых ресурсов абоненту и дает задание шлюзам открыть проход для линии доступа, применяя правила фильтрации пакетов, согласно которым осуществляется прием и передача входящих IP-пакетов, адресом источника которых является IP-адрес, присвоенный абоненту, а остальные входящие пакеты отбрасываются.

Обеспечение фильтрации IP-адресов источника, координируемой с аутентификацией линии доступа функцией NACF, как это описано выше, обеспечивает, что IP-адрес может использоваться только тем абонентом, которому этот адрес присвоен.

6 Функция NACF возвращает распределенный IP-адрес UE с другими параметрами конфигурации сети (например, адреса серверов DNS и P-CSC-FE). Это обычно выполняется путем передачи сообщений предложения DHCP и ответа на него.

7 После получения IP-подсоединения UE передает функции SCF запрос услуги (например, сигнал REGISTER в случае услуг на базе SIP). Ответ с предоставлением услуги будет пропущен шлюзами (брандмауэры с фильтрацией по адресу источника) к SCF, только если адрес источника запроса является одним из присвоенных функцией NACF.

8 Функция SCF извлекает из функции NACF информацию о преобразовании (т. е. ID абонента и присвоенный ему IP-адрес), соответствующую адресу источника запроса услуги.

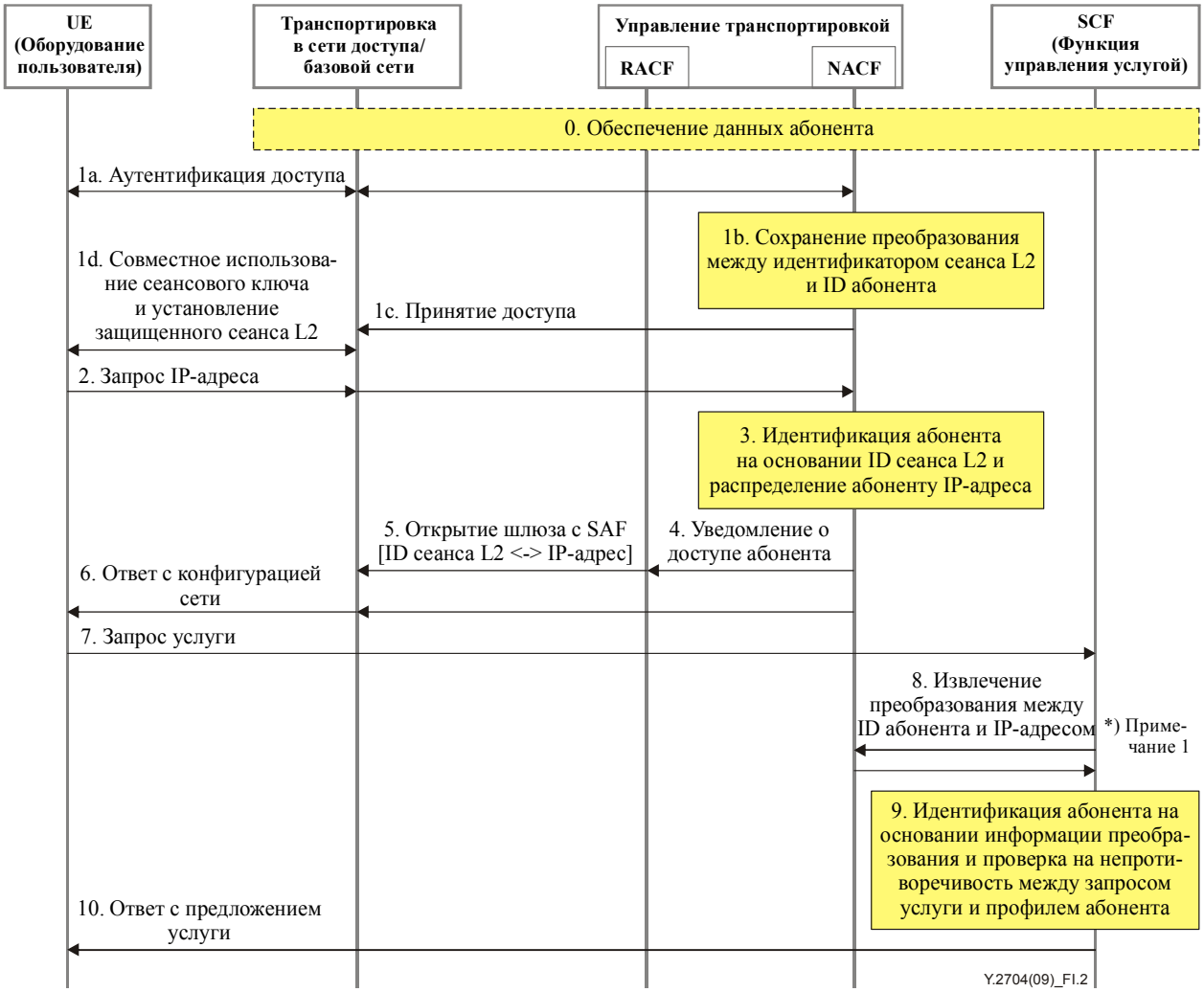
9 Функция SCF рассматривает запрос услуги как поступивший от абонента, которому присвоен ID абонента, содержащийся в извлеченной информации о преобразовании. В случае если пространство имени ID абонента в функции SCF отличается от пространства имени в функции NACF, требуется, чтобы выполнялась трансляция извлеченного ID абонента в ID абонента в пространстве имени, используемом функцией SCF, на основе преобразования между этими ID.

