Центральный банк Российской Федерации

П Р С

Платежные и расчетные системы

Международный опыт

Выпуск 39

Платежи, совершаемые
с использованием
мобильного телефона

Белая книга

2013

107016, Москва, ул. Неглинная, 12

Материалы подготовлены Департаментом регулирования расчетов совместно
с Европейским платежным советом
E-mail: prs@cbr.ru, тел. 771-45-64, факс 771-97-11

Издание подготовлено к печати отделом периодических изданий Банка России
Департамента внешних и общественных связей

Текст данного сборника размещен на сайте Центрального банка Российской Федерации в сети Интернет:
http://www.cbr.ru

Отпечатано в ООО «Полиграфический комплекс ТОЧКА»
Тел.: 8 (495) 995-52-80
www.pc-t.ru

ПЛАТЕЖИ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО ТЕЛЕФОНА

БЕЛАЯ КНИГА

Содержание

Краткое содержание[1]

Роль Европейского платежного совета (European Payments Council, EPC) заключается в развитии единого европейского рынка платежей посредством помощи или содействия в разработке и внедрении стандартов, передовой практики и схем. В секторе мобильной телефонной связи обеспечены полное проникновение на рынок и высокий уровень обслуживания, что позволяет расширить использование платежных средств SEPA (Единое европейское платежное пространство).

В данной «Белой книге»:

• заинтересованным сторонам сообщается о намерении EPC развивать на территории стран SEPA платежи, совершаемые с использованием мобильного телефона;

• излагаются некоторые элементы экономического обоснования для поставщиков платежных услуг (PSP), желающих работать на рынке розничных платежных услуг, совершаемых с использованием мобильного телефона;

• продемонстрированы возможности использования платежей, совершаемых с использованием мобильного телефона, потребителями путем представления нескольких практических иллюстраций сценариев применения таких платежей;

• собраны мнения и отзывы заинтересованных сторон.

Данная «Белая книга» написана не техническим языком с целью предоставить информацию PSPs, их клиентам и всем заинтересованным сторонам, вовлеченным в платежную систему. Издание также отражает точку зрения EPC на платежи, совершаемые с использованием мобильного телефона в странах SEPA. EPC предлагает всем заинтересованным сторонам прокомментировать информацию, представленную в данной «Белой книге».

Приступая к этой работе, EPC проанализировал различные категории платежей и обозначил в качестве приоритетных бесконтактные платежи, совершаемые с использованием мобильного телефона (MCPs), и дистанционные платежи, совершаемые с использованием мобильного телефона, а также кредитовые переводы (SCT). По каждой из этих категорий платежей, совершаемых с использованием мобильного телефона, в настоящем докладе представлен углубленный анализ посредством исследования основных примеров их применения, описания экосистемы, архитектуры высокого уровня и наиболее важных инфраструктурных аспектов. Кроме того, описываются принципы функционирования мобильных кошельков.

В контексте данного доклада «дистанционные» и «бесконтактные» платежи, совершаемые с использованием мобильного телефона, рассматриваются как дистанционные и бесконтактные платежи, совершаемые с использованием мобильного телефона путем введения реквизитов платежной карты SEPA.

Основные выводы из настоящего доклада следующие.

По бесконтактным платежам, совершаемым с использованием мобильного телефона, выбор элемента безопасности (SE) в значительной степени определяет модель обслуживания и роли различных заинтересованных сторон.

По дистанционным платежам, совершаемым с использованием мобильного телефона, определены три главные задачи:

• удобство инициирования трансакции и идентификации получателя в платежах, инициируемых плательщиком;

• определенность результата платежа для получателя;

• немедленные (или моментальные) платежи.

Хотя многие из определенных задач не являются специфичными для канала мобильной связи, их раннее окончательное решение важно для того, чтобы платежные средства SEPA стали общепринятыми в канале мобильной связи. Для заинтересованных лиц, которым требуется более детальная информация по MCP, EPC составил методические рекомендации по реализации операционной совместимости, затрагивающие вопросы обслуживания, технические вопросы и вопросы безопасности (см. [5]). EPC будет участвовать в разработке дальнейших методических рекомендаций по внедрению дистанционных

[1] Данный материал является неофициальным переводом публикации Европейского платежного совета «Белая книга. Платежи, совершаемые с использованием мобильного телефона» («White paper. Mobile payments», 2012). Электронная версия данной публикации на английском языке размещена на веб-сайте Европейского платежного совета (http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=564). Копирование без ссылки на источник запрещается. Действуют ограничения, предусмотренные оговоркой о конфиденциальности.

платежей, совершаемых с использованием мобильного телефона, документ по этому вопросу будет опубликован для открытых дискуссий. Хотя отдельные заинтересованные стороны в экосистеме платежей, совершаемых с использованием мобильного телефона, должны сами решить, будут ли они реализовывать свои услуги в этой области и когда именно, EPC планирует, опубликовав этот доклад, определить способы эффективного внедрения платежей, совершаемых при помощи мобильного телефона в зоне SEPA.

Структура доклада

В настоящем разделе описана структура «Белой книги». В начале издания представлены глоссарий терминов и список сокращений, используемых в настоящем докладе. Общая информация о EPC и его точке зрения содержится в разделе 1. В разделе 2 содержится введение в SEPA, услуги, связанные с платежами, совершаемыми с использованием мобильного телефона, и связанные с этим аспекты экономического обоснования. В следующем разделе представлен ряд сценариев платежей, совершаемых с использованием мобильного телефона, в виде описания событий из повседневной жизни потребителя. Здесь также содержатся общие сведения о платежах, их распределении по категориям и приоритетам, предложенным EPC. Раздел 4 посвящен бесконтактным платежам, совершаемым с использованием мобильного телефона посредством введения реквизитов платежной карты SEPA (MCPs). Он включает в себя более подробное описание примеров использования и обзор высокого уровня по экосистеме и архитектуре MCP. Аналогичным образом в разделе 5 дается описание дистанционных платежей, совершаемых с использованием мобильного телефона (MRPs), при этом рассматриваются как дистанционные платежи по картам, так и дистанционные кредитовые переводы. В разделе 6 показано, как можно легко и удобно подписаться на платежи, совершаемые с использованием мобильного телефона. Различные инфраструктурные компоненты, используемые для MCPs и MRPs, описаны в разделе 7. В разделе 8 представлено использование мобильных кошельков и их влияние на повседневную жизнь потребителей. В следующем разделе дан обзор наиболее важных стандартов, а также отраслевых организаций в экосистеме платежей, совершаемых с использованием мобильного телефона. Общие выводы, нерешенные задачи и будущая работа описываются в заключительном разделе 10. Наконец, в приложениях содержатся введение в платежные средства SEPA и основная информация об элементах безопасности. Библиография и ссылки даны в конце «Белой книги».

Список сокращений

AAUI	Пользовательский интерфейс включения приложения
B2B	Предприятие – предприятию
B2C	Предприятие – потребителю
C2B	Потребитель – предприятию
C2C	Потребитель – потребителю
CAP	Программа аутентификации микрочипа
CNP	«Карта отсутствует»
CSM	Механизм клиринга и расчетов
CVM	Метод верификации держателя карты
DPA	Динамическая аутентификация пароля
ETSI	Европейский институт по стандартам в области телекоммуникаций
GP	GlobalPlatform
GSMA	Ассоциация GSM
ID	Идентификатор
ISO	Международная организация по стандартизации
MCP	Бесконтактный платеж, совершаемый с использованием мобильного телефона
MNO	Оператор сети мобильной связи
MRP	Дистанционный платеж, совершаемый с использованием мобильного телефона
MVNO	Оператор мобильной виртуальной сети
NFC	Связь в ближней зоне
POI	Точка взаимодействия
PSD	Директива по платежным услугам
PSP	Поставщик платежных услуг
SCF	Система карт SEPA
SCP	Платеж по карте SEPA
SCT	Кредитовый перевод SEPA
SDD	Безакцептное списание SEPA
SE	Элемент безопасности
SEPA	Единое европейское платежное пространство
TEE	Надежная среда выполнения
TSM	Доверенный сервис-менеджер
TTP	Доверенная третья сторона
UICC	Универсальная карта с интегральной схемой
uSCT	Срочный кредитовый перевод SEPA

