

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2741

(01/2011)

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

Сети последующих поколений – Безопасность

Архитектура безопасных мобильных финансовых транзакций в сетях последующих поколений

Рекомендация МСЭ-Т Y.2741

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

**ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ
ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ**

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

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

Рекомендация МСЭ-Т Y.2741

Архитектура безопасных мобильных финансовых транзакций в сетях последующих поколений

Резюме

В Рекомендации МСЭ-Т Y.2741 определяется общая архитектура решения в области безопасности для мобильной коммерции и мобильного банкинга в условиях СПП. В ней описываются основные участники, их роли и сценарии эксплуатации систем мобильной коммерции и мобильного банкинга. В ней также представлены примеры моделей реализации систем мобильной коммерции и мобильного банкинга.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т Y.2741	28.01.2011 г.	13-я

Ключевые слова

Мобильный банкинг, мобильная коммерция, мобильные платежи, дистанционные платежи, защита и безопасность.

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

© ITU 2011

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

Содержание

	Стр.
1 Сфера применения	1
2 Справочные документы	1
3 Определения	1
3.1 Термины, определенные в других документах	1
3.2 Термины, определенные в настоящей рекомендации	1
4 Сокращения и акронимы	2
5 Условные обозначения	2
6 Роли, риски, участники и сценарии мобильных платежей в СПП	2
6.1 Роли в системах мобильной коммерции и мобильного банкинга	2
6.2 Риски в СМП и уровни безопасности СМП	3
6.3 Участники и архитектура системы мобильной коммерции и мобильного банкинга	3
6.4 Сценарии использования системы мобильных платежей	5
7 Переход от систем оплаты с помощью денежных и неденежных знаков	16
Дополнение I – Регистрация платежного инструмента в системе	17
Дополнение II – Модели реализации системы мобильного банкинга и мобильной коммерции	19
II.1 Реализация системы без использования клиентского приложения	20
II.2 Реализация системы с использованием клиентского приложения	20
Библиография	22

Архитектура безопасных мобильных финансовых транзакций в сетях последующих поколений

1 Сфера применения

В настоящей Рекомендации определяется архитектура безопасности, относящаяся к дистанционным мобильным финансовым транзакциям в СПП. В ней не охватываются все другие финансовые транзакции, а также транзакции, при которых для перечисления сумм используются денежные или неденежные знаки.

Благодаря организации широкого спектра услуг с гибкими функциями управления и персонализации, СПП могут обеспечивать удобный доступ к услугам системы мобильных платежей (MPS).

2 Справочные документы

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

[ITU-T Y.2740] Рекомендация МСЭ-Т Y.2740 (2011 г.), *Требования к безопасности мобильных дистанционных финансовых транзакций в сетях последующих поколений.*

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 сеть последующих поколений (СПП) (next generation network (NGN)) [b-ITU-T Y.2001]: Сеть с пакетной коммутацией, пригодная для предоставления услуг электросвязи и для использования нескольких широкополосных технологий транспортировки с включенной функцией QoS, в которой связанные с обслуживанием функции не зависят от примененных технологий, обеспечивающих транспортировку. Она обеспечивает свободный доступ пользователей к сетям и конкурирующим поставщикам услуг и/или выбираемым ими услугам. Она поддерживает универсальную подвижность, которая обеспечивает постоянное и повсеместное предоставление услуг пользователям.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 приложение (application): Специальное приложение мобильного банкинга или мобильной коммерции, закачанное в мобильное устройство клиента (пользователя).

3.2.2 банковский счет (bank account): Электронный денежный счет, который принадлежит физическому или юридическому лицу, в банке или другом финансовом учреждении, уполномоченном национальным денежно-кредитным учреждением страны (например, центральным банком), и который может использоваться для оплаты товаров и услуг.

3.2.3 клиент (client): Физическое или юридическое лицо, подписавшее договорное соглашение об использовании услуг электросвязи и системы мобильной коммерции.

3.2.4 финансовая транзакция (financial transaction): Событие или условие, охватываемое рамками контракта между покупателем и продавцом по обмену актива на платеж.

3.2.5 межсистемная среда (intersystem environment): Набор правил или система, которые дают возможность обеспечивать взаимодействие различных систем мобильного банкинга и мобильной коммерции.

3.2.6 мобильное устройства (mobile device): Электронное устройство, используемое для электросвязи по беспроводной сети СПП.

3.2.7 мобильная финансовая транзакция (mobile financial transaction): Финансовая транзакция, инициируемая и/или авторизуемая с использованием мобильного устройства.

3.2.8 система мобильных платежей (СМП) (mobile payment system (MPS)): Системы мобильного банкинга и/или мобильной коммерции.

3.2.9 денежный знак (monetary token): Электронное или физическое средство, используемое для платежей, которое представляется и измеряется в единицах национальной валюты страны, но при этом не хранится на банковском счете и напрямую не связано с ним.

Примером электронного денежного знака являются электронные деньги, которые хранятся в отдельном электронном кошельке, не отражающемся на банковском счете. Примерами физических денежных знаков являются монеты, банкноты, дорожные чеки и т. д.

3.2.10 неденежный знак (non-monetary token): Электронное или физическое средство, используемое для платежей, но которое не представляется в единицах национальной валюты. Примером электронных неденежных знаков являются неиспользованные "минуты" или "SMS-сообщения", которые хранятся на счетах абонента СПП и которые операторы СПП позволяют перечислять с одного счета абонента на другой.

3.2.11 идентификатор платежа (payment ID): Необходимый параметр запроса, который однозначным образом определяет получателя платежа. При внедрении межсистемной среды должны быть представлены идентификатор торгово-сервисного предприятия и идентификатор системы мобильных платежей (СМП) (уникальный идентификатор системы мобильных платежей).

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

DB	DataBase	БД	База данных
ID	Identification		Идентификатор
IS	Information System	ИС	Информационная система
MPS	Mobile Payment System	СМП	Система мобильных платежей
NGN	Next Generation Network	СПП	Сеть последующих поколений

5 Условные обозначения

Нет.

6 Роли, риски, участники и сценарии мобильных платежей в СПП

6.1 Роли в системах мобильной коммерции и мобильного банкинга

Основные роли участников СМП и их ответственность являются следующими:

- Клиент – абонент мобильной связи, обладающий платежным инструментом для совершения платежных операций.
- Клиентское приложение – специальное программное обеспечение, закачанное в мобильное устройство клиента (телефон, SIM-карту, устройство персональной связи и т. п.) и предназначенное для безопасного совершения мобильных платежных операций.
- Платежный инструмент – финансовый инструмент, используемый для осуществления платежей за товары и услуги.

