МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т J.262

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(10/2009)

СЕРИЯ J: КАБЕЛЬНЫЕ СЕТИ И ПЕРЕДАЧА СИГНАЛОВ ТЕЛЕВИЗИОННЫХ И ЗВУКОВЫХ ПРОГРАММ И ДРУГИХ МУЛЬТИМЕДИЙНЫХ СИГНАЛОВ

Проект IPCablecom

Описание аутентификации при преимущественной электросвязи в сетях IPCablecom2

Рекомендация МСЭ-Т J.262

Рекомендация МСЭ-Т J.262

Описание аутентификации при преимущественной электросвязи в сетях IPCablecom2

Резюме

Рекомендация МСЭ-Т J.262 относится к серии Рекомендаций, предоставляющих возможность обеспечить услуги преимущественной электросвязи в сетях IPCablecom. В ней даны описания аутентификации при преимущественной электросвязи в сетях IPCablecom2. Эти описания удовлетворяют требованиям, установленным в Рекомендации МСЭ-Т J.260. Ключевые аспекты преимущественной электросвязи в IPCablecom2 могут быть распределены по двум областям – назначению приоритета и аутентификации. В настоящей Рекомендации приводится только описание аутентификации. Аутентификация должна применяться для предотвращения несанкционированного использования услуг в IPCablecom2, предоставляемых за дополнительную плату, и услуг, предоставляемых при чрезвычайных ситуациях, в отношении которых может потребоваться преимущественное обслуживание (например, электросвязь для оказания помощи при бедствиях и услуга электросвязи в условиях чрезвычайных ситуаций).

Аутентификация пользователя является необходимой для определения того, санкционировать ли запрос на предоставление услуг преимущественной электросвязи. В настоящей Рекомендации представлены только вопросы аутентификации и не рассматривается, какие услуги разрешено использовать правомочному пользователю.

Источник

Рекомендация МСЭ-Т J.262 утверждена 30 октября 2009 года 9-й Исследовательской комиссией МСЭ-Т (2009–2012 гг.) в соответствии с Резолюцией 1 ВАСЭ.

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

СОДЕРЖАНИЕ

Введение

Электросвязь в условиях чрезвычайных ситуаций и бедствий, предназначенная для правомочных пользователей, играет жизненно важную роль в обеспечении здоровья, безопасности и благополучия народов во всех странах. Обычно в целях содействия осуществлению операций в условиях чрезвычайных ситуаций/бедствий используются гарантированные возможности в отношении ориентированных на пользователя услуг преимущественной электросвязи, которые могут быть реализованы с помощью технических решений и/или административной политики. Инфраструктура IPCablecom предоставляет важный ресурс для обеспечения гарантированной электросвязи в условиях чрезвычайных ситуаций/бедствий.

Чрезвычайные ситуации и бедствия могут оказывать воздействие на инфраструктуры электросвязи. Типичные воздействия могут включать чрезмерную нагрузку из-за перегрузки и необходимость перебазирования или расширения возможностей электросвязи сверх обеспечиваемых существующими инфраструктурами. Даже если эти ситуации не причиняют ущерб инфраструктурам электросвязи, спрос на ресурсы электросвязи резко возрастает в период этих событий. Поэтому необходимы механизмы приоритета, с тем чтобы при чрезвычайных ситуациях/бедствиях уполномоченным работникам, занятым в условиях чрезвычайных ситуаций и бедствий, могли быть распределены ограниченные ресурсы пропускной способности.

Как правило, при предоставлении возможностей электросвязи, относящихся к преимущественному или приоритетному обслуживанию, пользователи услуги будут аутентифицированы и санкционированы. Решение о том, требуются ли аутентификация и санкционирование, как и аспекты реализации, например базы данных для персональных идентификационных номеров (PIN), принимается на национальном уровне. Однако без аутентификации и санкционирования возможности преимущественного обслуживания могут стать предметом злоупотребления неправомочными лицами.

В настоящей Рекомендации содержатся описания, вытекающие из требований Рекомендации МСЭ-Т J.260 к механизмам обеспечения аутентификации в сетях IPCablecom2 для предоставления услуг преимущественной электросвязи, которые нуждаются в преимущественном обслуживании или пользуются им.

Рекомендация МСЭ-Т J.262

Описание аутентификации при преимущественной электросвязи в сетях IPCablecom2

1 Сфера применения

Настоящая Рекомендация относится к серии Рекомендаций, предоставляющих возможность обеспечить услуги преимущественной электросвязи в сетях IPCablecom. Эти описания не применяются к обычным экстренным вызовам, таким как вызовы людьми милиции, пожарных, скорой медицинской помощи и др.

Аспекты преимущественной электросвязи включают положения об аутентификации и приоритете (специальное обслуживание). Цель настоящей Рекомендации состоит в предоставлении начального набора описаний аутентификации для преимущественной электросвязи в сетях IPCablecom2 в соответствии с инфраструктурой, описанной в [ITU-T J.261]. В настоящей Рекомендации сформулированы описания возможностей, реализация которых должна содействовать обеспечению услуг преимущественной электросвязи.

ПРИМЕЧАНИЕ. – Описания, касающиеся приоритетного прерывания обслуживания, и описания санкционирования не входят в сферу применения настоящей Рекомендации и считаются вопросами, относящимися к национальной компетенции.

2 Справочные документы

Нижеследующие Рекомендации МСЭ-Т и другие ссылки содержат пункты, на которые имеются ссылки в тексте этих Рекомендаций. Во время опубликования все перечисленные издания были в силе. Все Рекомендации и другие ссылки могут пересматриваться: все пользователи настоящих Рекомендаций должны использовать возможность применения наиболее современного издания Рекомендаций и других ссылок приведенных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статуса Рекомендации.

[ITU-T J.260] Рекомендация МСЭ-Т J.260 (2005 г.), *Требования к предпочтительному использованию средств электросвязи в сетях IPCablecom*.

[ITU-T J.261] Рекомендация МСЭ-Т J.261 (2009 г.), *Структура для реализации преимущественной электросвязи в сетях IPCablecom*.