Функция SCF извлекает значение атрибутов, касающихся идентичности абонента (например, значение заголовка "From" в случае услуг на базе SIP), из запроса услуги и осуществляет проверку на противоречивость этих значений и профиля соответствующего абонента.

10 Если аутентификация и авторизация выполняются успешно, функция SCF возвращает нормальный ответ с предложением запрошенной услуги (например, "200 OK" в случае услуг на базе SIP).

I.2 Идентификация и авторизация абонента, связанные с явной аутентификацией доступа при установлении возможности IP-соединения

В данном пункте представлен пример идентификации и авторизации абонента, в котором IP-адрес присваивается как результат явной аутентификации доступа при установлении возможности IP-соединения. В примере каждый абонент динамически связан с сеансом L2, который устанавливается в момент аутентификации доступа. Вследствие этого, описанный в данном примере механизм применим как к кочевым, так и некочевым услугам.



ПРИМЕЧАНИЕ 1. – Информация преобразования между IP-адресом и ID абонента может предоставляться от функции NACF в функцию SCF в момент распределения адресов функцией NACF.

Рисунок I.2 – Потоки сообщений высокого уровня в примере 2

Описание

0 Профили абонентов имеют предварительно установленную конфигурацию с соответствующими FE (например, TUP-FE, SUP-FE) в функции NACF или SCF. В отличие от предыдущего примера от функции NACF не требуется поддержка преобразования между ID абонента и ID линии доступа.

В шлюзах транспортировки в сети доступа/базовой сети в соответствии с начальной конфигурацией все проходы для сеансов доступа L2 с UE закрыты, так что отбрасываются все входящие IP-пакеты, кроме пакетов, необходимых UE для присоединения к сети (например, передача запроса адреса или запроса аутентификации).

1a Когда UE запрашивает соединение с СПП, сеть доступа динамически создает сеанс L2 с UE, и выполняется процедура аутентификации доступа между UE и функцией NACF на основании полномочий абонента (как правило, с помощью метода явной аутентификации, такого как IEEE 802.1X и RADIUS/Diameter). Сообщения сигнализации для аутентификации направляются шлюзами.