- Оператор СПП обеспечивает сеть подвижной связи для дистанционного взаимодействия клиента с СМП, маршрутизации и передачи данных.
- Дистрибьютор клиентских приложений – участник, который обеспечивает, чтобы у клиентов были в наличии приложения.
- Поставщик услуг по безопасности – участник, который обеспечивает безопасную передачу данных по каналам связи.
- Оператор СМП (поставщик услуг, платежный шлюз) – участник, который обеспечивает взаимодействие в СМП и предоставляет конечному пользователю услуги по платежам.
- Эмитент – финансовое учреждение, которое осуществляет эмиссию платежных инструментов.
- Поставщик услуг по аутентификации клиента – подтверждает действительность операций клиента.
- Эквайер – финансовое учреждение, которое поддерживает договорные отношения с торгово-сервисным предприятием и через которое проходят все финансовые транзакции торгово-сервисного предприятия.
- Платежная система – организация, которая обеспечивает проведение межбанковских платежных транзакций.

6.2 Риски в СМП и уровни безопасности СМП

В настоящем разделе описываются основные риски информационной безопасности, которые могут возникнуть при проведении (т. е. при осуществлении) дистанционных мобильных платежей. Эти риски включают в том числе:

- Риск потери конфиденциальности – доступ несанкционированных третьих сторон к конфиденциальной информации.
- Риск нарушения целостности – искажение информации в процессе передачи или обработки.
- Риск подделки электронных документов – документ создается не имеющей на это разрешения стороной.
- Риск отказа от авторства – отказ от авторства электронного документа.
- Риск уничтожения информации, умышленно или по неосторожности.
- Транзакционный риск – невозможность завершить транзакцию (например, вследствие неустойчивой мобильной связи).
- В зависимости от внедренных механизмов безопасности, которые основываются на существующих рисках, имеются системы с четырьмя уровнями безопасности [ITU-T Y.2740].

6.3 Участники и архитектура системы мобильной коммерции и мобильного банкинга

Архитектура СМП должна соответствовать уже существующей системе взаимоотношений финансовых, юридических и коммерческих организаций и позволять участникам системы выполнять мобильные платежные транзакции с необходимой степенью безопасности, которая основана на предполагаемом уровне риска. Предлагаемая архитектура должна поддерживать схемы и спецификации осуществления платежных транзакций, которые уже используются участниками.

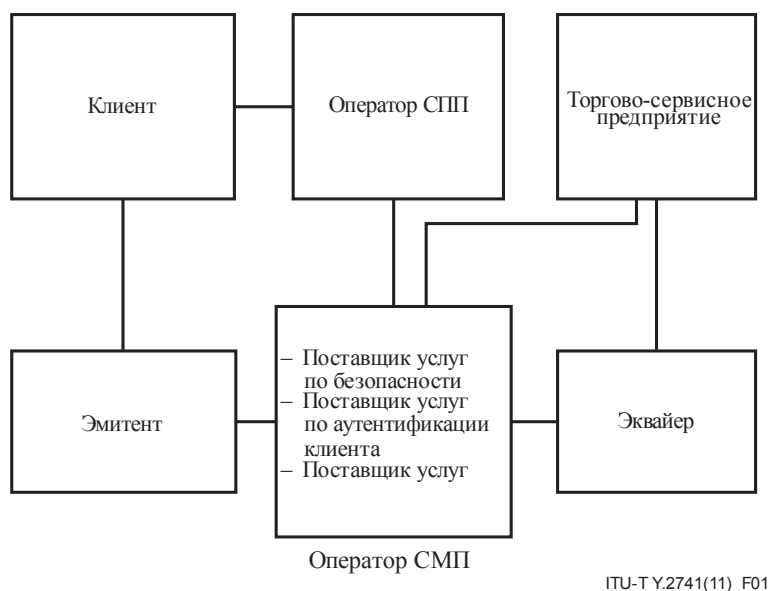


Рисунок 1 – Участники и архитектура системы мобильной коммерции и мобильного банкинга

Таблица 1 – Участники системы мобильных платежей

Участник	Описание, проблемы (цель, задача, интерес)	Роль
Клиент	Физическое или юридическое лицо, подписавшее договорное соглашение об использовании услуг электросвязи и системы мобильной коммерции. Имеет мобильное устройство и платежный инструмент. Основные проблемы: увеличение количества услуг, получение возможности осуществлять безопасные дистанционные финансовые транзакции, расширение сферы применения платежных инструментов.	Клиент
Оператор СПП	Учреждение, которое предоставляет клиенту услуги цифровой связи. Основные проблемы: увеличение числа клиентов, расширение диапазона предоставляемых услуг, увеличение трафика.	Оператор СПП
Оператор СМП	Учреждение, которое обеспечивает безопасное дистанционное взаимодействие финансовых структур, клиента и оператора СПП в рамках системы мобильных платежей. Основные проблемы: создание обширной сети мобильной коммерции, увеличение числа участников, а также количества дистанционных транзакций, обеспечение максимальной безопасности операций.	Поставщик услуг по безопасности, поставщик услуг, поставщик услуг по аутентификации клиента
Эмитент	Финансово-правовое учреждение, осуществляющее эмиссию и обслуживание платежных инструментов. Основные проблемы: расширение использования эмитированных платежных инструментов, увеличение числа клиентов.	Эмитент
Эквайер	Финансово-правовое учреждение, которое принимает платежи за продукты или услуги от имени торгово-сервисного предприятия. Основные проблемы: увеличение количества транзакций обслуживаемых торгово-сервисных предприятий.	Эквайер

Таблица 1 – Участники системы мобильных платежей

Участник	Описание, проблемы (цель, задача, интерес)	Роль
Торгово-сервисное предприятие	Юридическое лицо, предоставляющее товары или услуги и получающее оплату от клиента. Основные проблемы: рекламирование товаров и услуг, увеличение числа клиентов, увеличение числа возможных способов оплаты товаров и услуг.	Торгово-сервисное предприятие

Участники могут совмещать роли в зависимости от реализации архитектуры.

Для достижения требуемого уровня безопасности, изложенного в [ITU-T Y.2740] может потребоваться введение ролей клиентского приложения, дистрибьютора клиентских приложений или обеих ролей одновременно. Клиентское приложение закачивается в мобильные устройства клиента. Роль дистрибьютора клиентских приложений может выполняться оператором СПП, оператором мобильных платежей или третьей стороной.