[ITU-T J.360] Recommendation ITU-T J.360 (2006), *IPCablecom2 architecture framework*.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 гарантированные возможности [ITU-T J.260]: Возможности, обеспечивающие высокую достоверность того, что критически важная связь доступна и надежно работает, или уверенность в этом.

3.1.2 аутентификация [ITU-T J.260]: Действие или метод, используемый для проверки заявляемой идентичности.

3.1.3 санкционирование [ITU-T J.260]: Действие для определения того, можно ли предоставить предъявителю конкретного полномочия конкретную привилегию, такую как доступ к ресурсам электросвязи.

3.1.4 чрезвычайная ситуация [ITU-T J.260]: Опасная ситуация, которая наступает внезапно и неожиданно. Для восстановления нормального состояния, чтобы исключить дальнейший риск для людей или имущества, могут потребоваться масштабные неотложные значительные усилия, осуществлению которых содействует электросвязь. Если эта ситуация обостряется, то она может перерасти в кризис и/или бедствие.

3.1.5 международная чрезвычайная ситуация [ITU-T J.260]: Чрезвычайная ситуация, распространившаяся за пределы международных границ, которая затрагивает несколько стран.

3.1.6 метка [ITU-T J.260]: Идентификатор, находящийся внутри элемента данных или прикрепленный к элементу данных. В рамках преимущественной электросвязи – это индикатор приоритетности. Такой идентификатор может использоваться как механизм преобразования различных уровней приоритетности в сети.

3.1.7 политика [ITU-T J.260]: Правила (или методы) распределения ресурсов сети электросвязи по типам трафика, которые могут различаться метками.

3.1.8 предпочтительная [ITU-T J.260]: Возможность, предоставляющая преимущества, по сравнению с обычными возможностями.

3.1.9 возможности приоритетного обслуживания [ITU-T J.260]: Возможности, которые обеспечивают первоочередный доступ к ресурсам сетей электросвязи и/или их использованию.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяется следующий термин:

3.2.1 признак: Признак, используемый в процессе аутентификации, представляет собой то, что знают, как например PIN, пароль или пароль-фразу, либо то, чем владеют, как например картой с магнитной полоской или меткой безопасности, или что-то уникальное (отпечаток пальца или образец голоса), что относится к лицу, идентичность которого аутентифицируется.

4 Аббревиатуры

В настоящей Рекомендации используются следующие аббревиатуры:

AS	Application Server		Сервер приложений
CM	Cable Modem		Кабельный модем
HSS	Home Subscriber Server		Домашний сервер абонента
ISTP	Internet Signalling Transport Protocol		Транспортный протокол сигнализации интернета
MTA	Media Terminal Adapter		Адаптер медиатерминала
P-CSCF	Proxy Call Session Control Function		Функции управления сеансом связи вызова – прокси-сервер
PIN	Personal Identification Number		Персональный идентификационный номер
PSTN	Public Switched Telephone Network	КТСОП	Коммутируемая телефонная сеть общего пользования
S-CSCF	Serving Call Session Control Function		Функции управления сеансом связи вызова – обслуживающий сервер
SIP	Session Initiation Protocol		Протокол инициирования сеанса связи
UA	User Agent		Агент пользователя

5 Условные обозначения

Нет.

6 Аутентификация в IPCablecom2

На аутентификацию в сетях IPCablecom2 воздействуют два параметра:

- местоположение исходящего и завершающего устройств или функциональных средств агента пользователя (UA) VoIP; и
- вид идентичности, представляемой стороной, запрашивающей услугу преимущественной электросвязи, и способ проверки предъявляемой идентичности.

Аутентификация влечет за собой получение информации об идентификации и проверке/подтверждении идентичности, необходимой до завершения санкционирования преимущественного приоритетного вызова или сеанса. Эта возможность должна существовать в сети

доступа и должна также быть распространена на все соответствующие объекты сети для предоставления по мере возможности сквозного преимущественного обслуживания. Способ предоставления сквозного преимущественного обслуживания не входит в сферу применения настоящей Рекомендации.

Следует рассмотреть следующие четыре возможности в отношении вызовов, требующих преимущественного обслуживания, которые:

1) исходят от агента UA в местоположении, санкционированном для услуг с преимущественным обслуживанием, и завершаются в UA в любом общем местоположении;
2) исходят от агента UA в местоположении, санкционированном для услуг с преимущественным обслуживанием, и завершаются в UA в местоположении, санкционированном для услуг преимущественного обслуживания;
3) исходят от агента UA в общем местоположении и завершаются в UA в местоположении, санкционированном для услуг преимущественного обслуживания;
4) исходят от агента UA в общем местоположении и завершаются в UA в любом общем местоположении.

Саму аутентификацию можно подразделить на две (или иногда три) составляющие. Первая составляющая – получение информации об идентификации, которая идентифицирует сторону, запрашивающую преимущественное обслуживание. Вторая составляющая – получение информации о проверке идентификации, которая позволяет сети проверить правильность заявленной идентичности запрашивающей стороны при направлении вызова преимущественного обслуживания, так чтобы информация могла быть распространена на все соответствующие объекты в сети при условии санкционирования вызова. Третья составляющая, необходимая при некоторых ситуациях, может потребовать подтверждения идентичности по базе данных аутентифицированных идентичностей.

Другим фактором, который может оказывать воздействие на аутентификацию, является то, будет ли санкционировано преимущественное обслуживание для доступа:

- по каждому вызову; или
- на основе абонирования.

В настоящее время идентификация и аутентификация объединены путем использования персонального идентификационного номера (PIN), представляемого вызывающим абонентом после набора номера доступа для обеспечения возможности преимущественного обслуживания. Номер PIN может быть проверен по базе данных PIN для определения санкционированных услуг. В действительности на основе PIN аутентифицируется запрашивающая сторона, а не устройство, используемое при осуществлении запроса, и, таким образом, обеспечивается возможность инициализации запросов на преимущественное обслуживание с любого устройства. Этот подход позволяет также направлять вызовы, для которых требуется преимущественное обслуживание, с телефонных устройств коммутации каналов, соединенных с системами учрежденческой связи. Метод аутентификации на основе PIN был разработан специально для запросов по каждому вызову. Инфраструктуры на базе IPCablecom2 должны обеспечивать использование этого унаследованного метода вместе с предоставлением других видов идентификации и аутентификации в отношении вызовов на основе VoIP с использованием протокола инициализации сеанса (SIP).