Глоссарий используемых терминов

Термин	Определение
Бесконтактный платеж, совершаемый с использованием мобильного телефона (MCP)	Платеж, инициированный с мобильного телефона, когда держатель карты и предприятие торговли (и/или его оборудование) находятся в одном месте и связаны между собой напрямую с использованием бесконтактной технологии радиосвязи, такой как технология NFC, для передачи данных (также именуется бесконтактным платежом). В контексте настоящего доклада все бесконтактные платежи, совершаемые с использованием мобильного телефона, рассматриваются как бесконтактные платежи, совершаемые с использованием мобильного телефона путем введения реквизитов платежной карты SEPA
Держатель карты	Клиент, заключивший договор с эмитентом о возможности осуществления платежей, совершаемых с использованием мобильного телефона путем введения реквизитов платежной карты SEPA (MCP). Он должен быть подписчиком оператора сети мобильной связи (MNO) или оператора мобильной виртуальной сети (MVNO), имеющим мобильное оборудование NFC
Дистанционный платеж, совершаемый с использованием мобильного телефона (MRP)	Платеж, инициированный с помощью мобильного телефона или иного подобного устройства, когда операция проводится по сети мобильной связи (например, GSM, мобильная сеть Интернет и т.д.) и может быть выполнена независимо от места нахождения плательщика (и/или его оборудования)
Доверенная третья сторона (TTP)	Организация, обеспечивающая взаимодействие между заинтересованными сторонами экосистемы, в которой все доверяют этой третьей стороне (примеры – эмитент SE, TSM, управляющий общей инфраструктурой, и т.д.)
Доверенный сервис-менеджер (TSM)	Доверенное лицо, действующее от имени эмитента SE и/или эмитента приложения MRP, в случае если SE используется для размещения приложения (приложений) MRP
Идентификация получателя	Средство однозначной идентификации получателя и используемого им счета. Примеры включают использование IBAN[2]/BIC[3], уникальный идентификатор, номер карты, специальные удостоверения и др.
«Карта отсутствует»	Операция, совершаемая с дистанционным использованием карты, то есть при отсутствии физического взаимодействия между самой картой и POI на момент совершения операции
Клиент	Плательщик или получатель платежа, который может быть физическим лицом или предприятием
Контекст покупки	Различные способы, предлагаемые предприятием торговли (услуг) своим клиентам для совершения покупок (например, SMS, мобильный сайт в сети Интернет, выделенное мобильное приложение, заранее зарегистрированный уникальный идентификатор)
Мобильный кошелек	Цифровой кошелек, предоставляющий услугу, которая позволяет его владельцу безопасно получать доступ к средствам идентификации и платежным средствам, управлять ими и использовать их, чтобы инициировать платежи с мобильного телефона
Оператор сети мобильной связи (MNO)	Оператор сети мобильной телефонной связи, предоставляющий ряд услуг мобильной связи, потенциально включающих содействие услугам NFC. MNO обеспечивает возможность соединения «Over the Air» («по воздуху») между плательщиком (потребителем) и его PSP с использованием своей собственной или арендуемой сети (последние иногда именуются MVNO – операторы мобильной виртуальной сети)
Платежная операция	Действие, инициированное плательщиком или получателем платежа, по размещению, переводу или изъятию денежных средств независимо от лежащих в основе взаимных обязательств между плательщиком и получателем (согласно определению в [19])
Платежная система	Система перевода денежных средств с официальными стандартизированными договорами и общими правилами по обработке, клирингу и/или расчетам по платежным операциям (согласно определению в [14])
Платежная схема	Технико-коммерческая схема, обслуживающая одну или несколько платежных систем и предусматривающая организационные, юридические и операционные правила, необходимые для предоставления предлагаемых платежных услуг (например, карточная схема, услуга электронных платежей и т.д.)
Платежный счет	Счет, открытый на имя одного или нескольких пользователей платежной услуги и используемый для совершения платежных операций [19]
Плательщик	Физическое или юридическое лицо, имеющее платежный счет и направляющее платежное поручение с этого платежного счета, или, если платежный счет отсутствует, физическое или юридическое лицо, направляющее платежное поручение [14]
Подтверждение платежной услуги	В контексте настоящего документа – услуга, предусматривающая для получателя достаточную степень гарантии того, что платеж выполнен или будет выполнен (от простого подтверждения до фактического получения денежных средств)
Получатель	Физическое или юридическое лицо, являющееся получателем денежных средств, представляющих собой предмет платежной операции [19]
Пользовательский интерфейс приложения MCP	Приложение в мобильном телефоне, выполняющее действия пользователя, относящиеся к приложению MCP, если это разрешено эмитентом MCP
Пользовательский интерфейс приложения MRP	Приложение в мобильном телефоне, выполняющее действия пользователя, относящиеся к приложению MRP, если это разрешено эмитентом MRP

[2] BIC – банковский идентификационный код.

[3] IBAN – международный стандарт номера банковского счета.

Поставщики платежных услуг (PSP)	Организации, указанные в статье 1 [19], юридические и физические лица, использующие оговорку, предусмотренную в статье 26 [19]
Потребитель	Физическое лицо, которое в договорах о платежных услугах, указанных в [19], действует не в своих коммерческих, хозяйственных или профессиональных целях (согласно определению в [19])
Приложение MCP	Приложение, находящееся в элементе безопасности и выполняющее платежные функции по MCP согласно инструкциям эмитента MCP
Приложение MRP	Приложение, находящееся в SE и выполняющее платежные функции, относящиеся к MRP, согласно инструкциям эмитента MRP
Связь в ближней зоне (NFC)	Протокол бесконтактной связи, предусмотренный в ISO/IEC 18092
Служба электронных платежей	В контексте настоящего документа – служба дистанционных платежей на основе кредитового перевода SEPA (SCT), обеспечивающая подтверждение платежа для получателя (который должен быть зарегистрированным участником службы электронных платежей)
Торговое предприятие	Акцептор в схеме MCP по платежам за товары (услуги), приобретаемые потребителем (держателем карты – в контексте настоящего доклада). Также именуется «ожидаемым» в случае обслуживаемых POI. Предприятие торговли является клиентом для своего эквайрера
Трехсторонняя модель	Как плательщик, так и получатель являются клиентами одного и того же PSP, действующего в соответствии с платежной схемой
Уникальный идентификатор	По дистанционным платежам универсальный идентификатор – это идентификатор получателя, который может быть однозначно связан с именем получателя, его BIC и IBAN в случае использования дистанционных платежей (SCP) и служить для идентификации платежного счета получателя в случае дистанционных SCP. Использование уникального идентификатора возможно для идентификации плательщика
Устройство POI	Устройство в точке взаимодействия (например, кассовый аппарат, торговый автомат, банкомат и т.д.)
Четырехсторонняя модель	Плательщик и получатель являются клиентами разных PSPs, которые могут действовать в соответствии с одной и той же платежной схемой или в соответствии с разными платежными схемами
Эквайрер	PSP, обеспечивающий возможность обработки торговой трансакции с эмитентом посредством авторизации и клиринга. В контексте настоящего документа это фактически означает принятие платежа, совершаемого с использованием мобильного телефона
Элемент безопасности (SE)	Сертифицированная платформа с защитой от несанкционированного доступа (устройство или компонент), на которой могут безопасно размещаться приложения и их конфиденциальные и криптографические данные (например, управление ключами защиты) в соответствии с правилами и механизмами безопасности, установленными рядом известных доверенных организаций. Примеры включают UICC, встроенные элементы безопасности, карты с микрочипами и SD-карты
Эмитент	PSP, предоставляющий клиенту платежный счет и (в контексте настоящего доклада) приложение для платежей, совершаемых с использованием мобильного телефона
Эмитент MCP	PSP, предоставляющий потребителю приложение MCP
Эмитент MRP	PSP, предоставляющий потребителю приложение MRP
Эмитент элемента безопасности (эмитент SE)	Доверенная третья сторона, отвечающая за эмиссию и обслуживание SE. Типичные примеры – MNO и производители карт

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. ИНФОРМАЦИЯ О ЕВРОПЕЙСКОМ ПЛАТЕЖНОМ СОВЕТЕ

Европейский платежный совет (EPC, см. http://www.europeanpaymentscouncil.eu/index.cfm) является координирующим и принимающим решения органом европейской банковской системы[4] по расчетам. Цель EPC – поддержка и развитие единого европейского платежного пространства. EPC участвует в разработке платежных схем и систем, необходимых для реализации единого рынка платежей в евро. В частности, EPC работает над общими позициями PSPs[5] по объединению пространства платежных услуг, содействует процессам стандартизации, определяет наилучшие практики применения, поддерживает и контролирует реализацию принимаемых решений. Это осуществляется таким образом, чтобы PSPs сохраняли саморегулирование и отвечали ожиданиям органов регулирования и заинтересованных сторон наиболее эффективно.