При использовании в качестве платежных инструментов карточек международных платежных систем важную роль играет система платежей.

6.4 Сценарии использования системы мобильных платежей

6.4.1 Базовые сценарии использования

6.4.1.1 Регистрация клиента в СМП

Цель: подписать клиента на услугу в СМП.

Базовые роли: их цели и задачи

Клиент: получить возможность пользоваться услугами СМП.

Оператор СМП: зарегистрировать нового клиента в СМП.

Максимальные гарантии

Регистрируется согласие клиента с условиями СМП.

Клиент регистрируется в ИС оператора СМП.

Клиент получает код активации.

Минимальные гарантии

Клиенту отказывают в регистрации с указанием причины отказа.

Оператор СМП записывает информацию об отказе в регистрации клиента.

Исходные данные сценария

В СМП отсутствует активная учетная запись клиента: клиент не зарегистрирован в СМП или его учетная запись была ранее удалена.

Базовые шаги сценария

- 1 Клиент инициирует регистрацию:
 - а) в офисе оператора СМП;
 - б) с использованием веб-интерфейса: клиент авторизуется на веб-сайте оператора СМП, и направляется запрос на регистрацию.
- 2 Клиент аутентифицируется в СМП.
- 3 ИС оператора СМП включает в БД данные и учетную запись клиента.

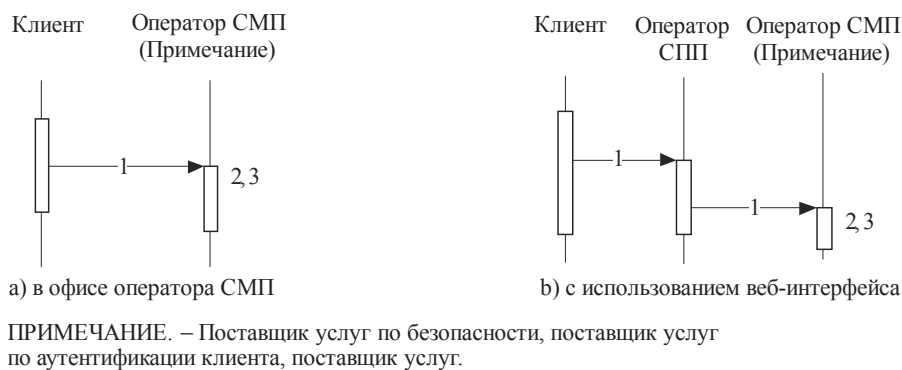


Рисунок 2 – Регистрация клиента в СМП

Альтернативные шаги сценария

3a Клиент уже зарегистрирован в СМП (есть активная учетная запись)

ИС оператора СМП информирует клиента, что услуга была подключена ранее.

3b У клиента есть счет в СМП, но он заблокирован

ИС оператора СМП активирует счет клиента.

3c ИС оператора СМП отказывает в регистрации

а) ИС оператора СМП записывает информацию о попытке подключения услуги клиенту.

б) ИС оператора СМП информирует клиента об отказе в подключении услуги и указывает причины.

6.4.1.2 Регистрация платежного инструмента, которая должна использоваться в СМП

Клиенту следует зарегистрировать свой платежный инструмент. В процессе регистрации следует соблюдать следующие условия:

- Клиенту следует подтвердить полномочия на использование регистрируемого платежного инструмента.
- В процессе регистрации платежного инструмента в БД оператора СМП следует сохранить минимально необходимое количество параметров для осуществления транзакции дистанционного платежа.
- Параметры платежного инструмента следует надежно хранить оператору СМП таким образом, который исключает несанкционированный доступ и делает невозможным проведение финансовых транзакций, которые не были санкционированы клиентом.

Средства подключения платежного инструмента описаны в Дополнении I.

6.4.1.3 Осуществление клиентом финансовых операций в домашней зоне в рамках собственной системы платежей

Цель: предоставить клиенту возможность пользоваться финансовыми услугами СМП.

Базовые роли: их цели и задачи

Клиент: пользоваться услугами, дистанционно предоставляемыми торгово-сервисным предприятием.

Оператор мобильной связи: передавать сообщения по каналам связи.

Оператор СМП – предоставить клиенту возможность оплачивать товары и услуги с применением СМП.

Торгово-сервисное предприятие: предоставлять дистанционные услуги клиенту.

Эмитент: предоставить авторизацию для платежной операции клиента и инициировать расчеты.

Эквайер: передать ответ с авторизацией на операции торгово-сервисного предприятия.

Максимальные гарантии

Клиент оплачивает услугу торгово-сервисного предприятия.

Торгово-сервисное предприятие предоставляет услугу.

Минимальные гарантии

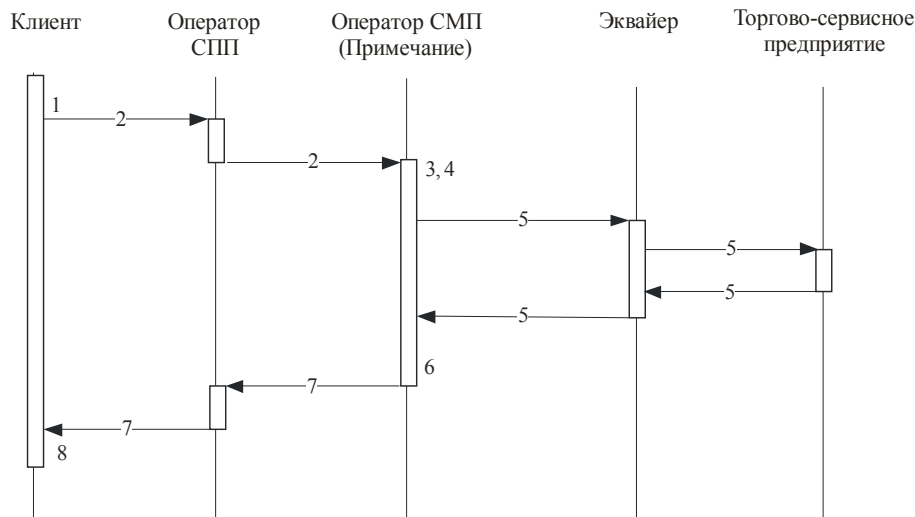
Клиенту отказывают в оплате товаров и услуг оператора СМП.

Исходные данные сценария

Клиент зарегистрирован в СПМ и имеет платежный инструмент, зарегистрированный в СМП.