В Дополнении III к [ITU-T J.360] и [b-ITU-T J.366.8] описаны три механизма аутентификации с использованием SIP, указанные в [b-IETF RFC 3261]:

- использование аутентификации HTTP (п. 22), называемой также сжатой аутентификацией;
- использование безопасности транспортного уровня (п. 26.2.1) на основе TLS; и
- использование безопасности транспортного уровня (п. 26.2.1) на основе IPsec.

Идентификация вызывающей и вызываемой сторон в сети IPCablecom2 обеспечивается с помощью регистрации SIP. Аутентификация вызывающей стороны при предоставлении услуг, требующих преимущественного обслуживания, обеспечивается путем включения PIN с механизмами SIP Digest или SIP поверх TLS, или SIP поверх IPSec.

6.1 Аутентификация вызова преимущественного обслуживания на основе VoIP, направляемого UA в КТСОП, с использованием PIN в IPCablecom2

Функции агента пользователя (UA) SIP должны регистрироваться с функцией обработки вызовов IMS поставщика услуг, чтобы они могли направлять и принимать вызовы с сигнализацией на основе SIP независимо от типа вызова. На рисунке 1 показан запрос на преимущественное обслуживание с использованием аутентификации на основе PIN между UA, использующим SIP и VoIP, и устройством

в КТСОП, при котором запрашивающая сторона вызывает конкретный телефонный номер, связанный с функцией сервера приложения преимущественного обслуживания. Для регистрации вызывающего UA и вызываемого UA, а также аутентификации на основе PIN для предоставления преимущественного обслуживания выполняются следующие этапы (ряд подтверждений и других второстепенных сообщений не показан или не рассматривается). Несмотря на то что обмены сообщениями о регистрации не имеют отношения к преимущественному обслуживанию, они включены для предоставления полного порядка операций:

1) Вызывающий UA направляет сообщение REGISTER (регистрация) обслуживающей его функции P-CSCF, так же как (1) на рисунке III.4 в [ITU-T J.360].

2) Функция P-CSCF осуществляет действие, так же как (2) на рисунке III.4 в [ITU-T J.360].

3) Функция S-CSCF создает и направляет ответ 401 (несанкционирован), так же как (5) на рисунке III.4 в [ITU-T J.360].

4) Функция P-CSCF выполняет те же действия и направляет ответ 401 (несанкционирован), так же как (6) на рисунке III.4 в [ITU-T J.360].

5) Вызывающий UA выполняет те же действия, как в (7) на рисунке III.4 в [ITU-T J.360].

6) Функция P-CSCF выполняет те же действия в отношении сообщения REGISTER, так же как (8) на рисунке III.4 в [ITU-T J.360].

7) Функция S-CSCF выполняет те же действия и дает ответ 200 OK, так же как (11) на рисунке III.4 в [ITU-T J.360].

8) Функция P-CSCF переадресует 200 OK, так же как (12) на рисунке III.4 в [ITU-T J.360].

9) Вызывающий UA направляет сообщение INVITE (приглашение), маршрутизацию которого осуществляет функция сервера приложения для услуг преимущественного обслуживания (PrefTreat-AS), ответственная за инициализацию аутентификации пользователя. Это может потребовать ввода пользователем специального телефонного номера, предоставляемого вместе с PIN.

10) Сервер приложения (AS) преимущественного обслуживания направляет сообщение INVITE функции медиасервера (PrefTreat-MS), которая осуществит сбор информации о PIN пользователя и UA назначения.

11) Сервер PrefTreat-MS направляет сообщение 200 OK серверу PrefTreat-AS.

12) Сервер PrefTreat-AS направляет сообщение 200 OK вызывающему UA.

13) Вызывающий UA и сервер PrefTreat-MS могут теперь обмениваться медиатрафиком RTP для сбора информации о PIN пользователя и UA назначения, введенной пользователем.

14) Сервер PrefTreat-MS пропускает полученную информацию о PIN пользователя и UA назначения в PrefTreat-AS.

15) Сервер PrefTreat-AS направляет сообщение функции аутентификации (PrefTreat-A), которая проверит, действителен ли PIN, представленный пользователем.

16) Функция аутентификации проверит правильность PIN по разрешенному набору услуг и проинформирует сервер PrefTreat-AS о том, имеет ли пользователь право инициировать вызов, к которому применяется преимущественное обслуживание. Другой подход состоит в предоставлении серверу PrefTreat-AS информации об услугах, разрешенных для данного пользователя, а PrefTreat-AS определяет, включена ли запрашиваемая услуга в список.

17) Сервер PrefTreat-AS направляет повторное сообщение reINVITE вызывающему UA.

18) Сервер PrefTreat-AS дает разрешение серверу PrefTreat-MS и направляет сообщение BYE (прощание).

19) Вызывающий UA направляет сообщение 200 OK серверу PrefTreat-AS.

20) Сервер PrefTreat-MS направляет сообщение 200 OK серверу PrefTreat-AS.

21) Сервер PrefTreat-AS направляет сообщение INVITE в шлюз сигнализации (SG) поставщика услуг для направления сигнала в КТСОП.

22) Шлюз направляет сообщение 200 OK серверу PrefTreat-AS.

23) Сервер PrefTreat-AS направляет сообщение reINVITE (повторное приглашение) вызывающему UA.

24) Вызывающий UA направляет сообщение 200 OK серверу PrefTreat-AS.

25) Вызов с преимущественным обслуживанием теперь установлен между вызывающим UA и номером в КТСОП. Они могут обмениваться информацией, которая будет преобразовываться между средой RTP и оцифрованными аналоговыми форматами.