EPC состоит из 74 членов: это банки, банковские сообщества и платежные организации. В рабочей программе EPC непосредственно заняты более 360 специалистов из 32 стран, они представляют организации различного масштаба, затрагивающие все сферы деятельности европейской банковской системы. Европейский центральный банк выступает в качестве наблюдателя для рабочих групп и групп поддержки EPC, а также для Пленума EPC (орган EPC, принимающий решения). EPC является некоммерческой организацией, предлагающей все результаты своей деятельности, включая Операционные правила SEPA и связанную с этим документацию, для бесплатной загрузки с сайта EPC в сети Интернет. Следует отметить, что EPC не поставляет технологии, товары и услуги.

Более подробная информация о платежных средствах SEPA приведена в Приложении I «Платежные средства SEPA».

Рисунок 1. **Зона SEPA**

1.2. КОНЦЕПЦИЯ

Концепция EPC – участие в развитии единого рынка платежных услуг путем помощи или содействия в разработке и внедрении стандартов, схем и передовой практики. В соответствии с этой задачей EPC по поручению своих членов – банков и платежных организаций – сотрудничает с другими заинтересованными сторонами в практической реализации проведения платежей, совершаемых с использованием мобильного телефона на территории SEPA.

Платежные операции с использованием мобильных устройств и услуг могут быть основаны на существующих Сводах правил SEPA, платежных системах SEPA и мировых стандартах. Поэтому EPC планирует помогать в разработке стандартов и методических рекомендаций, способствующих созданию необходимых условий для того, чтобы поставщики платежных услуг могли предложить безопасные, эффективные и удобные для пользователей мобильные решения по доступу к платежным средствам SEPA.

Важным фактором успеха является межотраслевое сотрудничество, в особенности между платежным сектором и операторами мобильной связи (MNO). Поэтому EPC намеревается содействовать межотраслевому сотрудничеству в разработке правил, стандартов и оптимальных методов в этой области. Потребители (см. определение в Глоссарии) не должны быть привязаны к конкретному MNO и конкретному оборудованию мобильной связи, а должны сохранить имеющуюся у них возможность переходить от одного поставщика платежных услуг к другому.

---

[4] Банковская система включает банки, банковские сообщества и платежные организации.

[5] Ссылка на банки в настоящем документе не ограничивает предоставление услуг мобильных платежей исключительно банками, а означает PSP.

1.3. ПРЕДМЕТ И ЦЕЛИ

Предметом «Белой книги» являются платежи, совершаемые с использованием мобильного телефона в зоне SEPA. Это означает использование платежных средств SEPA по мобильному каналу. Настоящее второе издание включает детальный анализ бесконтактных и дистанционных платежей в соответствии с приоритетами, установленными EPC (см. раздел 3.2.2).

При публикации настоящей «Белой книги» EPC ставит перед собой следующие цели:

• сообщить заинтересованным сторонам о намерении EPC развивать платежи, совершаемые с использованием мобильного телефона в зоне SEPA, и возможности построения мобильного канала на основе платежных средств SEPA;

• сообщить о новом удобном, единообразном и постоянном доступе к услугам и новых возможностях деловой деятельности, открывающихся благодаря каналу мобильной связи;

• обозначить приоритетные категории при оплате товаров (услуг) посредством мобильного телефона;

• проанализировать бесконтактные платежи и дистанционные платежи, совершаемые с использованием мобильного телефона, путем введения реквизитов платежной карты SEPA;

• предоставить другую информацию и примеры существующей реализации на практике платежей посредством мобильного телефона.

1.4. ДОКУМЕНТЫ, НЕ ЯВЛЯЮЩИЕСЯ ПРЕДМЕТОМ РАССМОТРЕНИЯ, И ПОСЛЕДУЮЩИЕ ПУБЛИКАЦИИ

Настоящий доклад является самостоятельным. Следует отметить, что он не описывает все аспекты услуг по осуществлению платежей, совершаемых с использованием мобильного телефона, а сосредоточен на инициировании платежей по каналу мобильной связи с использованием существующих платежных средств SEPA (SCT, SDD и SEPA по карточным платежам). Читателю предлагается ознакомиться со стандартами и сводами правил EPC (www.europeanpaymentscouncil.eu), где описаны общие аспекты трансакции, совершаемой с использованием мобильного телефона.

Настоящий доклад не содержит исследования рынка, поскольку многочисленные исследования рынка уже опубликованы.

Хотя в докладе описаны некоторые элементы экономического обоснования деятельности поставщиков платежных услуг, желающих работать на рынке платежей, совершаемых с использованием мобильного телефона, более подробная информация приведена в «Методических рекомендациях по реализации операционной совместимости при использовании бесконтактных платежей по картам в зоне SEPA» [5] и в готовящихся «Методических рекомендациях по реализации операционной совместимости в дистанционных платежах посредством мобильного телефона», которые должны быть опубликованы EPC. Эти методические рекомендации сосредоточены на операционной совместимости между различными заинтересованными сторонами, вовлеченными в мобильные экосистемы, такими как эмитент SE, эмитент MCP, MNO, TSM и др., в контексте их сотрудничества. Кроме того, рассмотрены технические аспекты и аспекты безопасности, касающиеся управления жизненным циклом приложений для платежей, совершаемых с использованием мобильного телефона, и платежных операций, совершаемых посредством мобильного телефона.

1.5. АУДИТОРИЯ

Настоящий доклад предназначен главным образом для поставщиков платежных услуг, указанных в Директиве по платежным услугам (PSD) [19], таких как банки и платежные организации.

Кроме того, настоящий доклад может предоставить ценную информацию другим сторонам, занимающимся реализацией платежей, совершаемым с использованием мобильного телефона, таким как:
• операторы сетей мобильной связи (MNO);
• доверенные сервис-менеджеры (TSM);
• производители оборудования;
• торговые предприятия и торговые организации;
• потребители;
• разработчики приложений;
• государственные органы;
• органы регулирования;
• организации по стандартизации и отраслевые организации;
• другие заинтересованные стороны.

2. ВВЕДЕНИЕ

2.1. РАЗВИТИЕ УСЛУГ, ОСНОВАННЫХ НА МОБИЛЬНОЙ СВЯЗИ, В ЗОНЕ SEPA

Согласно [14], существующее рыночное проникновение мобильных телефонов в развитых странах близко к уровню насыщения. Большинство потребителей уже используют мобильные телефоны для получения других услуг, помимо традиционных голосовых звонков и обмена краткими сообщениями (SMS). Эти услуги развиваются во многом благодаря существующей инфраструктуре MNO, поддерживающей пакетный доступ в сеть Интернет с помощью технологий GPRS и 3G с практически полным географическим сетевым покрытием. В последнее время ожидания потребителей по функциональным возможностям мобильных телефонов резко возросли. Об этом говорит тот факт, что рыночный сегмент смартфонов растет более уверенно и гораздо быстрее, чем любой другой [11]. Потребители считают, что эта тенденция сохранится, и готовы пользоваться новыми сервисными решениями на основе этой платформы, которые могут облегчить их повседневную жизнь. Очевидно, что финансовые услуги считаются самыми важными среди этих новых мобильных услуг, и потому возникают высокие ожидания. Кроме того, переход на платежи, совершаемые с использованием мобильного телефона, сокращает использование денежной наличности и чеков. EPC и PSPs уверены, что платежи, инициированные посредством мобильного телефона, будут очень востребованы клиентами.