Базовые шаги сценария

- 1 Клиент с помощью своего мобильного устройства составляет запрос, содержащий параметры финансовой операции и платежного инструмента.
- 2 Запрос передается по каналам связи оператора СПП.
- 3 Оператор СМП получает запрос.
- 4 Клиент аутентифицирован.
- 5 Проводится требуемая финансовая операция (перевод денег/платеж) с использованием реквизитов платежного инструмента клиента.
- 6 Результат выполнения операции отправляется клиенту.
- 7 Ответ передается по каналам связи оператора СПП.
- 8 Клиент получает результат выполнения финансовой операции.



ПРИМЕЧАНИЕ. – Поставщик услуг по безопасности, поставщик услуг по аутентификации клиента, поставщик услуг.

ITU-T Y.2741(11)_F03

Рисунок 3 – Осуществление клиентом финансовых операций

Альтернативные шаги сценария

6 Клиент не аутентифицирован

7 Финансовая операция невозможна

- a) Выполняется откат транзакции.
- b) Результат выполнения операции возвращается клиенту.

Альтернативный сценарий: торгово-сервисное предприятие инициирует платеж

Базовые шаги сценария являются следующими

- 1 a) Торгово-промышленное предприятие составляет предложение произвести платеж и направляет его оператору СМП.
- b) Оператор СМП определяет клиента и способ доставки ему предложения произвести платеж.
- c) Запрос направляется клиенту по каналам связи оператора СПП.
- 2 Клиент получает запрос по своему мобильному устройству и составляет ответ, содержащий параметры финансовой операции и платежного инструмента.
- 3 Запрос передается по каналам связи оператора СПП.
- 4 Оператор СМП получает запрос клиента.
- 5 Аутентификация клиента.
- 6 Осуществляется требуемая финансовая операция (перевод денег/платеж) с использованием реквизитов платежного инструмента клиента.
- 7 Результат выполнения операции отправляется клиенту.
- 8 Ответ передается по каналам связи оператора СПП.
- 9 Клиент получает результат выполнения финансовой операции.

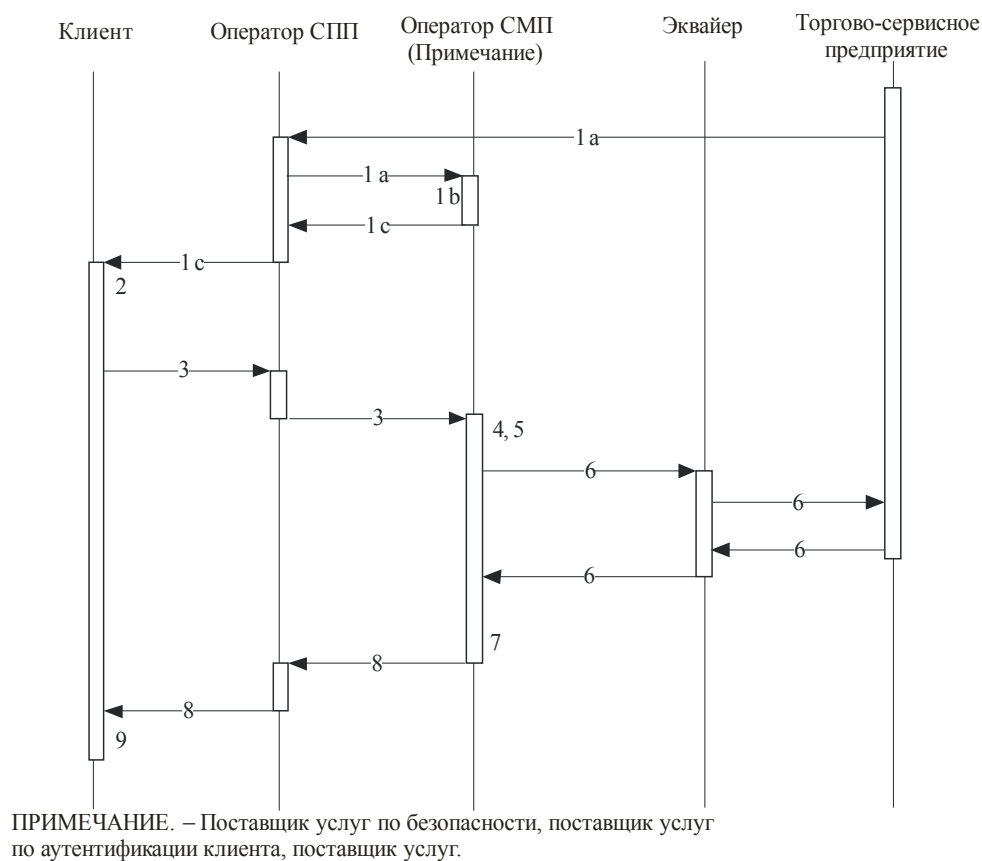


Рисунок 4 – Осуществление платежей, инициированных торгово-сервисным предприятием

6.4.1.4 Отключение платежного инструмента в СМП

Цель: предоставить клиенту возможность удалить из СМП данные о платежном инструменте.

Базовые роли: их цели и задачи

Клиент: отключить платежный инструмент в СМП.

Оператор мобильной связи: передать сообщение по каналам связи.

Оператор СМП: предоставить клиенту возможность отключить платежный инструмент.

Максимальные гарантии

Клиент отключает платежный инструмент в СМП.

Минимальные гарантии

Клиент не может отключить платежный инструмент.

Исходные данные сценария

Клиент зарегистрирован в СМП и имеет подключенный платежный инструмент.

Базовые шаги сценария

- 1 Клиент с помощью своего мобильного устройства составляет запрос на отключение определенного платежного инструмента.
- 2 Запрос передается по каналам связи оператора СПП.
- 3 Оператор СМП получает запрос.

- 4 СМП аутентифицирует клиента.
- 5 Платежный инструмент исключается из БД ИС.
- 6 Результат отключения платежного инструмента отправляется клиенту.
- 7 Ответ передается по каналам связи оператора СПП.
- 8 Клиент получает результат выполнения операции.