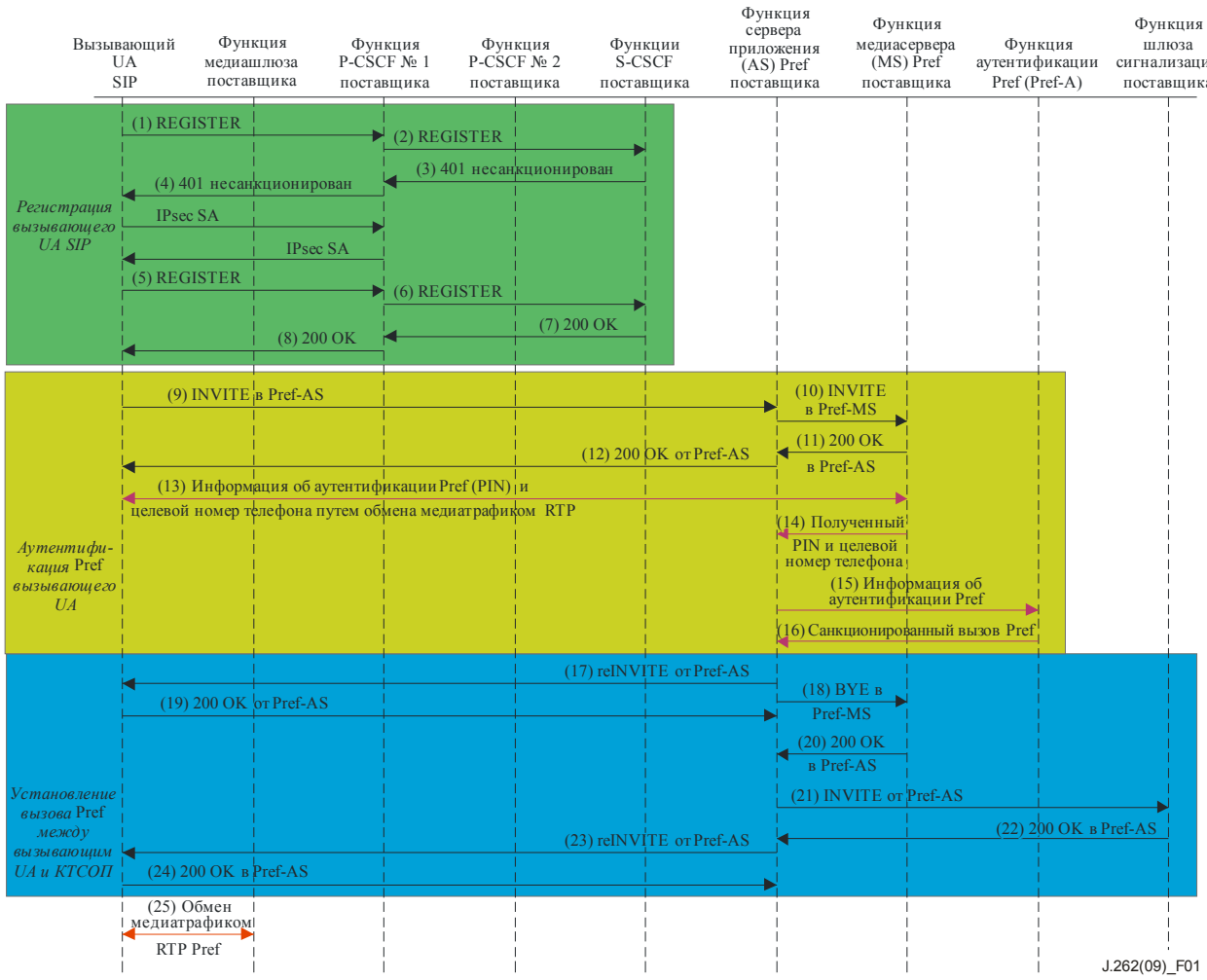

Рисунок 1 – Преимущественное обслуживание VoIP с использованием потока сообщений аутентификации на основе PIN

6.2 Вызов между двумя UA VoIP с аутентификацией на основе PIN в IPCablecom2

Функции агента пользователя (UA) SIP должны быть зарегистрированы вместе с функцией обработки вызовов IMS поставщика услуг, так чтобы они могли направлять и принимать вызовы на основе сигнализации SIP независимо от типа вызова. На рисунке 2 показан запрос на преимущественное обслуживание с использованием аутентификации на основе PIN между двумя UA, использующими SIP и VoIP, при котором сторона, запрашивающая преимущественное обслуживание, вызывает специальный телефонный номер, связанный с функцией сервера приложения преимущественного обслуживания. Для регистрации вызывающего UA, вызываемого UA и аутентификации на основе PIN выполняются следующие этапы (ряд подтверждений и других второстепенных сообщений не показан или не рассматривается). Несмотря на то что обмены сообщениями о регистрации не имеют отношения к преимущественному обслуживанию, они включены для предоставления полного порядка операций:

1) Вызывающий UA направляет сообщение REGISTER (регистрация) обслуживающей его функции P-CSCF, так же как (1) на рисунке III.4 в [ITU-T J.360].

2) Функция P-CSCF осуществляет действие, так же как (2) на рисунке III.4 в [ITU-T J.360].

3) Функция S-CSCF создает и направляет ответ 401 (несанкционирован), так же как (5) на рисунке III.4 в [ITU-T J.360].

4) Функция P-CSCF выполняет те же действия и направляет ответ 401 (несанкционирован), так же как (6) на рисунке III.4 в [ITU-T J.360].

5) Вызывающий UA выполняет те же действия, как в (7) на рисунке III.4 в [ITU-T J.360].

6) Функция P-CSCF выполняет те же действия в отношении сообщения REGISTER, так же как (8) на рисунке III.4 в [ITU-T J.360].

7) Функция S-CSCF выполняет те же действия и дает ответ 200 OK, так же как (11) на рисунке III.4 в [ITU-T J.360].

8) Функция P-CSCF переадресует 200 OK, так же как (12) на рисунке III.4 в [ITU-T J.360].

9) Так же как в п. 1, выше, но между вызываемым UA и обслуживающей его P-CSCF.

10) Так же как в п. 2, выше, но между функцией P-CSCF, обслуживающей вызываемый UA, и S-CSCF.

11) Так же как в п. 3, выше, но между функцией P-CSCF, обслуживающей вызываемый UA, и S-CSCF.