1b В ходе процедуры аутентификации идентификатор сеанса L2 (например, VLAN-ID, L2-адрес UE и т. д.), присвоенный оборудованию UE, передается функции NACF. Если аутентификация завершается успешно, NACF сохраняет этот идентификатор сеанса L2 вместе с ID аутентифицированного абонента.

1c Функция NACF извещает сеть доступа о том, что UE было успешно аутентифицировано и что разрешен доступ к сети (например, сообщение ACCESS ACCEPT в случае использования протокола RADIUS).

1d По получении от функции NACF извещения об успешной аутентификации абонента сеть доступа устанавливает ассоциацию безопасности (SA) с UE для защиты целостности и конфиденциальности сеанса L2. Обычно это выполняется с помощью механизмов вывода сеансовых ключей, определенных в IEEE 802.1X, и защитных процедур, определенных для каждой технологии L2 (например, TKIP/CCMP, определенный в IEEE 802.11i для беспроводных локальных сетей 802.11).

Описанные выше механизмы обеспечения безопасности защищают сеанс L2 от использования его другими абонентами и предоставляют необходимые параметры для предупреждения имитации IP-адресов.

2 UE запрашивает распределение IP-адреса. Это, как правило, выполняется путем направления сообщения об обнаружении и запросе DHCP; эти сообщения ретранслируются шлюзами к функции NACF.

3 Функция NACF идентифицирует ID абонента UE на основании идентификатора сеанса L2, в рамках которого передан запрос. Далее, функция NACF распределяет IP-адрес запрашивающему UE и сохраняет преобразование между ID абонента и распределенным IP-адресом.

Эта информация преобразования может быть передана от функции NACF к функции SCF и сохранена (кэширована) в SCF. В этом случае шаг 8, ниже, может быть пропущен.

4 Функция NACF уведомляет функцию RACF о том, что абонент подсоединен. Это уведомление включает ID абонента, ID сеанса L2 (физический/логический), распределенный IP-адрес и профили QoS.

5 Функция RACF принимает определяемое политикой решение о распределении сетевых ресурсов абоненту и дает задание шлюзам открыть проход для сеанса L2, применяя правила фильтрации пакетов, согласно которым осуществляется прием и передача входящих IP-пакетов, адресом источника которых является IP-адрес, присвоенный абоненту, а остальные входящие пакеты отбрасываются.

Обеспечение фильтрации IP-адресов источника, координируемой с аутентификацией линии доступа функцией NACF, как это описано выше, обеспечивает, что IP-адрес может использоваться только тем абонентом, которому этот адрес присвоен.

Шаги 6–10 аналогичны шагам, описанным в предыдущем примере в пункте I.1.

Дополнение II

Безопасность при присоединении службы электросвязи в чрезвычайных ситуациях (ETS)

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

II.1 Базовая информация

Служба электросвязи в чрезвычайных ситуациях (ETS) является национальной службой, обеспечивающей приоритетное предоставление услуг электросвязи авторизованным пользователям ETS во время бедствий и чрезвычайных ситуаций. Реализация ETS является внутренним делом каждой страны. Однако бедствия/чрезвычайные ситуации могут выходить за географические границы, и потому существует вероятность того, что страны/администрации могут заключить двусторонние и/или многосторонние соглашения по соединению своих соответствующих систем ETS. Это сделает возможной поддержку предоставления во время бедствий и чрезвычайных ситуаций приоритетных услуг электросвязи (например, голос, сообщения, видео и данные) в рамках ETS между различными государственными сетями, имеющими двусторонние и/или многосторонние соглашения. Гарантия и доступность связи ETS будет определяться функциями и мерами безопасности, которые применяются в каждой национальной сети, участвующей в обеспечении связи между оконечными устройствами.

II.2 Сфера применения/задачи

В настоящем Дополнении представлено руководство для поддержания безопасности, обеспечиваемой сетью для служб ETS, при работе через разные национальных сети (т. е. страны/администрации).