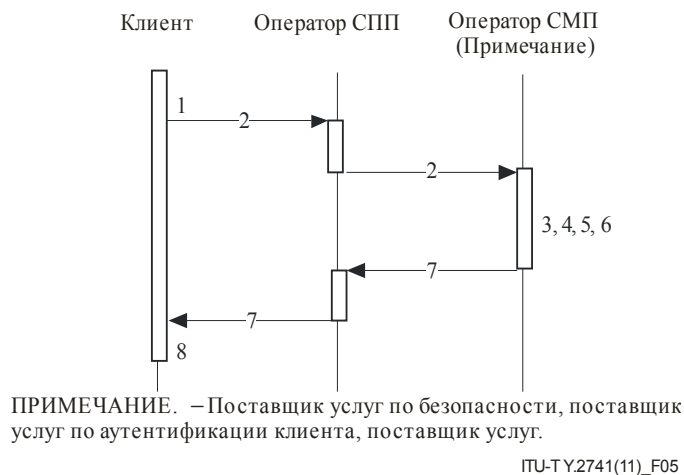


Рисунок 5 – Отключение платежного инструмента в СМП

Альтернативные шаги сценария

7 Отказ в отключении платежного инструмента в СМП

- а) ИС оператора СМП информирует клиента о невозможности отключения платежного инструмента.

6.4.1.5 Отключение клиента от СМП

Цель: отключить клиента от услуг СМП.

Базовые роли: их цели и задачи

Клиент: отказаться от использования услуг СМП.

Оператор СМП: сделать услуги недоступными для клиента.

Максимальные гарантии

Регистрируется факт отказа клиента от услуг СМП.

Услуги СМП становятся недоступными для клиента.

Минимальные гарантии

Клиенту отказывают в отключении от услуг с указанием причины отказа.

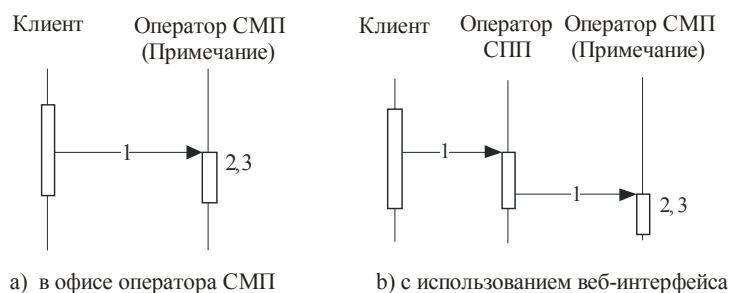
Клиент аннулирует отключение от услуг СМП.

Исходные данные сценария

Клиент зарегистрирован в СМП.

Базовые шаги сценария

- 1 Клиент инициирует отключение от услуг:
 - в офисе оператора СМП;
 - с использованием веб-интерфейса: клиент авторизуется на веб-сайте оператора СМП и распоряжается отключить услугу.
- 2 Клиент аутентифицируется в СМП.
- 3 ИС оператора СМП вносит изменения в статусе клиента в БД (учетная запись блокируется).
- 4 Клиент не может пользоваться услугами СМП без повторной регистрации.



ПРИМЕЧАНИЕ. – Поставщик услуг по безопасности, поставщик услуг по аутентификации клиента, поставщик услуг.

ITU-T Y.2741(11)_F06

Рисунок 6 – Отключение клиента от СМП

Альтернативные шаги сценария

1 В СМП используется платежное приложение

Клиент инициирует отключение от СМП в приложении.

3 Клиент не может отключиться от услуг СМП

ИС оператора СМП информирует клиента о том, что услуга в настоящий момент не может быть отключена.

6.4.2 Сценарий использования с платежным приложением

6.4.2.1 Получение платежного приложения

Цель: предоставить клиенту возможность использовать приложение в СМП.

Базовые роли: их цели и задачи

Клиент: получить платежное приложение для использования в мобильном устройстве.

Дистрибьютор клиентских приложений: предоставить клиенту приложение.

Максимальные гарантии

Клиент получает приложение.

Минимальные гарантии

Клиенту отказывают в предоставлении приложения.

Клиент не имеет возможности использовать полученное приложение из-за некоторых технических характеристик мобильного устройства.

Исходные данные сценария

Клиент зарегистрирован в СМП и имеет техническую возможность использовать приложение.

Базовые шаги сценария

- 1 Клиент получает приложение от дистрибьютора клиентских приложений:
 - в офисе дистрибьютора клиентских приложений;
 - с использованием веб-интерфейса (на веб-сайте дистрибьютора клиентских приложений).
- 2 Клиент получает возможность использовать приложение на своем мобильном устройстве.

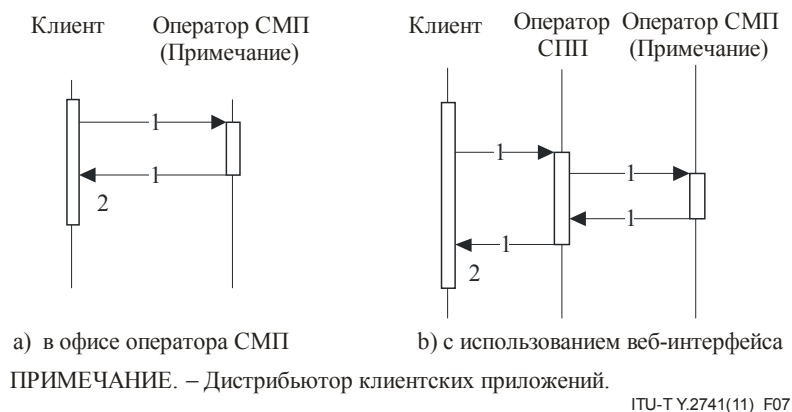


Рисунок 7 – Получение платежного приложения

Альтернативные шаги сценария

1а Клиент получает обновленную версию приложения

Клиент получил приложение раньше.

1б Клиент не получает приложение

Клиент обращается за помощью в службу поддержки дистрибьютора клиентских приложений.

6.4.2.2 Активации платежного приложения

Цель: активировать платежное приложение клиента.

Базовые роли: их цели и задачи

Клиент: получить возможность пользоваться услугами СМП с помощью приложения.

Оператор СМП: утвердить использование данного платежного приложения в СМП данным клиентом.

Оператор мобильной связи: передать сообщение по каналам связи.

Максимальные гарантии

Клиент активирует приложение.

Ключи клиента загружаются в приложение.

Ключи клиента заносятся в БД ИС оператора СМП.

Минимальные гарантии

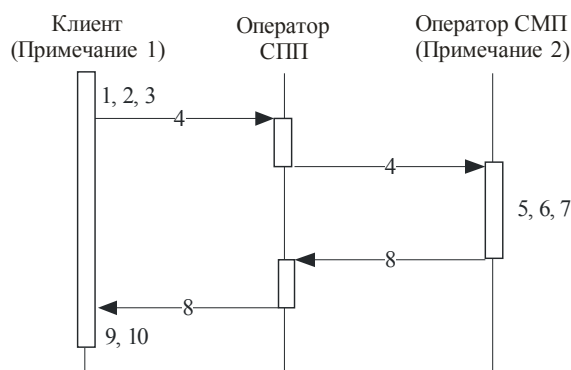
Клиенту отказывают в активации приложения с указанием причины отказа.