12) Так же как в п. 4, выше, но между вызываемым UA и обслуживающей его P-CSCF.

13) Так же как в п. 5, выше, но между вызываемым UA и обслуживающей его P-CSCF.

14) Так же как в п. 6, выше, но между функцией P-CSCF, обслуживающей вызываемый UA, и S-CSCF.

15) Так же как в п. 7, выше, но между функцией P-CSCF, обслуживающей вызываемый UA, и S-CSCF.

16) Так же как в п. 8, выше, но между вызываемым UA и обслуживающей его P-CSCF.

17) Вызывающий UA направляет сообщение INVITE (приглашение), маршрутизацию которого осуществляет функция сервера приложения PrefTreat (PrefTreat-AS), ответственная за инициализацию аутентификации пользователя.

18) Сервер PrefTreat-AS направляет сообщение INVITE функции медиасервера PrefTreat (PrefTreat-MS), которая осуществит сбор информации о PIN пользователя и UA назначения.

19) Сервер PrefTreat-MS направляет сообщение 200 OK серверу PrefTreat-AS.

20) Сервер PrefTreat-MS направляет сообщение 200 OK вызывающему UA.

21) Вызывающий UA и сервер PrefTreat-MS могут теперь обмениваться медиатрафиком RTP для сбора информации о PIN пользователя и UA назначения, введенной вызывающим пользователем.

22) Сервер PrefTreat-MS пропускает полученную информацию о PIN пользователя и UA назначения в PrefTreat-AS.

23) Сервер PrefTreat-AS направляет сообщение функциям аутентификации (PrefTreat-A), которая проверит, является ли действительным представленный PIN пользователя. Другой подход состоит в предоставлении серверу PrefTreat-AS информации об услугах, разрешенных для данного пользователя, а PrefTreat-AS определяет, включена ли запрашиваемая услуга в этот список.

24) Функция PrefTreat-A проинформирует сервер PrefTreat-AS о том, имеет ли пользователь право инициировать вызов, к которому применяется преимущественное обслуживание.

25) Сервер PrefTreat-AS направляет сообщение reINVITE (повторное приглашение) вызывающему UA.

26) Сервер PrefTreat-AS дает разрешение серверу PrefTreat-MS и направляет сообщение BYE (прощание).

27) Вызывающий UA направляет сообщение 200 OK серверу PrefTreat-AS.

28) Сервер PrefTreat-MS направляет сообщение 200 OK серверу PrefTreat-AS.

29) Сервер PrefTreat-AS направляет сообщение INVITE вызываемому UA.

30) Вызываемый UA направляет сообщение 200 OK серверу PrefTreat-AS.

31) Сервер PrefTreat-AS направляет сообщение reINVITE вызывающему UA.

32) Вызывающий UA направляет сообщение 200 OK серверу PrefTreat-AS.

33) Теперь между вызывающим и вызываемым агентами UA установлен вызов с преимущественным обслуживанием, и они могут обмениваться медиатрафиком RTP.

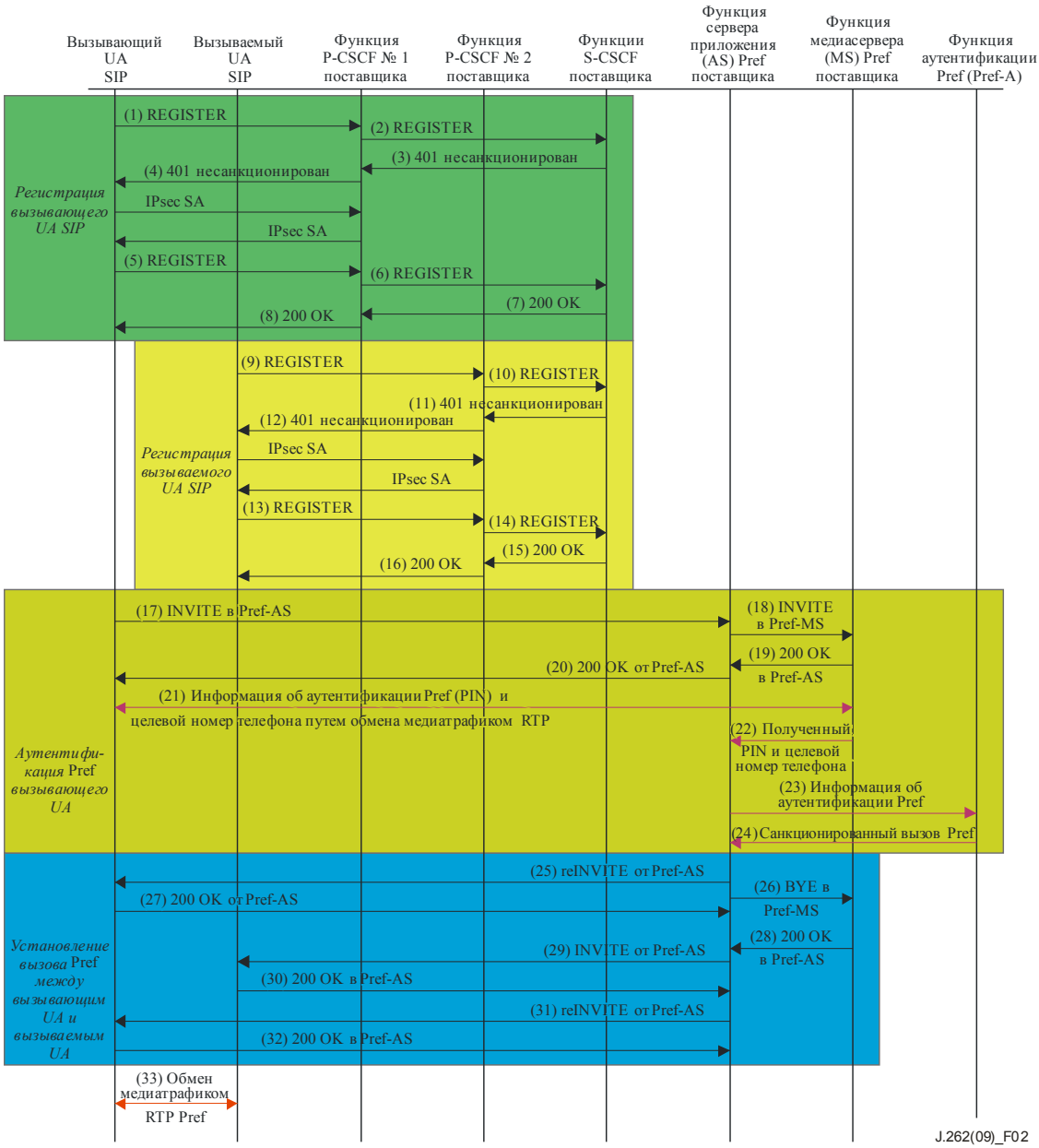

Рисунок 2 – Поток сообщений с целью аутентификации на основе PIN при преимущественном обслуживании услуг VoIP