Торговым предприятиям необходимо, чтобы новые технические решения напрямую повышали эффективность их деятельности, приводя в конечном итоге к снижению издержек и увеличению торгового оборота. Они также ожидают, что новые технологии снизят риски, связанные с вопросами безопасности (такие как хищение денежной наличности) и финансовой ответственности (такие как незаконные платежи). Наконец, торговые предприятия ожидают, что предлагаемые новые услуги создадут новые возможности для сбыта, предоставления дополнительных услуг и повышения привлекательности бренда. EPC считает, что платежи, совершаемые с использованием мобильного телефона, в частности бесконтактные, хорошо подходят для достижения всех этих преимуществ для торговых предприятий и других заинтересованных сторон, которые непосредственно предоставляют услуги потребителям.

Что касается отношений между самими потребителями, новые электронные средства позволят осуществлять платежи в зоне SEPA посредством мобильного телефона, основанные на платежном счете или карте, по модели «потребитель – потребителю» (C2C).

Наконец, согласно [1], многие PSPs уже обозначили платежи, совершаемые с использованием мобильного телефона, в качестве цели для новых возможностей роста. В зоне SEPA и других регионах осуществляются различные пилотные проекты по проведению платежей посредством мобильного телефона и коммерческой реализации этих платежей, и реакция заинтересованных сторон неизменно положительна. Следовательно, рынок зоны SEPA готов к немедленному внедрению платежей посредством мобильного телефона.

2.2. ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ

По определению, экосистема для платежей, совершаемых с использованием мобильного телефона, независимо от формы, которую она примет, обеспечивает для PSPs в своей стоимостной цепочке роль, которую играют расчеты (банки, платежные организации или организации по операциям с электронными средствами платежа). В настоящей «Белой книге» не анализируется хозяйственная составляющая по платежным организациям в системе платежей посредством мобильного телефона (поскольку это относится к конкурентному пространству, см. раздел 2.4). В ней лишь описаны некоторые элементы коммерческого обоснования для PSPs, желающих работать на рынке платежей посредством мобильного телефона.

PSPs должны предвидеть будущее поведение потребителей и приспосабливаться к нему. Мобильный канал обеспечивает огромные возможности для PSPs по расширению и улучшению платежных услуг, предлагаемых их клиентам. Очень важно использовать эти возможности, поскольку новое поколение потребителей в значительной степени полагается на мобильные телефоны в повседневной жизни. Потребители все чаще пользуются финансовыми услугами посредством своего мобильного телефона, и платежи, совершаемые с использованием мобильного телефона, представляются следующим логическим шагом.

Распространение мобильных устройств во всей Европе (а также более широкая доступность смартфонов с множеством приложений) и потенциал их использования для инициирования платежей, совершаемых посредством мобильного телефона, обеспечивают большие возможности для наращивания использования платежных средств SEPA. Использование мобильного канала может также обеспечить возможности для дополнительных услуг, таких как подписание или передача поручений для безакцептного списания.

Как заявлено в его концепции и плане действий, одна из целей EPC заключается в стимулировании развития и внедрения платежей, совершаемых с использованием мобильного телефона. На этом начальном этапе с участием большого числа заинтересованных сторон важно сосредоточиться на основных аспектах экосистемы, чтобы перейти от фрагментации к стандартизации и обеспечить возможность предложения услуг во всей зоне SEPA. Примером является способность связать уникальные идентификаторы с расчетами для MRPs.

Как уже сказано, настоящий документ не содержит конъюнктурных данных и исследования рынка. Читателю предлагается ознакомиться с многочисленными имеющимися исследованиями рынка, которые показывают, что, помимо высокого рыночного потенциала, платежи, совершаемые с использованием мобильного телефона, востребованы. Однако каждый PSP должен самостоятельно определить, будут ли они выгодны с коммерческой точки зрения, исходя из исследования рынка, потенциальных доходов и ожидаемых инвестиций и издержек. Он должен также определить свое положение, ресурсы, которые он готов вложить, и роль, которую он намерен играть в стоимостной цепочке. Очевидно, что ситуация будет различаться для каждого PSP в зависимости от его клиентской базы, стратегии и целей бизнеса, географических условий, технической инфраструктуры и используемых ресурсов.

Основные элементы, на которых базируется коммерческое обоснование, следующие:

• высокая степень проникновения мобильных телефонов на рынок: в последние два десятилетия их количество значительно превысило количество платежных карт во всем мире, и все больше потребителей готовы и намерены использовать мобильный канал связи для проведения платежей;

• потенциал новых платежных схем SEPA и инвестиционного механизма по платежам, инициированным при помощи мобильного телефона;

• удобство для пользователей – удовлетворение потребностей потребителей и торговых предприятий;

• необходимость стимулировать инновации путем конкурентных предложений, выгодных для потребителей, в более сложной экосистеме, включающей новые заинтересованные стороны, в соответствии с предложенной EPC концепцией SEPA, что обеспечит растущий рынок платежей и переход потребителей к более быстрым, более эффективным и более удобным средствам платежа.

Как уже отмечалось, целью данного доклада и целю EPC не является обсуждение стратегии работы PSPs на рынке и конкретных моделей обслуживания, включая различные способы взаимодействия между различными заинтересованными сторонами в стоимостной цепочке. Однако представлено общее описание различных моделей обслуживания по бесконтактным платежам, совершаемым с использованием мобильного телефона (см. раздел 4), и дистанционных платежей посредством мобильного телефона (см. раздел 5). Эти модели более подробно анализируются в [5] для MCPs и будут проанализированы для MRPs в готовящихся методических рекомендациях по реализации операционной совместимости.

Основные стимулы для заинтересованных сторон, участвующих в экосистеме, по скорейшему внедрению платежей, совершаемых с использованием мобильного телефона, следующие.

Ожидания и потребности потребителей:

• эффективность: скорость инициирования платежа;

• удобство и мобильность: безналичные платежи можно совершать везде и в любое время;

• уверенность и доверие;

• незамедлительность платежа / подтверждение платежа: гарантия совершения платежа в режиме реального времени для выгодоприобретателя / предприятия торговли (услуг), что позволяет немедленно передать потребителю (плательщику) товар или услугу;

• возможность связаться с плательщиками / клиентами-выгодоприобретателями / предприятиями торговли (услуг).

Ожидания и потребности выгодоприобретателей / предприятий торговли (услуг):

• стоимостная эффективность (например, для предприятий торговли (услуг));

• уверенность и доверие;

• незамедлительность платежа / подтверждение платежа: гарантия совершения платежа в режиме реального времени для получателя (например, предприятия торговли (услуг), потребителя);

• стремление к замещению денежной наличности и в некоторых странах к замещению чеков;

• возможность связаться с выгодоприобретателем / предприятием торговли (услуг) для плательщиков / потребителей;

• предоставление связанных с этим дополнительных услуг, например, одновременное предложение клиенту ряда связанных услуг и/или маркетинг на основе географического местонахождения;

• простота реализации.

Ожидания и потребности PSPs:

• сохранение / привлечение клиентов;

• стоимостная эффективность;

• снижение риска / улучшение контроля;

• предоставление связанных с этим дополнительных услуг, например управление поручениями, наличие реквизитов получателя в случае дистанционного платежа;

• стремление к замещению денежной наличности и, в некоторых странах, к замещению чеков;

• ожидания регулирующих органов.

Очевидно, мобильный телефон станет дополнительным каналом инициирования платежей, сосуществующим с другими каналами и способами оплаты товаров (услуг).

2.3. АСПЕКТЫ БЕЗОПАСНОСТИ

Одним из основных факторов широкого распространения платежей, совершаемых с использованием мобильного телефона, является доверие к способу расчета со стороны потребителей и торговых предприятий. Ощущение надежности платежных операций посредством мобильного телефона – важный аспект в формировании этого доверия; другие аспекты включают договорные отношения между клиентами и их PSPs и прозрачность процессов, лежащих в основе их деятельности. Если в этом отношении возникнут сомнения, взаимоотношения между PSP и его клиентами, а также, что еще хуже, репутация PSPs в целом, их услуг и используемых технологий сильно пострадает.

Для поддержания надлежащего уровня доверия и прозрачности в отношении клиентов, осуществляющих операции посредством мобильного телефона, при существующих каналах инициирования платежей важно сформировать надежную однородную экосистему, охватывающую также новые заинтересованные стороны, чтобы было очевидно, что:

• ответственность распределена;

• вопросы безопасности последовательно регулируются заинтересованными участниками;

• платежные операции безопасны, понятны и надежны;

• личная тайна сохраняется.