Исходные данные сценария

Клиент зарегистрирован в СМП, имеет код активации и приложение в мобильном устройстве.

Базовые шаги сценария

- 1 Клиент выбирает в меню приложения позицию "активация".
- 2 Клиент вводит в приложение код активации, полученный при процедуре регистрации.
- 3 Приложение составляет и отправляет запрос в СМП.
- 4 Запрос передается по каналам связи оператора СПП.
- 5 Оператор СМП получает запрос. Проверяется код активации.
- 6 Создаются ключи клиента, которые сохраняются в БД ИС оператора СМП.
- 7 Ключи и результат выполнения активации отправляются клиенту.
- 8 Ответ передается по каналам связи оператора СПП.
- 9 Приложение клиента получает сообщение, сохраняет ключи клиента, и клиенту выводится на экран результат выполнения активации.
- 10 Клиент получает доступ к услугам СМП в приложении.



ПРИМЕЧАНИЕ 1. – Клиент, платежный документ, платежное приложение .

ПРИМЕЧАНИЕ 2. – Поставщик услуг по безопасности, поставщик услуг по аутентификации клиента, поставщик услуг .

ITU-T Y.2741(11)_F08

Рисунок 8 – Активации платежного приложения

Альтернативные шаги сценария

5 Ошибка проверки кода активации

- а) ИС оператора СМП информирует клиента, что код активации введен неправильно.
- б) Счет клиента блокируется, если превышен лимит попыток ввода кода активации.

6.4.3 Сценарии использования межсистемного взаимодействия

В настоящей Рекомендации рассматриваются общие вопросы и предлагаются базовые сценарии взаимодействия.

6.4.3.1 Осуществление финансовых транзакций, когда клиент пользуется роумингом

Цель: предоставить клиенту возможность пользоваться подключенной услугой СМП, находясь вне зоны покрытия оператора (домашней зоны).

Базовые роли: их цели и задачи

Клиент: получить возможность оплачивать услуги с использованием СМП, находясь за пределами домашней зоны.

Оператор мобильной связи: передать сообщение по каналам связи.

Оператор СМП: предоставить клиенту возможность оплачивать товары и услуги с помощью СМП.

Торгово-сервисное предприятие: предоставлять клиенту дистанционные услуги.

Эмитент: предоставить авторизацию для платежных операций клиента и инициировать производство расчетов.

Эквайер: передать ответ с авторизацией на операции торгового-сервисного предприятия.

Максимальные гарантии

Клиент оплачивает услугу торгового-сервисного предприятия.

Торгово-сервисное предприятие предоставляет услугу.

Минимальные гарантии

Клиенту отказывают в оплате товаров и услуг оператора СМП.

Исходные данные сценария

Клиент зарегистрирован в СМП; клиент находится в зоне роуминга (за пределами домашней зоны) и имеет подключенный платежный инструмент.

Базовые шаги сценария

Базовые шаги сценария аналогичны шагам, описанным в сценарии финансовых транзакций в домашней зоне. Запрос клиента и результат операции направляются из зоны роуминга и обратно в домашнюю зону в соответствии с правилами роуминга и в настоящей Рекомендации не рассматриваются.

6.4.3.2 Осуществление клиентом финансовых операций в другой СМП

Цель: предоставить клиенту возможность пользоваться услугами различных СМП, в которых клиент не зарегистрирован.

Базовые роли: их цели и задачи

Клиент: получить возможность оплачивать услуги, предоставляемые торгового-сервисным предприятием, которое расположено в зоне покрытия другой СМП.

Оператор мобильной связи: передать сообщение по каналам связи.

Оператор СМП: предоставить клиенту возможность оплачивать товары и услуги с помощью другой СМП.

Торгово-сервисное предприятие: предоставлять клиенту дистанционные услуги.

Эмитент: предоставить авторизацию для платежных операций клиента и инициировать производство расчетов.

Эквайер: передать ответ с авторизацией на операции торгового-сервисного предприятия.

Максимальные гарантии

Клиент оплачивает услугу торгового-сервисного предприятия.

Торгово-сервисное предприятие предоставляет услугу.

Минимальные гарантии

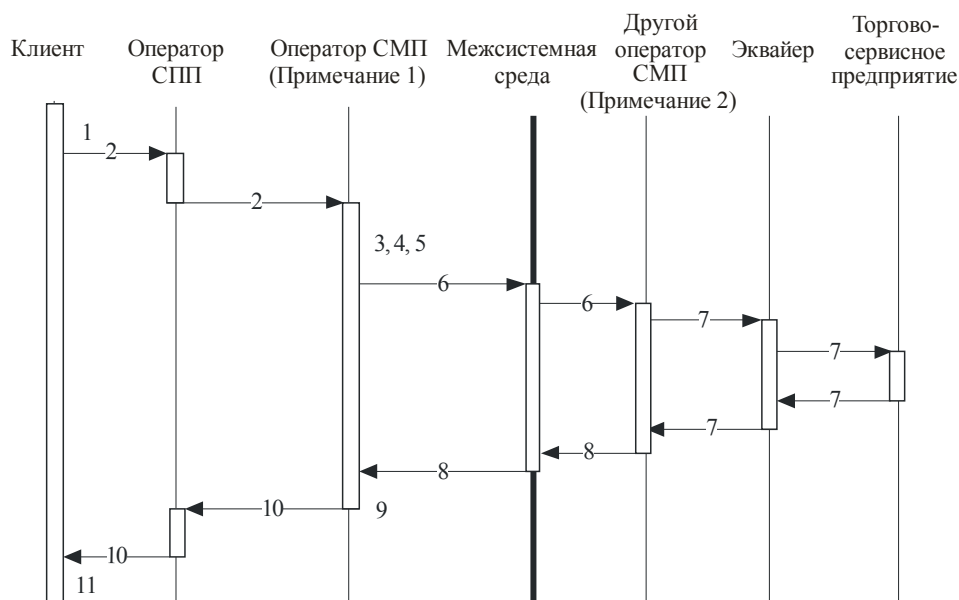
Клиенту отказывают в оплате товаров и услуг оператора СМП.