6.3 Вызов между двумя UA VoIP с аутентификацией на основе абонирования услуг преимущественного обслуживания в IPCablecom2 – Сигнализация приоритета агентом UA с использованием заголовка R-P в сообщении INVITE

Функции агента пользователя (UA) SIP должны быть зарегистрированы вместе с функцией обработки вызовов IMS поставщика услуг, так чтобы они могли направлять и принимать вызовы на основе сигнализации SIP независимо от типа вызова. На рисунке 3 показан запрос на преимущественное обслуживание с использованием аутентификации на основе абонирования между двумя UA, использующими SIP и VoIP, при котором сторона, запрашивающая преимущественное обслуживание, вызывает специальный телефонный номер, связанный с функцией сервера приложения преимущественного обслуживания. Для регистрации вызывающего UA, вызываемого UA и аутентификации на основе PIN выполняются следующие этапы (ряд подтверждений и других второстепенных сообщений не показан или не рассматривается). Несмотря на то что обмены сообщениями о регистрации не имеют отношения к преимущественному обслуживанию, они включены для предоставления полного порядка операций:

1) Вызывающий UA направляет сообщение REGISTER (регистрация) обслуживающей его функции P-CSCF, так же как (1) на рисунке III.4 в [ITU-T J.360].

2) Функция P-CSCF осуществляет действие, так же как (2) на рисунке III.4 в [ITU-T J.360].

3) Функция S-CSCF создает и направляет ответ 401 (несанкционирован), так же как (5) на рисунке III.4 в [ITU-T J.360].

4) Функция P-CSCF выполняет те же действия и направляет ответ 401 (несанкционирован), так же как (6) на рисунке III.4 в [ITU-T J.360].

5) Вызывающий UA выполняет те же действия, так же как (7) на рисунке III.4 в [ITU-T J.360].

6) Функция P-CSCF выполняет те же действия в отношении сообщения REGISTER, как (8) на рисунке III.4 в [ITU-T J.360].

7) Функция S-CSCF выполняет те же действия и дает ответ 200 OK, так же как (11) на рисунке III.4 в [ITU-T J.360].

8) Функция P-CSCF переадресует 200 OK, так же как (12) на рисунке III.4 в [ITU-T J.360].

9) Так же как в п. 1, выше, но между вызываемым UA и обслуживающей его P-CSCF.

10) Так же как в п. 2, выше, но между функцией P-CSCF, обслуживающей вызываемый UA, и S-CSCF.

11) Так же как в п. 3, выше, но между функцией P-CSCF, обслуживающей вызываемый UA, и S-CSCF.

12) Так же как в п. 4, выше, но между вызываемым UA и обслуживающей его P-CSCF.

13) Так же как в п. 5, выше, но между вызываемым UA и обслуживающей его P-CSCF.

14) Так же как в п. 6, выше, но между функцией P-CSCF, обслуживающей вызываемый UA, и S-CSCF.

15) Так же как в п. 7, выше, но между функцией P-CSCF, обслуживающей вызываемый UA, и S-CSCF.

16) Так же как в п. 8, выше, но между вызываемым UA и обслуживающей его P-CSCF.

17) Вызывающий UA направляет сообщение INVITE (предложение), маршрутизацию которого осуществляет функция S-CSCF. Сообщение INVITE содержит заголовок R-P, указывающий на приоритетное обслуживание.

18) Функция S-CSCF запрашивает HSS для определения, разрешено ли вызывающему UA направлять вызов, относящийся к услуге преимущественного обслуживания.

19) Сервер HSS отвечает S-CSCF, что это разрешено (подтверждение) или не разрешено.

20) Функция S-CSCF направляет сообщение INVITE функции P-CSCF, обслуживающей вызываемый UA.

21) Функция P-CSCF, обслуживающая вызываемый UA, переадресует сообщение INVITE вызываемому UA.

22) Вызываемый UA направляет сообщение 200 OK функции S-CSCF.

23) Функция S-CSCF направляет сообщение 200 OK функции P-CSCF, обслуживающей вызывающий UA.

24) Функция P-CSCF, обслуживающая вызывающий UA, направляет сообщение 200 OK вызывающему UA.

25) Теперь между вызывающим и вызываемым агентами UA установлен вызов с преимущественным обслуживанием и они могут обмениваться медиатрафиком RTP.