Следовательно, должна быть полностью создана архитектура безопасности, покрывающая все аспекты безопасности экосистемы платежей, совершаемых с использованием мобильного телефона, в соответствии с признанными международными стандартами. Эта архитектура безопасности должна включать как минимум следующие аспекты:

Уровень процессов

Каждая заинтересованная сторона (например, PSP, MNO и TSM) в экосистеме платежей посредством мобильного телефона должна обеспечить наличие соответствующей системы управления информационной безопасностью. Каждый поставщик услуг должен быть способен соответствующим образом заявить об этом аудиторам или определить это в условиях договоров об уровне обслуживания по безопасности в соответствующих договорных отношениях.

Система управления информационной безопасностью должна включать как минимум методы и процедуры контроля соответствующих рисков и управления ими, а также распределения соответствующих ресурсов и ответственности в целях снижения этих рисков. Каждая участвующая сторона должна определить свои обязанности и ресурсы, которые необходимо сохранять в ее сфере ответственности.

Уровень приложений

По каждому примеру использования должна существовать документированная концепция безопасности. На этом уровне известны приложения и последовательность операций. Абстрактные компоненты, относящиеся к используемым устройствам, поведению потребителей, атакам, среде выполнения приложений и т.д., могут быть описаны и использованы для анализа рисков. Это относится ко всей цепочке поставки, и можно выделить различные аспекты – в отношении клиента, поставщиков услуг и партнеров по договору соответственно.

Уровень реализации

На уровне реализации выбор необходимых средств управления безопасностью и показателей зависит главным образом от технических решений, используемых для реализации услуг, и соответствующих внешних условий.

Путем анализа конкретной реализации можно выявить внешнюю атаку в вопросах безопасности и принять соответствующие меры противодействия, как технические, так и организационные. Например, для MCP наиболее заметной определенной мерой противодействия является «элемент безопасности», который описан ниже в данном докладе (см. также [5]).

2.4. АРХИТЕКТУРА ПЛАТЕЖЕЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО ТЕЛЕФОНА

EPC предлагает принципы высокого уровня и архитектуру платежей, совершаемых с использованием мобильного телефона, с целью создания необходимых стандартов и бизнес-правил для PSPs в новой области. Платежи, совершаемые с использованием мобильного телефона, представляют собой новый канал, в котором могут использоваться существующие платежные средства SEPA, т.е. схемы SEPA (SCT, SDD) и карты SEPA (SCP). Основное внимание уделяется инициированию и получению кредитовых и дебетовых платежей (включая карточные платежи) посредством мобильного телефона. Платежи, совершаемые с использованием мобильного телефона, должны соответствовать PSD [19], а также существующим правилам по базовым платежным средствам SEPA. В результате мобильный канал не налагает ограничений на сумму и виды осуществляемых через него платежей (платежные средства SEPA не зависят от суммы операции). Это относится к конкурентным решениям каждой схемы и/или отдельного PSP.

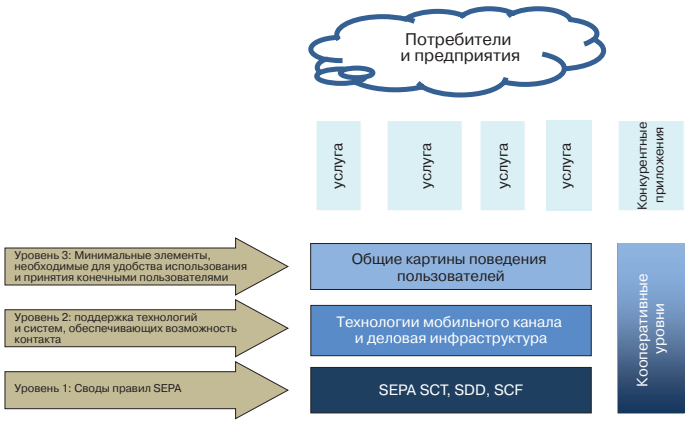
Принципы высокого уровня и архитектура платежей, совершаемых посредством мобильного телефона, включая стандартные правила и ссылки на них и оптимальные методы, разработанные EPC, открыто передаются участникам рынка и поставщикам в стоимостной цепочке в мобильном канале, чтобы предоставить им возможность внести вклад в разработку стандартов и бизнес-правил в этой области. Каждый из них или любая их группа самостоятельно решают, когда и каким образом следует принять эти стандарты и бизнес-правила, в частности, в каком сегменте или сегментах платежного рынка должны присутствовать их продукты и услуги. Это может быть, например, сегмент микроплатежей или любой другой сегмент.

Один из наиболее привлекательных аспектов в области платежей, совершаемых с использованием мобильного телефона, заключается в повсеместном предложении услуг, заменяющих денежную наличность. Эти услуги должны увеличить скорость проведения текущих операций и сократить общие операционные издержки предприятий. EPC развивает это направление, в частности, путем использования передового опыта пользователей, когда это позволяет политика управления рисками. В связи с этим EPC и другие организации предъявляют минимальные требования к безопасности. Однако практическая реализация этих услуг остается в конкурентном пространстве.

EPC сосредоточивает свое внимание на областях, составляющих основу операционной совместимости, но не на областях, находящихся в конкурентном пространстве. EPC также поощряет межотраслевое сотрудничество, чтобы мобильный телефон стал эффективным каналом для инициирования платежей.

На следующем рисунке показано участие EPC на разных уровнях в рамках предмета и объема платежей посредством мобильного телефона.

Рисунок 2. **Предмет мобильных платежей**



Примечание: Насыщенность синего цвета означает степень сотрудничества на каждом уровне.

Уровень 1 обозначает уже существующие Своды правил SEPA для SCT и SDD, а также карточный механизм SEPA. Этот уровень включает базовые платежные средства по платежам посредством мобильного телефона.

Уровень 2 включает используемые технологии и системы, обеспечивающие возможность контакта в платежных средствах SEPA. Примечательный пример в этой области содержится в документах EPC «Методические рекомендации по реализации операционной совместимости при использовании бесконтактных платежей по картам в зоне SEPA» [5] и «Роли в управлении услугами по бесконтактным платежам EPC–GSMA, совершаемым с использованием мобильного телефона – требования и технические условия» [6], подготовленных совместно EPC и Ассоциацией GSM (GSMA).

Элементы уровня 3 по определению находятся по большей части в конкурентном пространстве. Однако для преодоления потенциальной сложности работы пользователя с мобильным телефоном и обеспечения возможности контакта будет предложено минимальное количество методических рекомендаций. В них будут представлены картины поведения реальных клиентов и, если это применимо, будут определены минимальные требования по безопасности для обеспечения надежности бизнес-цепочек в интересах клиентов. Примеры областей, оставленных полностью открытыми для конкуренции между различными PSP, – ценообразование, конкретные действия пользователя, управление рисками, отчетность, совместный маркетинг с предприятиями торговли (услуг) или другими поставщиками услуг, продвижение торговой марки и т.д.

2.5. РУКОВОДЯЩИЕ ПРИНЦИПЫ ВЫСОКОГО УРОВНЯ

EPC рассматривает следующие принципы высокого уровня в поддержку своей концепции по платежам SEPA, совершаемым с использованием мобильного телефона.

1. Чтобы помочь в разработке стандартов и правил по проведению платежей посредством мобильного телефона, EPC принимает за основу существующие платежные средства SEPA[6].

2. Поставщики платежных услуг должны иметь возможность диверсифицировать предлагаемые ими услуги с достаточной свободой, чтобы не препятствовать конкуренции на существующем рынке платежных услуг.

3. Обеспечение легкости, удобства и доверия для конечных потребителей (выгодоприобретатели / потребители и получатели / предприятия торговли (услуг)) при проведении платежей посредством мобильного телефона для инициирования самого платежа важно для дальнейшего развития в этой области.

4. Потребители должны иметь возможность совершать платежи с использованием мобильного телефона в зоне SEPA независимо от страны, где первоначально оформлена подписка на услуги по совершению платежей SEPA с использованием мобильного телефона.