Сквозная одноранговая функция конечного пользователя с использованием специальных функций безопасности оборудования конечного пользователя не входит в сферу применения данного Дополнения. Сфера применения Дополнения ограничена безопасностью, обеспечиваемой сетью для услуг ETS по нескольким сетям на основе транзитных участков. Вместе с тем рекомендуется, чтобы СПП обладала возможностью прозрачной поддержки таких одноранговых функций.

В данном Дополнении не ставится задача определения условий для национальных реализаций ETS. Основной задачей Дополнения является безопасность, обеспечиваемая сетью для услуг ETS (т. е.приоритетная голосовая связь, видео, передача данных и передача сообщений) через разные национальные сети (т. е. страны/администрации).

II.3 Задачи безопасности и руководящие принципы для присоединения служб ETS

Информация о задачах безопасности и руководящие принципы для присоединения служб ETS представлена в Дополнении I к [ITU-T Y.2701].

II.4 Аутентификация и авторизация

Рекомендуется, чтобы национальные сети поддерживали и реализовывали механизмы и функциональные возможности, необходимые для аутентификации и авторизации пользователя, устройства или сочетание пользователя и устройства ETS исходя из уровня безопасности, необходимого для доступа к конкретной услуге (например, передача голоса, данных, видео), и применимой политики.

Рекомендуется, чтобы механизмы безопасности для идентификации и аутентификации пользователей и устройств пользователей, описанные в основной части настоящей Рекомендации, использовались соответствующим образом для поддержки реализаций ETS в национальных сетях:

- ассоциации IPsec/TLS;
- вызов/ответ SIP и сертификаты X.509;
- общая архитектура начальной загрузки.

Кроме того, в целях обнаружения и предупреждение атак типа "отказ в обслуживании" рекомендуется реализация мер безопасности для контроля доступа к ресурсам ETS.

Информацию о примерах подходов к аутентификации и авторизации в ETS содержится также в Дополнении I к [ITU-T Y.2702].

II.5 Безопасность транспортировки для сигнализации и OAMP

Рекомендуется, чтобы механизмы безопасности, IPsec и TLS, описанные в основной части настоящей Рекомендации, использовались соответствующим образом для защиты сигнализации и трафика OAMP ETS в национальных сетях.

II.6 Трафик медиапотоков

Рекомендуется, чтобы механизмы безопасности для идентификации и защиты трафика медиапотоков, описанные в основной части настоящей Рекомендации, использовались соответствующим образом для защиты трафика медиапотоков ETS в национальных сетях.

II.7 Поддержка функций ограничений по ID номера вызывающей стороны и ID имени вызывающей стороны

ID номера вызывающей стороны и ID имени вызывающей стороны – это две унаследованные функции КТСОП, которые дают пользователям возможность узнать, кто осуществляет вызов. Вызовы ETS могут обслуживать разные национальные сообщества пользователей, у которых могут быть разное отношение к раскрытию такой информации вызываемой стороне. Поэтому рекомендуется поддерживать соответствующий механизм для обеспечения применения политики, касающейся отображения или раскрытия информации о пользователе ETS. Поэтому рекомендуется, поддерживать необходимые механизмы принуждения соблюдения правил касательно воспроизведения или раскрытия информации пользователя ETS.

II.8 Невозможность прослеживания

Для некоторых видов связи ETS важно, чтобы информации о местоположении вызывающей и вызываемой стороны была в максимальной степени недоступной для всех участников. В частности, рекомендуется, чтобы любая связанная с местоположением информация подавлялась или, при необходимости, заменялась не имеющей смысла информацией в соответствии с применимой политикой. Связанная с местоположением информация может включать, в том числе, следующую:

1) NPA-NXX или URI вызывающей или вызываемой стороны;
2) географический адрес вызывающей или вызываемой стороны;
3) координаты по осям x и y вызывающей или вызываемой стороны;
4) информация о соте вызывающей или вызываемой стороны, которая может использоваться для уточнения местоположения до соты;
5) IP-адрес вызывающей или вызываемой стороны;
6) оконечная станция вызывающей или вызываемой стороны или другая информация об объектах, по которой может быть определен географический ориентир вызывающей или вызываемой стороны.