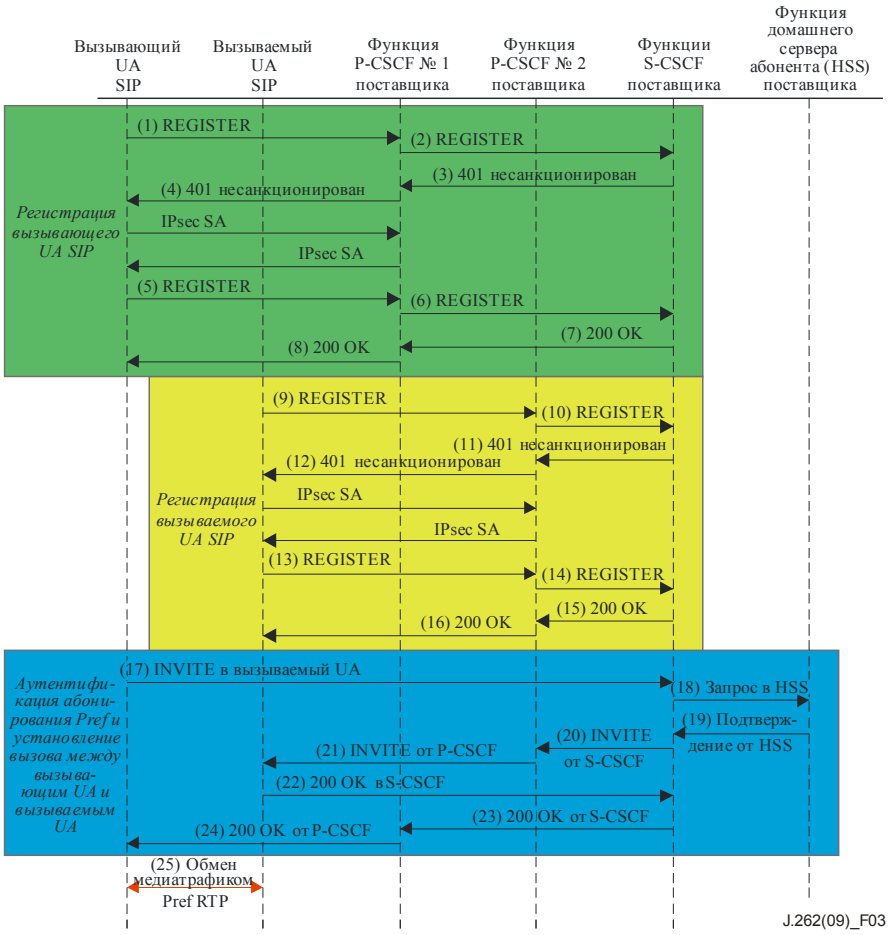

Рисунок 3 – Поток сообщений аутентификации на основе подписки при VoIP – Сигнализация приоритета агентом UA с использованием заголовка R-P в запросе INVITE

6.4 Вызов между двумя UA VoIP с аутентификацией на основе абонирования на услуги преимущественного обслуживания в IPCablecom2 – Сигнализация приоритета агентом UA с использованием идентификатора

В [b-ITU-T J.263] определены две возможности для указания того, что вызову должно быть предоставлено преимущественное обслуживание. В данном пункте агент UA направляет идентификатор, включенный в качестве инициирующего фактора в первоначальные критерии для отбора, которые содержатся в профиле пользователя. Обслуживание вызова будет таким же, как на рисунке 3 за исключением следующих шагов. Запрос в HSS для извлечения информации о профиле пользователя направляется после шага 6, на котором функция P-CSCF направляет сообщение REGISTER функции S-CSCF, а не когда получают запрос INVITE на шаге 18. Сервер HSS возвращает первоначальные критерии отбора, относящиеся к пользователю, которые включают обеспечение возможности обнаружения идентификаторов, например установление идентификационного кода со специальным номером назначения или специальным номером доступа и PIN для определения того, что пользователю требуется вызов с преимущественным обслуживанием. Шаги 18 и 19 выполняются в ходе регистрации, а не после инициализации сообщения INVITE на шаге 17. Первоначальный критерий отбора используется для определения сервера приложения преимущественного обслуживания, которому переадресуется запрос INVITE. На шаге 17 сообщение INVITE включает идентификатор в протоколе SDP вместо заголовка R-P, как в предыдущем случае. Идентификатор инициирует обработку, относящуюся к преимущественному обслуживанию, в P-CSCF, где осуществляется вставка заголовка R-P, содержащего соответствующее значение приоритета, рассматриваемое в [b-ITU-T J.263].

1) Вызывающий UA направляет сообщение REGISTER (регистрация) обслуживающей его функции P-CSCF, так же как (1) на рисунке III.4 в [ITU-T J.360]. Это сообщение содержит идентификатор, указывающий пользователя услуги преимущественной связи.

2) Функция P-CSCF осуществляет действие, так же как (2) на рисунке III.4 в [ITU-T J.360].

3) Функция S-CSCF создает и направляет ответ 401 (несанкционирован), так же как (5) на рисунке III.4 в [ITU-T J.360].

4) Функция P-CSCF выполняет те же действия и направляет ответ 401 (несанкционирован), так же как (6) на рисунке III.4 в [ITU-T J.360].

5) Вызывающий UA выполняет те же действия, как в (7) на рисунке III.4 в [ITU-T J.360].

6) Функция P-CSCF выполняет те же действия в отношении сообщения REGISTER, так же как (8) на рисунке III.4 в [ITU-T J.360].

7) Функция S-CSCF запрашивает HSS для определения, разрешено ли вызывающему UA направлять вызов, относящийся к услуге преимущественного обслуживания.

8) Сервер HSS выдает первоначальные критерии отбора, относящиеся к пользователю, если он авторизован, которые включают обеспечение возможности обнаружения идентификаторов, например установление идентификационного кода со специальным номером назначения или специальным номером доступа и PIN для определения пользователя, которому требуется вызов с преимущественным обслуживанием, или он выдает результат "несанкционирован".

9) Функция S-CSCF выдает сообщение 200 OK, так же как (11) на рисунке III.4 в [ITU-T J.360].

10) Функция P-CSCF переадресует сообщение 200 OK, так же как (12) на рисунке III.4 в [ITU-T J.360].

11) Так же как в п. 1, выше, но между вызываемым UA и обслуживающей его P-CSCF.

12) Так же как в п. 2, выше, но между функцией P-CSCF, обслуживающей вызываемый UA, и S-CSCF.

13) Так же как в п. 3, выше, но между функцией P-CSCF, обслуживающей вызываемый UA, и S-CSCF.

14) Так же как в п. 4, выше, но между вызываемым UA и обслуживающей его P-CSCF.

15) Так же как в п. 5, выше, но между вызываемым UA и обслуживающей его P-CSCF.

16) Так же как в п. 6, выше, но между функцией P-CSCF, обслуживающей вызываемый UA, и S-CSCF.

17) Так же как в п. 9, выше, но между функцией P-CSCF, обслуживающей вызываемый UA, и S-CSCF.