5. Платежные обязательства заинтересованных сторон (включая плательщиков / потребителей и получателей / предприятия торговли) не отличаются от платежных обязательств по существующим платежным средствам SEPA.

6. PSP самостоятельно решает, является ли его пользовательский графический интерфейс, включая бренды и логотипы, бренды карточных схем, тип платежа и т.д., соответствующим. Пользовательский интерфейс мобильных телефонов должен поддерживать эти разработки.

7. Потребители не должны быть привязаны к конкретному MNO и конкретному мобильному оборудованию, а должны сохранить имеющуюся у них возможность переходить от одного PSP к другому.

8. Если в платеже, совершаемом посредством мобильного телефона, используется элемент безопасности (SE), который поддерживается несколькими PSPs, клиент должен иметь возможность использовать все предлагаемые ему услуги в области мобильных платежей с помощью одного мобильного телефона, а также выбрать соответствующее приложение для мобильных платежей, которое будет использоваться для конкретной платежной операции.

9. В основе платежей, совершаемых посредством мобильного телефона, должны лежать технологии и инфраструктура, которые могут широко использоваться в этой области. Однако все указанные технологии и системы должны находиться в сфере права на использование интеллектуальной собственности.

10. Существующие модели и структуры обслуживания, используемые для платежей SEPA, должны быть сохранены максимально.

11. Все данные персонификации PSP по клиентам при осуществлении платежей посредством мобильного телефона должны оставаться собственностью клиентского PSP.

12. По платежам MCPs клиенты должны совершать одинаковые действия при осуществлении бесконтактных платежей посредством мобильного телефона независимо от места проведения операции. Это включает взаимодействие с принимающим устройством (POI).

---

[6] Обратите внимание, что это не исключает другие виды платежей, совершаемых с использованием мобильного телефона и основанных не на платежных средствах SEPA (см. также разделы 1.3 и 1.4).

3. ПЛАТЕЖИ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО ТЕЛЕФОНА, В ЗОНЕ SEPA

3.1. ДЕНЬ ИЗ ЖИЗНИ ПОТРЕБИТЕЛЯ, ИСПОЛЬЗУЮЩЕГО МОБИЛЬНЫЕ ПЛАТЕЖИ

В настоящем разделе говорится о том, каким образом повседневная жизнь потребителя может стать легче благодаря использованию мобильного телефона для проведения платежей. В данном разделе представлено несколько примеров, иллюстрирующих некоторые практики применения. Следует отметить, что существует много других вариантов и примеров проведения платежей, инициированных при помощи мобильного телефона.

Г-н Гарсия, часто пользующийся мобильным телефоном и ведущий очень активный образ жизни, является предполагаемым клиентом данного PSP. В частности, он использует свой мобильный телефон не только для звонков и отправки текстовых сообщений. Наличие в любой момент под рукой и удобство эксплуатации этого карманного устройства привлекает также возможностью подключения новых услуг. В частности, ощущение полного контроля над этим устройством создает условия для уверенного проведения платежей. Рисунок 3 отражает типичный день из его жизни.

Рисунок 3. **День из жизни г-на Гарсии**

3.1.1. ПЛАТЕЖ ЗА ПОЕЗДКУ НА ПОЕЗДЕ НА РАБОТУ

На дисплее мобильного телефона предлагается продлить проездной билет. Г-н Гарсия принимает решение уйти из очереди и продлить проездной билет в билетном автомате с помощью своего банковского счета для операций с использованием платежных карт. Он непосредственно подтверждает продление проездного билета посредством мобильного телефона, а затем подносит телефон к билетному автомату. Вернувшись к турникету, он может теперь пройти на платформу, чтобы сесть на поезд, и благодаря такой оперативности успевает на свой обычный поезд в 8:15.

3.1.2. МОБИЛЬНЫЙ ДОСТУП К КАЧЕСТВЕННОМУ ОТДЫХУ

Комфортно усевшись в поезде, г-н Гарсия использует свой мобильный телефон для развлечения во время поездки, зайдя на сайт в сети Интернет для просмотра видео по запросу. Однако сайт сообщает ему, что услуга платная. С помощью простой опции меню на дисплее своего мобильного телефона г-н Гарсия выбирает свою кредитную карту (реквизиты которой введены в память мобильного телефона) для оплаты услуг сайта. Затем он получает доступ к выбранному фильму.

3.1.3. ОПЛАТА БИЗНЕС-ЛАНЧА

Во время обеда г-н Гарсия приглашает потенциального клиента в ресторан. Проверив счет, он принимает решение использовать для оплаты корпоративную карту, реквизиты которой введены в память мобильного телефона. Он делает это, выбрав соответствующую карту в опциях меню на дисплее своего

мобильного телефона, и разрешает платежную операцию, введя свой мобильный код идентификации и просто приблизив телефон к кассовому терминалу, предложенному официантом.

3.1.4. ПОСЕЩЕНИЕ БУФЕТА В ТЕЧЕНИЕ РАБОЧЕГО ДНЯ

В середине дня г-н Гарсия делает небольшой перерыв в работе, чтобы восстановить силы. Недалеко от его офиса находится небольшой буфет с несколькими торговыми автоматами. Выбрав свою любимую газировку, он подносит к торговому автомату мобильный телефон, чтобы совершить операцию с помощью своей платежной карты. Одновременно с платежом торговый автомат (если для платежа используется мобильный телефон) показывает веб-сайт производителя газировки со специальным предложением. Затем г-н Гарсия загружает купон на скидку в свой мобильный телефон для использования при следующей покупке газировки.

3.1.5. ПОКУПКА ПРОДОВОЛЬСТВЕННЫХ ТОВАРОВ

По пути домой г-н Гарсия останавливается у местного супермаркета, чтобы купить продукты. На кассе он сначала отправляет в кассовый терминал свой купон на скидку за покупку газировки. Затем он решает использовать свою расчетную карту, реквизиты которой внесены в его мобильный телефон, чтобы оплатить оставшуюся сумму. Он делает это, выбрав расчетную карту из опций в меню на дисплее телефона. Сначала он подносит его к кассовому терминалу для получения реквизитов платежа и вводит свой универсальный мобильный код в мобильном телефоне. Наконец, он снова подносит мобильный телефон к кассовому терминалу, чтобы подтвердить платеж. После совершения платежа кассовый терминал обновляет карту скидок г-на Гарсии в его мобильном телефоне, записав туда баллы, начисленные за совершенную покупку.

3.1.6. ДИСТАНЦИОННАЯ ПОДПИСКА НА СЕМЕЙНУЮ ИГРУ В СЕТИ ИНТЕРНЕТ

Путешествуя по сети Интернет с помощью домашней игровой консоли, дочь г-на Гарсии нашла новую распространяемую по подписке игру для нескольких участников, которую ей хочется купить. Г-н Гарсия согласен заплатить за игру и вводит номер своего мобильного телефона на экране консоли. Мобильный телефон немедленно показывает запрос на разрешение безакцептного списания. Выбрав эту опцию, г-н Гарсия поручает списать начисленную сумму со своего платежного счета. Затем его дочь может сразу начать играть, а г-н Гарсия уезжает на футбольный матч.

3.1.7. БИЛЕТ НА ФУТБОЛЬНЫЙ МАТЧ

Сегодня вечером г-н Гарсия договорился с друзьями пойти на стадион, чтобы поддержать местную футбольную команду. Вход на стадион он снова оплатил со своего мобильного телефона. Сначала он выбрал соответствующую платежную карту в опциях меню на дисплее телефона. Затем он поднес его к билетному терминалу, который записал в мобильный телефон билет на футбольный матч. После этого г-н Гарсия вошел на стадион, поднеся мобильный телефон к входному турникету.

3.1.8. ВОЗВРАТ ДОЛГА ЗНАКОМОЙ

Во время перерыва в игре знакомая г-на Гарсии предложила купить рыбу с чипсами. Когда она вернулась, г-н Гарсия настоял на том, чтобы вернуть ей деньги. Для этого он выбрал номер ее мобильного телефона в списке контактов в своем мобильном телефоне. Затем, выбрав подходящий платежный счет в опциях меню на дисплее, г-н Гарсия перевел соответствующую сумму на ее счет. Наконец, его знакомая получила сообщение на дисплее своего телефона, подтверждающее получение кредитового перевода.