II.9 Сквозное одноранговое шифрование

Некоторые пользователи могут требовать вызовы/сеансы ETS, шифрование которых осуществляет оборудование пользователя (UE). Для этих вызовов/сеансов применяются обычные процедуры установления вызова/сеанса ETS, а UE обеспечивает процесс сквозного шифрования для информации, поступающей по каналу-носителю (например, передача голоса) к оконечному UE. Этот процесс шифрования прозрачен для СПП. Вместе с тем рекомендуется, чтобы СПП обладала возможностью прозрачной поддержки таких одноранговых функций.

Дополнение III

Примеры передового опыта в области обеспечения безопасности

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

III.1 Введение

Для обеспечения требований, определенных в [ITU-T Y.2701], могут потребоваться дополнительные механизмы безопасности, не входящий в круг описанных в настоящей Рекомендации. Для защиты инфраструктуры СПП можно использовать передовой опыт в области обеспечения безопасности, в том числе применение брандмауэров, усиление операционной системы, контроль уязвимостей и систем обнаружения проникновений (IDS). Руководство по системам обнаружения и предупреждения проникновений см. в [b-NIST SP 800-94], руководство по предупреждению и обработке инцидентов, связанных с вредоносным программным обеспечением, см. в [b-NIST SP 800-83].

В данном Дополнении кратко представлены примеры передового опыта по применению механизмов безопасности, которые следует использовать.

III.2 Брандмауэры

Брандмауэры – это основные структурные элементы безопасности, которые обеспечивают изоляцию сети на границах между сегментами сети или между разными сетями. Брандмауэры обеспечивают изоляцию на основе конкретных правил фильтрации трафика, включенных в конфигурацию брандмауэров. Для обеспечения дополнительного уровня безопасности брандмауэры могут использоваться в сочетании с другими механизмами безопасности. Дополнение брандмауэров способствует обеспечению безопасности путем "эшелонированной защиты", когда для достижения более устойчивой защиты выполняется перекрытие несколько механизмов безопасности.

Брандмауэр анализирует входящий и исходящий трафик, и его конфигурация должна обеспечивать отклонение любого трафика, кроме конкретно разрешенного правилами брандмауэра. Брандмауэр может также выполнять регистрацию трафика и включать сигнал тревоги при обнаружении неразрешенных пакетов. Физически брандмауэры могут быть выполнены как отдельные устройства или как программное обеспечение на самих хост-машинах. По типу брандмауэры подразделяются на брандмауэры со статической фильтрацией пакетов, прикладного уровня и с фильтрацией пакетов с учетом состояния, а выбор брандмауэров определяется конкретными потребностями и предпочтениями клиента.

Брандмауэры со статической фильтрацией пакетов анализируют входящие и исходящие пакеты и применяют набор правил для определения того, будет ли пакету разрешено проследовать брандмауэр или он будет отброшен. Такое определение, как правило, выполняется исходя из IP-адресов источника и получателя пакета, типа протокола и портов TCP источника и получателя. В зависимости от пакета и критериев, брандмауэр либо отбросит, либо переправит пакет и, возможно, создаст запись в журнале регистрации и/или подаст сигнал тревоги. Некоторые брандмауэры со статической фильтрацией пакетов могут также обеспечивать более глубокую проверку пакетов – до прикладного уровня.

Брандмауэры прикладного уровня запускают приложения от имени находящихся под их защитой машин в сети и часто называются "прокси"-брандмауэрами. При выполнении приложений брандмауэры прикладного уровня определят любое аномальное действие и в таком случае не пропустят данные на защищаемые ими машины. Брандмауэры прикладного уровня должны поддерживаться всеми необходимыми приложениями и должны запускать эти приложения от имени всех защищаемых машин. Вследствие этого, брандмауэры прикладного уровня оказывают значительное воздействие на производительность сети.