Исходные данные сценария

Клиент зарегистрирован в СМП, имеет подключенный платежный инструмент и знает реквизиты торгового-сервисного предприятия, необходимые для платежной транзакции.

Базовые шаги сценария

- 1 Клиент составляет запрос с использованием своего мобильного телефона. Запрос содержит параметры финансовой транзакции (включая идентификатор платежа) и параметры платежного инструмента.
- 2 Запрос передается по каналам связи оператора.
- 3 Оператор СМП получает запрос.
- 4 Клиент аутентифицируется.
- 5 Оператор СМП идентифицируется с помощью идентификатора платежа.
- 6 Запрос передается по соответствующему адресу (оператора другой СМП) по защищенным каналам межсистемной связи.
- 7 Требуемая финансовая транзакция осуществляется с использованием реквизитов платежного инструмента клиента.
- 8 Результаты транзакции направляются домашней СМП клиента.
- 9 СМП составляет ответ клиенту.
- 10 Ответ передается по каналам связи оператора.
- 11 Клиент получает результат транзакции.



ПРИМЕЧАНИЕ 1. – Поставщик услуг по безопасности, поставщик услуг по аутентификации клиента, поставщик услуг.

ПРИМЕЧАНИЕ 2. – Поставщик услуг по безопасности, поставщик услуг.

ITU-T Y.2741(11)_F09

Рисунок 9 – Осуществление клиентом финансовых операций в другой СМП

Альтернативные шаги сценария

- 4 **Клиент не аутентифицирован**
- 5 **СМП не может быть идентифицирована**
- 7 **Финансовая операция невозможна**
 - а) Выполняется откат транзакции.
 - б) Результат выполнения операции возвращается клиенту.

7 Переход от систем оплаты с помощью денежных и неденежных знаков

Некоторые операторы внедрили услуги, предоставляющие возможность перевода денежных и неденежных знаков в качестве платежей за товары и услуги в рамках систем выставления счетов операторов СПП (а иногда и между такими системами).

Хотя такие услуги часто представляют способствующими развитию стран с недостаточным уровнем развития и большой долей населения, не имеющего доступа к банковским услугам, в долгосрочной перспективе такие услуги могут быть разрушительными для финансово-денежных систем этих стран.

Развивающиеся страны сталкиваются с целым рядом проблем, касающихся преступности, которая связана с наличными средствами. Развитие систем электронного банкинга в таких странах приводит к сокращению объема наличных средств в обращении и, таким образом, приводит к уменьшению преступности, связанной с наличными средствами.

В связи с этим операторам СПП, которые предлагают услуги по оплате денежными и неденежными знаками, следует разработать дорожные карты по переходу от таких систем оплаты с помощью знаков к системам, в которых для обмена стоимостями используются финансовые транзакции.

Дополнение I

Регистрация платежного инструмента в системе

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Цель: предоставить клиенту возможность пользоваться своим платежным инструментом в СМП.

Базовые роли: их цели и задачи

Клиент: иметь возможность пользоваться преимуществами СМП с применением платежного инструмента.

Оператор мобильной связи: передать сообщение по каналам связи.

Оператор СМП: утвердить использование данного платежного приложения в СМП данным клиентом.

Поставщик услуг по аутентификации клиента: аутентифицировать клиента и его/ее платежный инструмент.

Максимальные гарантии

Клиент получает возможность воспользоваться СМП для использования платежного инструмента.

Минимальные гарантии

Отказ в использовании клиентом данного платежного инструмента.

Исходные данные сценария

Клиент зарегистрирован в СМП и имеет платежный инструмент.

Базовые шаги сценария

- 1 С помощью своего мобильного устройства клиент передает параметры платежного инструмента оператору СМП.
- 2 Запрос передается по каналам связи оператору СМП.
- 3 Оператор СМП получает запрос.
- 4 ИС оператора СМП генерирует случайную сумму.
- 5 Оператор СМП направляет в систему эквайера запрос на резервирование этой суммы в данном платежном инструменте. Эквайер направляет запрос на авторизацию эмитенту платежного инструмента. Клиент связывается с эмитентом и выясняет эту сумму для подтверждения того, что он/она является законным владельцем платежного инструмента.
- 6 Эмитент платежного инструмента аутентифицирует клиента с использованием своих стандартных способов аутентификации.
- 7 После аутентификации эмитент информирует клиента о размере зарезервированной суммы.
- 8 Клиент передает данные о размере этой суммы оператору СМП через клиентское приложение.
- 9 Запрос передается по каналам связи оператору СМП.
- 10 По получении от клиента данных о размере зарезервированной суммы оператор СМП сравнивает их с предыдущей генерированной суммой.
- 11 Если обе суммы совпадают, оператор СМП сохраняет в безопасном месте информацию о платежном инструменте для дальнейшего использования и направляет клиенту извещение с результатами проведенной операции.
- 12 Одновременно с этим эмитенту (через эквайера) направляется запрос на аннулирование зарезервированной суммы в платежном инструменте.

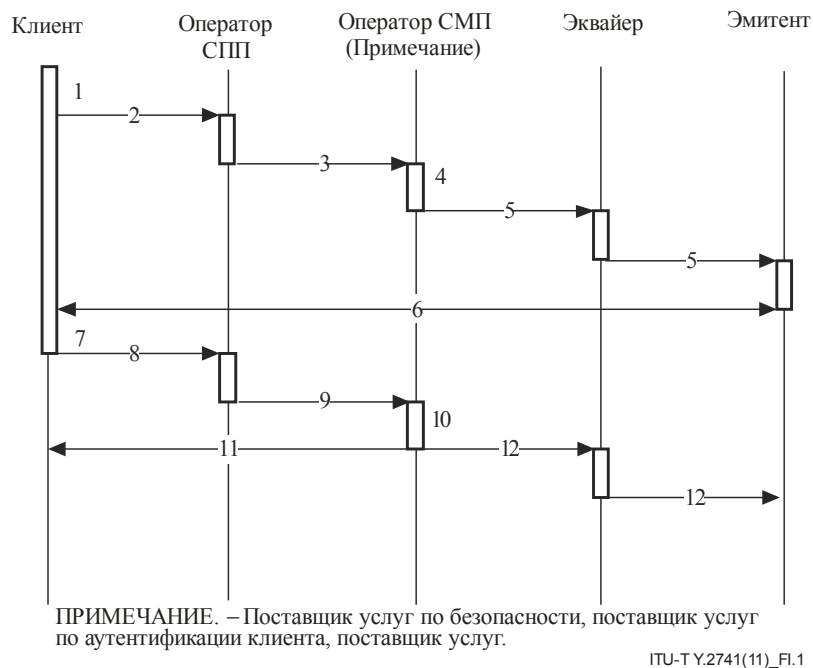


Рисунок I.1 – Регистрация платежного инструмента в СМП

Альтернативные шаги сценария

10 Размер ранее зарезервированной суммы не совпадает с суммой, введенной клиентом

Клиент получает уведомление об ошибке. Если число неудачных попыток превышает три, учетная запись мобильного устройства клиента блокируется в системе СМП. Зарезервированная сумма аннулируется.