3.2. ОБЩИЕ СВЕДЕНИЯ О ПЛАТЕЖАХ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО ТЕЛЕФОНА

3.2.1. ВВЕДЕНИЕ

Как сказано в разделе 2.2, платежи, совершаемые с использованием мобильного телефона, представляют собой новый канал для повторного использования существующих платежных средств SEPA.

Платежи, совершенные с использованием мобильного телефона, в широком смысле подразделяются на бесконтактные и дистанционные. При бесконтактных платежах потребитель и торговое предприятие (и/или его оборудование) находятся в одном месте и обмениваются данными друг с другом непосредственно с использованием бесконтактных технологий передачи данных по радио, таких как передача данных при помощи технологии NFC. При дистанционных платежах операция проводится по сетям связи, таким как GSM или сеть Интернет, и может быть совершена независимо от места нахождения плательщика (и/или его оборудования). Чтобы в максимальной степени воспользоваться общей инфра-

структурой для бесконтактных платежей в зоне SEPA, бесконтактные платежи посредством мобильного телефона основываются только на использовании технологии NFC в режиме эмуляции карты.

В зависимости от характера плательщика и получателя, которые могут являться потребителем[7] или предприятием, платежи, совершаемые посредством мобильного телефона, могут также подразделяться на категории «потребитель – потребителю» (C2C), «потребитель – предприятию» (C2B), «предприятие – потребителю» (B2C) и «предприятие – предприятию» (B2B).

В таблице 1 показано, как примеры использования, описанные в разделе 3.1, можно реализовать с помощью существующих платежных средств SEPA. Следует отметить, однако, что каждый пример использования можно реализовать посредством большего числа платежных средств SEPA, что указано в таблице 1. Поэтому пример использования, указанный в таблице, не следует считать образцом данной категории платежей. Кроме того, поскольку в разделе 3.1 представлены только несколько примеров использования, покрываются не все категории, представленные в таблице 1.

Таблица 1. **Иллюстрация мобильных платежей с использованием платежных средств SEPA**

		Кредитовый перевод SEPA	Безакцептное списание SEPA (поручение)	Платежи по карте SEPA
Бесконтактные платежи	C2C			
	C2B			Билет на футбольный матч Покупка продовольственных товаров Посещение буфета в течение рабочего дня
	B2C			
	B2B			Оплата бизнес-ланча
Дистанционные платежи	C2C	Возврат долга знакомой		
	C2B	Платеж за поездку на поезде на работу	Дистанционная подписка на семейную игру в сети Интернет	Мобильный доступ к качественному отдыху
	B2C			
	B2B			

3.2.2. КАТЕГОРИИ ПЛАТЕЖЕЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО ТЕЛЕФОНА, КОТОРЫЕ EPC СЧИТАЕТ ПРИОРИТЕТНЫМИ

Для достижения максимальной потенциальной и общей выгоды от проведения платежей с использованием мобильного телефона EPC намерен содействовать их быстрому внедрению на рынке. В рамках этой стратегии EPC провел исследование рынка в 2008 году для определения приоритетов в своей работе в области платежей, совершаемых с использованием мобильного телефона, исходя из следующих критериев оценки: хозяйственные и экономические аспекты, инфраструктура и выход на рынок, а также последнее, но не менее важное – потенциал рынка.

Анализ различных видов платежей, SCT, SDD и карты SEPA с точки зрения потребителей и предприятий (торговых предприятий) полезен при определении приоритетных сценариев использования и при выявлении пробелов, которые могут стать препятствиями для полной реализации мобильного канала в SEPA .

Примеры использования построены на основе следующих принципов:

- отсутствуют различия между внутренними и трансграничными (в зоне SEPA) операциями;
- характер лежащей в основе покупки выходит за рамки предмета и объема;
- сумма операции и другие лимиты определяются каждым поставщиком платежных услуг и/или схемой.

Кроме того, поскольку пользователи будут инициировать платежи с персональных мобильных устройств, при подготовке примеров использования будут рассматриваться преимущественно:

- потребительские платежи
- или коммерческие платежи (в частности, малый бизнес), инициированные физическими лицами,

которые в целом, таким образом, охватываются теми же примерами использования.

[7] Согласно [19], «потребитель» – это физическое лицо, которое в договорах о платежных услугах, покрываемых [19], действует в целях, выходящих за пределы его коммерческой, хозяйственной или профессиональной деятельности. Таким образом, «предприятие» означает физическое или юридическое лицо, не являющееся потребителем.

3.2.2.1. Анализ бесконтактных платежей, совершаемых с использованием мобильного телефона

В следующей таблице проиллюстрирован уровень приоритета по каждому потенциальному сценарию по бесконтактным платежам в зоне SEPA с использованием мобильного телефона.

Таблица 2. **Бесконтактные платежи, совершаемые с использованием мобильного телефона: приоритеты**

	Карты SEPA	SDD	SCT
C2C			
C2B			
B2C			
B2B			

Низкий приоритет
Средний приоритет
Высокий приоритет

Далее рассматривается каждый из трех указанных видов платежей.

Бесконтактные платежи в зоне SEPA, совершаемые с использованием мобильного телефона

Проанализированы сценарии платежей посредством платежной карты SEPA и определены два основных приоритета: «потребитель – предприятию» (C2B) и «потребитель – потребителю» (C2C, часто именуется P2P).

Типичный платеж по карте – C2B, получателем обычно является предприятие торговли (услуг). Чтобы предложить приемлемую альтернативу денежной наличности для операций на небольшие суммы, в секторе платежных услуг разрабатывается концепция бесконтактных платежей, которые позволяют держателю карты просто поднести карту к платежному терминалу предприятия торговли (услуг), чтобы совершить платеж. Мобильные устройства способны поддерживать такую технологию и поэтому могут использоваться держателем карты вместо физического наличия платежной карты. Таким образом, это перспективное направление становится приоритетным для развития бесконтактных платежей в зоне SEPA, совершаемых с использованием мобильного телефона.

Мобильные устройства открывают возможность для бесконтактных платежей «потребитель – потребителю» (C2C). Конечно, реализация данной разработки зависит от участия платежной системы, но представляется, что эта возможность имеет достаточный потенциал, оправдывающий распределение приоритетов по указанным примерам использования.

Таблица 3. **Бесконтактные платежи в зоне SEPA, совершаемые с использованием мобильного телефона: определение и приоритеты**

Карта SEPA	Потребитель	Предприятие
Потребитель	**C2C** • Обеспечивает практическое решение для персональных платежей, включая замещение чеков и наличных денег • Для достижения более широкого охвата нужна поддержка со стороны карточных схем	**C2B** • Имеется технология, позволяющая использовать мобильные устройства вместо физических карт для бесконтактных платежей по картам SEPA • Торговые предприятия не пострадают от использования мобильных устройств вместо физических карт • Использование мобильных устройств обеспечивает возможности для роста и развития рынка бесконтактных платежей по картам SEPA, а также способствует предложению дополнительных услуг со стороны эмитентов карт
Предприятие	**B2C** • Очень маловероятно, что предприятие будет совершать платеж потребителю по карте, еще менее вероятно, что будут использоваться бесконтактные технологии, и наверняка не будут использоваться бесконтактные мобильные технологии • Даже если карта является картой компании или закупочной картой, держатель карты выступает в качестве потребителя, поэтому сценарий будет такой же, как в случае C2C	**B2B** • Даже если карта является картой компании или закупочной картой, держатель карты выступает в качестве потребителя • Поэтому сценарий будет такой же, как в случае C2B • Отдельные примеры использования не требуются

Низкий приоритет
Средний приоритет
Высокий приоритет

На платежи SEPA «предприятие–предприятию» (B2B) приходится сравнительно небольшая часть всех платежей, совершаемых при помощи платежной карты, и обычно они производятся с использованием карты компании или закупочной карты[8]. Однако когда совершаются эти операции, держатель карты компании фактически ведет себя подобно потребителю, и лежащий в основе платежный процесс идентичен другим платежам в зоне SEPA. Поскольку в настоящем докладе рассматриваются бесконтактные платежи с использованием мобильного телефона, в этом случае поведение держателя карты еще более схоже с поведением потребителя. Поэтому нет необходимости разрабатывать специальные сценарии для платежей B2B в зоне SEPA.