Брандмауэры, учитывающие состояние, выполняют функции фильтрации пакетов, аналогичные выполняемым брандмауэрами со статической фильтрацией пакетов, и, кроме того, сохраняют информацию о состоянии соединений трафика. Информация о состоянии позволяет брандмауэру принимать более точные решения относительно пропуска или отклонения конкретного трафика. Например, конфигурация учитывающего состояние брандмауэра может предусматривать пропуск трафика только от машин с одной стороны сети для инициирования связи. Это целесообразно, в частности, когда частные сети подсоединяются к сетям общего пользования.

При использовании брандмауэров для обеспечения дополнительной безопасности плоскости сигнализации и управления, их конфигурация должна предусматривать пропуск только полезных сигналов, относящихся к сигнализации и управлению, между некоторым набором машин. Любой другой трафик в сети, отличный от полезных сигналов, должен отклоняться, что обеспечивает уровень защиты для этих машин.

Следует отметить, что применение брандмауэров может влиять на системотехнику и результаты работы, и для некоторых приложений может потребоваться информация о наличии брандмауэров. Также следует отметить, что брандмауэры не защищают от всех атак, предпринимаемых с целью нарушения безопасности, например от имитации информации о законном пакете сигнализации.

III.3 Усиление операционной системы

Серверы и элементы сети, используемые для сигнализации и функций плоскости управления, уязвимы к любым атакам, включая следующие:

- программы проникновения "с черного хода";
- программы пассивного прослушивания сети;
- программы – захватчики и инструменты вскрытия паролей;
- использование дефектов в службах операционной системы;
- отказ в обслуживании (DoS).

В основе некоторых из этих атак лежат получившие широкую огласку методы, а доступность средств создания сценариев и других инструментов предоставляют даже не очень квалифицированным взломщикам возможность использования уязвимостей для атак на систему. После нарушение безопасности системы злоумышленник может предпринять ряд действий, в том числе:

- изменять или уничтожать информацию;
- раскрывать конфиденциальную информацию;
- устанавливать вредоносную программу для сбора информации;
- использовать пораженный сервер для атак на другие системы.

Для повышения уровня защищенности операционной системы от атак могут использоваться процедуры усиления операционной системы. Такие процедуры являются весьма полезными мерами, которые применяются в процессе выполнения инсталляции и конфигурации операционной системы. Поскольку ни одна система не является полностью защищенной, следующие процедуры усиления операционной системы сделают ее более устойчивой к атакам взломщиков, направленных на нарушение безопасности.

По существу, усиление операционной системы включает ограничение на использование служб, портов и доступ к приложениям и фалам. Усиление операционной системы включает также запуск приложений только ограниченным числом пользователей, имеющих привилегии доступа и использование только абсолютно необходимых портов и служб. Следует обращаться за консультацией к производителям операционных систем для получения новейших процедур усиления ОС и обновлений системы безопасности.

III.4 Оценка уязвимости

Целью оценки уязвимости элементов сети является обнаружение уязвимости, слабых мест и областей риска системы безопасности. Проверка на уязвимость заключается в том, чтобы вызвать отказ системы путем прерывания обслуживания, попыток обхода средств управления безопасностью, сбора конфиденциальных данных, получения незаконного доступа в систему или перехвата обслуживания или отказа в обслуживании. Оценка уязвимости может выполняться для элементов СПП, с тем чтобы обеспечить даже более высокий уровень безопасности.

Оценка уязвимости для элементов сети может выполняться на этапе проверки изделия и затем осуществляться постоянно в рамках технического обслуживания сети. Целесообразно проводить испытания на уязвимость системы безопасности на этапе проверки изделия, поскольку уже существует предварительно установленная процедура регистрации и подачи запроса на внесение изменения. Плановые регулярные оценки безопасности полезны для выявления новых угроз и уязвимостей и введения мер по смягчению последствий выявленных проблем.