18) Так же как в п. 10, выше, но между вызываемым UA и обслуживающей его P-CSCF.

19) Вызывающий UA направляет сообщение INVITE с идентификатором преимущественного пользователя, которое маршрутизируется в S-CSCF.

20) Функция S-CSCF направляет сообщение INVITE функции P-CSCF, обслуживающей вызываемый UA.

21) Функция P-CSCF, обслуживающая вызываемый UA, переадресует сообщение INVITE вызываемому UA.

22) Вызываемый UA направляет сообщение 200 OK функции S-CSCF.

23) Функция S-CSCF направляет сообщение 200 OK функции P-CSCF, обслуживающей вызывающий UA.

24) Функция P-CSCF, обслуживающая вызывающий UA, направляет сообщение 200 OK вызывающему UA.

25) Теперь между вызывающим и вызываемым агентами UA установлен вызов с преимущественным обслуживанием, и они могут обмениваться медиатрафиком RTP.

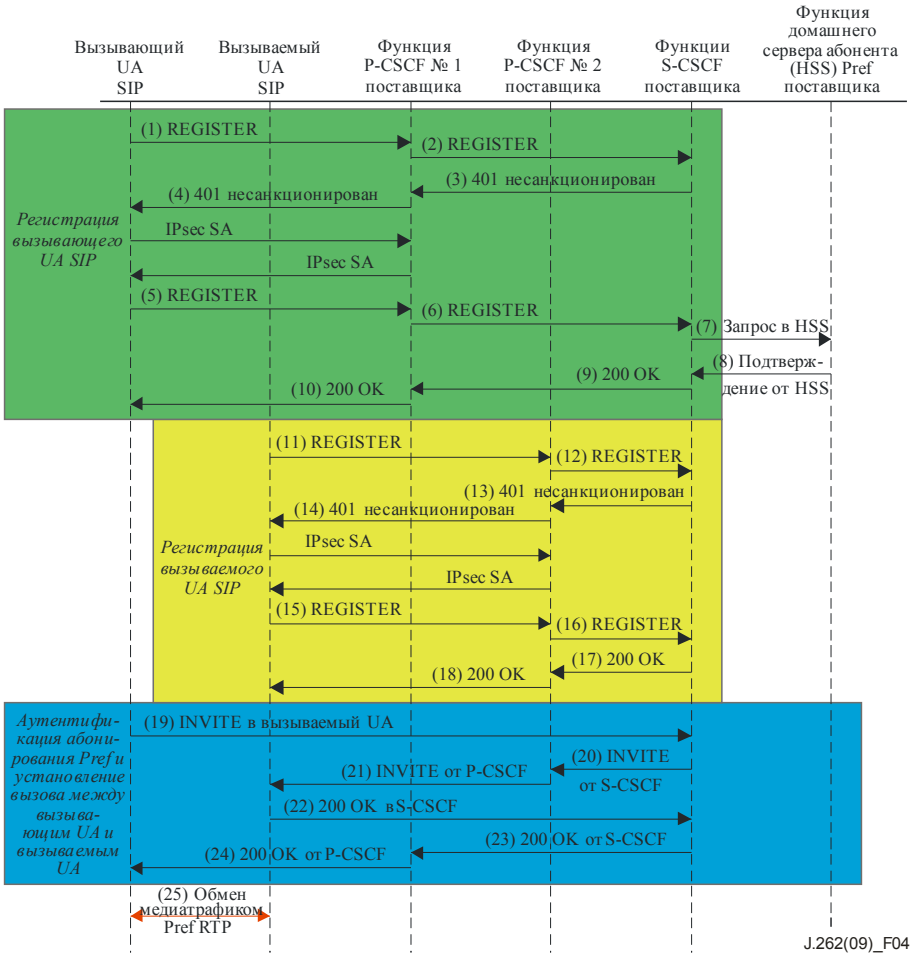

Рисунок 4 – Поток сообщений аутентификации на основе подписки при VoIP – Сообщение о приоритете, осуществляемое агентом UA с использованием идентификатора

7 Требования к аутентификации услуг преимущественной электросвязи в IPCablecom2

Ниже приводятся конкретные требования к аутентификации сеансов преимущественной электросвязи в рамках архитектуры IPCablecom2.

При использовании различного оборудования пользователя имена пользователей и пароли должны надежно храниться в нем так, чтобы опасность была сведена к минимуму. Если используется этот подход, то оборудование пользователя должно напоминать пользователям о необходимости ввести имя пользователя и пароль.

Библиография

[b-ITU-T E.106] Рекомендация МСЭ-Т E.106 (2003 г.), *Международная схема аварийных приоритетов (IEPS) для операций по ликвидации последствий чрезвычайных ситуаций*.

[b-ITU-T J.263] Recommendation ITU-T J.263 (2009), *Specification for priority in preferential telecommunications over IPCablecom2 networks*.

[b-ITU-T J.366.8] Recommendation ITU-T J.366.8 (2006), *IPCablecom2 IP Multimedia Subsystem (IMS); Network domain security specification*.

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

[b-ITU-T Y.1271] Рекомендация МСЭ-Т Y.1271 (2004 г.), *Концептуальные требования и сетевые ресурсы для обеспечения экстренной связи по сетям связи, находящимся в стадии перехода от коммутации каналов к коммутации пакетов*.

[b-ITU-T Y.2205] Рекомендация МСЭ-Т Y.2205 (2008 г.), *Сети последующего поколения – Электросвязь в чрезвычайных ситуациях – Технические соображения*.

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

[b-IETF RFC 2560] IETF RFC 2560 (1999), *Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*.

[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 3550] IETF RFC 3550 (2003), *Transport protocol for Real-Time Applications.*

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

[b-IETF RFC 4120] IETF RFC 4120 (2005), *The Kerberos Network Authentication Service (V5)*.

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

[b-IETF RFC 4302] IETF RFC 4302 (2005), *IP Authentication Header*.

[b-IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP).*

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

[b-IETF RFC 4346] IETF RFC 4346 (2006), *The Transport Layer Security (TLS) Protocol Version 1.1*.

[b-IETF RFC 4513] IETF RFC 4513 (2006), *Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms.*

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.