Дополнение II

Модели реализации системы мобильного банкинга и мобильной коммерции

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В этом Дополнении описываются примеры базовых моделей реализации системы мобильного банкинга и мобильной коммерции в зависимости от реализованного уровня безопасности.

В этом Дополнении используются следующие термины:

Канал передачи сообщения: средство передачи запроса клиента об осуществлении финансовой операции (перевод денег), для которой требуется дистанционный доступ к платежным инструментам. К примерам каналов передачи сообщений относятся SMS-сообщения, USSD-запросы, пакетная передача данных (GPRS, EDGE, данные 3G, HSDPA и т. д.).

Платежный инструмент: набор законных мер для перевода средств, как наличных, так и безналичных, для целей осуществления платежа. Примерами платежных инструментов являются банковские счета, счета операторов и банковские карты.

Доступные операции: перечень имеющихся в системе операций с определенным уровнем безопасности.

Ограничения: ограничения на использование системы, которые предусматриваются принятой моделью рисков и которые устанавливаются в законном порядке или оговариваются в двусторонних контрактах.

Предварительно определенный номер телефона: номер телефона, ранее указанный клиентом в специальной форме поставщика услуг.

Конкретный номер телефона: номер телефона, указанный клиентом непосредственно при осуществлении платежа.

Предварительно определенный счет: номер счета, ранее указанный клиентом в специальной форме поставщика услуг.

Конкретный счет: номер счета, указанный клиентом непосредственно при осуществлении платежа.

Предварительно определенный платеж: платеж, осуществляемый согласно ранее представленным параметрам, когда получатель платежа может быть выбран из списка, определенного поставщиком услуг СМП (например, платеж за предоставленные услуги, осуществленный физическим лицом в пользу юридического лица).

Конкретный платеж: платеж, произведенный клиентом за услуги и не включенный в список, который определен поставщиком услуг СМП, при условии что осуществление такого платежа технически выполнимо. Предварительное условие: обязательно, чтобы или у поставщика услуг был канал связи для взаимодействия с поставщиком СМП, или услуга предоставлялась другим поставщиком СМП, и между этими двумя сторонами должно быть установлено взаимодействие.

Автоматический платеж: регулярный автоматический платеж, инициируемый поставщиком услуг СМП с предварительного согласия клиента. Автоматический платеж с подтверждением – регулярный автоматический платеж, инициируемый поставщиком услуг СМП с согласия клиента.

Платеж, инициируемый торгово-сервисным предприятием: платеж, параметры которого определяются и вводятся торгово-сервисным предприятием. Клиент может подтвердить или отклонить обработку предлагаемого платежа.

Информационная служба: ряд информационных услуг, предоставляемых поставщиком системы СМП, которые не связаны с проведением финансовой операции (например, контроль остатков средств в платежном документе, предоставление справочной информации).

Модели реализации системы мобильного банкинга и мобильной коммерции

Ниже рассматриваются возможные модели систем мобильного банкинга и мобильной коммерции в зависимости от реализованных уровней безопасности. Каждая модель реализации предусматривает определенные требования к платежному инструменту, доступным операциям, ограничениям и приложениям, используемым в системе.

II.1 Реализация системы без использования клиентского приложения

Соответствует уровню 1 и уровню 2 безопасности системы (см. [ITU-T Y.2740]).

Канал передачи сообщений: SMS-сообщения с открытым текстом, USSD-запросы.

Платежный инструмент: платежи, осуществляемые с банковских счетов и счетов оператора, предварительно определенных в соглашении о предоставлении услуги.

Доступные операции: платежи осуществляются только получателям, определенным ранее в контракте. При подписании контракта указывается список возможных операций:

- платеж с предварительно определенного номера телефона;
- платеж на предварительно определенный счет;
- осуществление предварительно определенного платежа;
- осуществление автоматических платежей;
- осуществление автоматических платежей с подтверждением;
- информационная услуга.

Ограничения: максимальный предельный уровень платежей, который может включать предельные суммы транзакций; предельные уровни транзакций за сутки; ограничения на доступные финансовые транзакции, которые предполагают платежи только за заранее согласованные услуги.

II.2 Реализация системы с использованием клиентского приложения

Соответствует уровню 3 и уровню 4 безопасности системы (см. [ITU-T Y.2740]).

Канал передачи сообщений: SMS-сообщения, пакетная передача данных (GPRS, EDGE, данные 3G, HSDPA и т. д.). Канал передачи сообщений и передаваемое сообщение должны быть зашифрованы с использованием сильной криптографии.

Платежный инструмент: платежи, осуществляемые с банковских счетов и счетов оператора, предварительно определенных в соглашении о предоставлении услуги; платежи с использованием банковских карт, а также карт международных платежных систем (платежи включают передачу важнейших данных по каналам связи).

Доступные операции: возможно дистанционное подключение к системе; широкий диапазон платежей за различные услуги, подключенные к системе; возможность существенного увеличения количества операций, которые выполняются в СМП (введение новых платежей и услуг; подключение новых торгово-сервисных предприятий); список доступных платежей может на гибкой основе определяться как поставщиком услуг, так и клиентом; различные СМП могут взаимодействовать при предоставлении услуг. Можно осуществлять следующие операции:

- платеж с предварительно определенного номера телефона;
- платеж на предварительно определенный счет;
- осуществление предварительно определенного платежа;
- осуществление автоматических платежей;
- осуществление автоматических платежей с подтверждением;
- информационная услуга;
- платеж с конкретного телефона;

- платеж на конкретный счет;
- конкретные платежи;
- платежи, инициированные торгово-сервисным предприятием.

Ограничения: ограничения на платежи определяются в двусторонних контрактах участников системы.

Приложение: использовать приложение обязательно для обеспечения безопасности (кодирования сообщений), а также подходящего способа использования системы.

Библиография

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

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	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