III.5 Системы обнаружения проникновений

Системы обнаружения проникновений могут использоваться в целях обеспечения защиты от проникновения и неразрешенных действий. Например, системы обнаружения проникновений могут использоваться для оповещения сетевых администраторов о вероятности инцидентов в системе безопасности, таких как поражение сервера SIP или атака типа "отказ в обслуживании".

Системы обнаружения проникновений (IDS) могут быть сгруппированы в широкие категории по следующим критериям:

- обнаружение инцидентов в реальном времени или обнаружение инцидентов в автономном режиме: IDS в реальном режиме времени анализирует сетевой трафик и регистрирует происходящие события. Когда такие события происходят, трафик сети IDS записывается в реальном времени. Автономная система IDS в пакетном режиме анализирует проникновение, после того как произошел инцидент.
- Установка на базе сети или на базе хост-машины: в состав IDS на базе сети обычно входят несколько мониторов, установленные в точках на границах зон сети, где возможен контроль всего реального трафика между двумя пунктами. IDS на базе хост-машины требует установки программного обеспечения непосредственно на серверах, подлежащих защите, и контролирует сетевые соединения и действия пользователей на этих серверах.
- Реагирующие и пассивные: реагирующие IDS принимают активные меры для противодействия атакам путем изменения правил брандмауэров или фильтров маршрутизаторов или выполняют иные действия. Пассивные IDS лишь уведомляют администраторов или другие сетевые системы о возникновении проблемы.

Большинство коммерческих IDS обеспечивают сочетание возможностей контроля на базе сети и на базе хост-машин и имеют центральное устройство управления, которое принимает отчеты от различных мониторов и уведомляет об опасности сетевых администраторов.

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 M.3016.0] Рекомендация МСЭ-Т M.3016.0 (2005 г.), *Безопасность для плоскости административного управления: обзор*.

[b-ITU-T X.690] Recommendation ITU-T X.690 (2008) | ISO/IEC 8825-1:2008, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T Y.2091] Рекомендация МСЭ-Т Y.2091 (2008 г.), *Термины и определения для сетей последующих поколений.*

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

[b-3GPP TS 33.328] 3GPP TS 33.328, *IP Multimedia System (IMS) media plane security*.

[b-ETSI TS 133 220] ETSI TS 133 220 V9.2.0 (2010), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

[b-IETF RFC 1155] IETF RFC 1155 (1990), *Structure and Identification of Management Information for TCP/IP-based Internets*.

[b-IETF RFC 1212] IETF RFC 1212 (1991), *Concise MIB definitions*.

[b-IETF RFC 1215] IETF RFC 1215 (1991), *A Convention for Defining Traps for use with the SNMP*.

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[b-IETF RFC 2367] IETF RFC 2367 (1998), *PF_KEY Key Management API, Version 2*.

[b-IETF RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*.

[b-IETF RFC 2409] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

[b-IETF RFC 2451] IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms*.

[b-IETF RFC 2578] IETF RFC 2578 (1999), *Structure of Management Information Version 2 (SMIv2)*.

[b-IETF RFC 2579] IETF RFC 2579 (1999), *Textual Conventions for SMIv2*.

[b-IETF RFC 2580] IETF RFC 2580 (1999), *Conformance Statements for SMIv2*.

[b-IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*.

[b-IETF RFC 2808] IETF RFC 2808 (2000), *The SecurID® SASL Mechanism*.

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)*.

[b-IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[b-IETF RFC 3310] IETF RFC 3310 (2002), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)*.

[b-IETF RFC 3410] IETF RFC 3410 (2002), *Introduction and Applicability Statements for Internet Standard Management Framework*.

[b-IETF RFC 3411] IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*.

[b-IETF RFC 3413] IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) Applications*.

[b-IETF RFC 3414] IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

[b-IETF RFC 3415] IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.

[b-IETF RFC 3416] IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*.

[b-IETF RFC 3417] IETF RFC 3417 (2002), *Transport Mappings for the Simple Network Management Protocol (SNMP)*.

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

[b-IETF RFC 3602] IETF RFC 3602 (2003), *The AES-CBC Cipher Algorithm and Its Use with IPsec*.

[b-IETF RFC 3711] IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP)*.

[b-IETF RFC 3713] IETF RFC 3713 (2004), *A Description of the Camellia Encryption Algorithm*.

[b-IETF RFC 3830] IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing*.

[b-IETF RFC 4132] IETF RFC 4132 (2005), *Addition of Camellia Cipher Suites to Transport Layer Security (TLS)*.

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*.

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*.

[b-IETF RFC 4312] IETF RFC 4312 (2005), *The Camellia Cipher Algorithm and Its Use with IPsec*.

[b-IETF RFC 4422] IETF RFC 4422 (2006), *Simple Authentication and Security Layer (SASL)*.

[b-IETF RFC 4492] IETF RFC 4492 (2006), *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*.

[b-IETF RFC 4566] IETF RFC 4566 (2006), *SDP: Session Description Protocol*.

[b-IETF RFC 4567] IETF RFC 4567 (2006), *Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)*.

[b-IETF RFC 4568] IETF RFC 4568 (2006), *Session Description Protocol (SDP) Security Descriptions for Media Streams*.

[b-IETF RFC 4590] IETF RFC 4590 (2006), *RADIUS Extension for Digest Authentication*.

[b-IETF RFC 4648] IETF RFC 4648 (2006), *The Base16, Base32, and Base64 Data Encodings*.

[b-IETF RFC 4740] IETF RFC 4740 (2006), *Diameter Session Initiation Protocol (SIP) Application*.

[b-IETF RFC 4835] IETF RFC 4835 (2007), *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*.

[b-IETF RFC 5077] IETF RFC 5077 (2008), *Transport Layer Security (TLS) Session Resumption without Server-Side State*.

[b-IETF RFC 5090] IETF RFC 5090 (2008), *Radius Extension for Digest Authentication*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 5282] IETF RFC 5282 (2008), *Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol*.

[b-IETF RFC 5424] IETF RFC 5424 (2009), *The Syslog Protocol*.

[b-ISO/IEC 15946-1] ISO/IEC 15946-1:2008, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General*.

[b-ISO/IEC 15946-2] ISO/IEC 15946-2:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures*.

[b-ISO/IEC 15946-3] ISO/IEC 15946-3:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment*.

[b-ISO/IEC 15946-4] ISO/IEC 15946-4:2004, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 4: Digital signatures giving message recovery*.

[b-ISO/IEC 15946-5] ISO/IEC 15946-5:2008, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation*.

[b-ISO/IEC 18033-3] ISO/IEC 18033-3:2005, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*.

[b-NIST FIPS 197] NIST Federal Information Processing Standards (FIPS) 197 (2001), *Advanced Encryption Standard*.

[b-NIST FIPS 198-1] NIST Federal Information Processing Standards (FIPS) 198-1 (2008), *The Keyed-Hash Message Authentication Code (HMAC)*.

[b-NIST FIPS SP 800-38a] NIST Federal Information Processing Standards (FIPS), *Special Publication 800-38: Recommendation for Block Cipher Modes of Operations. Methods and Techniques, December 2001*.

[b-NIST SP 800-44 v2] NIST Special Publication 800-44 Version 2, *Guidelines on Securing Public Web Servers*.

[b-NIST SP 800-57] NIST Special Publication 800-57, *Recommendation on Key Management – Part 1: General (Revised)*.

[b-NIST SP 800-83] NIST Special Publication 800-83 (2005), *Guide to Malware Incident Prevention and Handling*.

[b-NIST SP 800-94] NIST Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*.

[b-TIA 683-D] TIA Standard TIA-683-D (2006), *Over the Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

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

Отпечатано в Швейцарии
Женева, 2010 г.