Платежи «предприятие–потребителю» (B2C) обычно ограничиваются возвратом денег, и для них использование мобильных бесконтактных технологий весьма маловероятно.

Бесконтактные платежи по операциям безакцептного списания в зоне SEPA, совершаемые посредством мобильного телефона

Безакцептное списание инициируется PSP получателя, далее средства списываются со счета плательщика. SDDs не могут совершаться бесконтактно и потому не являются предметом рассмотрения в настоящем разделе.

Что касается использования мобильного канала для развития SDDs, здесь могут возникнуть возможности разработки дополнительных услуг на основе поручений пользователей на безакцептное списание и даже возможность передачи поручения на SDD с использованием мобильного устройства.

Бесконтактные кредитовые платежи в зоне SEPA, совершаемые с использованием мобильного телефона

В докладе проанализированы возможные примеры использования бесконтактных платежей посредством мобильного телефона с целью распределения приоритетов. Во всех случаях, когда платеж совершается с использованием бесконтактных технологий, в основе лежит платеж, совершаемый путем введения реквизитов платежной карты SEPA.

Существуют возможности совершения некоторой операции, например продления проездного билета, с помощью мобильных бесконтактных технологий в результате кредитового перевода в зоне SEPA. Однако поручение и авторизация по кредитовому переводу передаются в основном дистанционно, что облегчает последующие операции.

Предполагается, что если будет разработана схема C2C для SCT, то она может быть усовершенствована для сочетания мобильных и бесконтактных технологий при идентификации получателя, но поручение и авторизация все равно могут передаваться плательщиком дистанционно. Поскольку такой схемы нет и поскольку сам платеж не будет с технической точки зрения бесконтактным, приоритет не может быть определен.

3.2.2.2. Анализ дистанционных платежей, совершаемых с использованием мобильного телефона

В нижеследующей таблице показан уровень приоритета по каждому потенциальному сценарию по MRP SEPA в соответствии с анализом, выполненным EPC для разработки своей стратегии по платежам, совершаемым с использованием мобильного телефона.

Таблица 4. **Дистанционные платежи, совершаемые с использованием мобильного телефона: приоритеты**

	Карты SEPA	SDD	SCT
C2C			
C2B			
B2C			
B2B			

Низкий приоритет
Средний приоритет
Высокий приоритет

В следующих разделах рассматривается каждый из трех указанных видов платежей.

Дистанционные платежи в зоне SEPA, совершаемые с использованием мобильного телефона (MRP)

Операции по картам чаще всего производятся держателями карт, когда получатели являются предприятиями. Хотя понятно, что некоторые операции совершаются с помощью закупочных карт и карт компаний / корпоративных карт, эти операции инициируются и авторизуются так же, как и потребительские. Следовательно, нет необходимости разрабатывать отдельные примеры использования по этим сценариям.

[8] Закупочная карта – вид корпоративных платежных карт, используемых для закупки оборудования, материалов и товаров для вспомогательных служб и офиса, учета и контроля над расходами вспомогательного и непроизводственного профиля.

В том виде, как сейчас организованы процессы платежей с использованием платежных карт, MRPs SEPA считаются операциями «Card-Not-Present» (CNP – «карта отсутствует»). Это означает, что все характеристики и вопросы, относящиеся к операциям CNP, сохраняют актуальность и здесь.

Требуются некоторые усовершенствования, касающиеся авторизации и большей определенности для получателя платежа, чтобы предприятия торговли (услуг) были больше заинтересованы в проведении трансакций с использованием платежных карт. Хотя эти вопросы решаются, но существуют некоторые возможности для улучшений именно в отношении платежей, совершаемых с использованием мобильного телефона, для развития платежей, осуществляемых по каналам SEPA.

Операции по оплате товаров (услуг) с использованием платежных карт «потребитель – потребителю» перспективны для мобильного канала. Некоторые платежные системы уже предоставляют такие услуги на праве владения, но их широкое внедрение на рынке в значительной степени зависит от операционной совместимости всех участвующих платежных систем, осуществляющих свою деятельность с использованием платежных карт.

Как уже сказано, объем платежей посредством банковской карты, совершаемых коммерческими организациями, меньше по сравнению с потребительскими платежами, но, когда они совершаются, они подпадают под «потребительские» примеры использования.

В случае вероятного возврата средств предприятиями торговли (услуг) эти операции будут инициированы с использованием мобильного устройства, и поэтому они не описываются приведенными в докладе примерами использования.

Таблица 5. **Дистанционные платежи в зоне SEPA, совершаемые посредством мобильного телефона: определение и приоритеты**

Карта SEPA	Потребитель	Предприятие
Потребитель	**C2C** • Обеспечивает практическое решение для персональных платежей, включая замещение чеков и денежной наличности • Требует сотрудничества карточных схем • Существующий номер карты может служить практическим идентификатором получателя • Возможность быстрого роста	**C2B** • Уже доступно через браузеры и приложения • Определенность результата по операциям CNP заинтересует торговые предприятия • Ожидаются изменения, касающиеся именно мобильного канала
Предприятие	**B2C** • Очень маловероятно, что предприятие будет совершать платеж потребителю по карте • Даже если карта является картой компании или закупочной картой, держатель карты выступает в качестве потребителя, поэтому сценарий будет такой же, как в случае C2C • Малое предприятие, принимающее платежи, совершаемые с использованием мобильного телефона, может инициировать возврат средств по мобильному каналу, но в большинстве случаев это маловероятно	**B2B** • Даже если карта является картой компании или закупочной картой, ее держатель выступает в качестве потребителя • Поэтому сценарий будет такой же, как в случае C2B • Может оказаться очень хорошим вариантом замещения чеков для малых предприятий

Дистанционные платежи в зоне SEPA, совершаемые с использованием мобильного телефона путем безакцептного списания денежных средств (SDD)

Хотя SDDs прямо не исключаются при рассмотрении канала мобильной связи, операции безакцептного списания, учитывая их особый характер, инициируются (почти всегда) предприятиями, поэтому примеры использования с инициированием потребителями не имеют большого значения.

Кроме того, предприятия, инициирующие SDDs, обычно не используют при этом мобильное устройство, поэтому примеры использования с такими сценариями также не имеют большого значения.

Что касается использования канала мобильной связи для развития SDDs, то существуют возможности разработки дополнительных услуг посредством безакцептного списания денежных средств пользователей и возможность передачи поручения SDD с использованием мобильного устройства.

Дистанционные кредитовые переводы в зоне SEPA, совершаемые с использованием мобильного телефона (SCT)

SCT предоставляют возможность реализации платежей SEPA на платформе мобильного телефона. Поскольку платеж является переводом PSP–PSP, он в равной степени подходит для потребительских, коммерческих и правительственных (бюджетных) платежей. Эта категория платежей, если она будет полностью реализована, также позволяет отказаться от чеков, денежной наличности и других бумажных платежных средств в тех странах, где они все еще используются (в частности, во Франции, Ирландии и Соединенном Королевстве).

Таблица 6. **Дистанционные платежи в зоне SEPA, совершаемые с использованием мобильного телефона путем безакцептного списания: определение и приоритеты**

SDD	Потребитель	Предприятие
Потребитель	**C2C** • Потребители (обычно) не инициируют SDDs • Если это происходит, то потребитель ведет себя подобно предприятию • Поэтому см. сценарий B2C	**C2B** • Потребители обычно не инициируют SDDs • Еще менее вероятно, что потребитель будет инициировать SDD по коммерческому дебитору • Если это происходит, то потребитель ведет себя подобно предприятию • Поэтому см. сценарий B2B
Предприятие	**B2C** • Маловероятно, что предприятие будет инициировать SDD с использованием мобильного устройства • Имеется возможность предложения услуг по передаче поручений в мобильном канале	**B2B** • Маловероятно, что предприятие будет инициировать SDD с использованием мобильного устройства • Имеется возможность предложения услуг по передаче поручений в мобильном канале

При реализации SCT с использованием канала мобильной связи необходимо решить два очевидных вопроса:

• для получателей, в частности предприятий торговли (услуг), работающих с потребителями, во многих случаях требуется некоторая уверенность в немедленном (моментальном) проведении платежа или его подтверждение;

• для плательщиков, в частности когда платеж производится предприятию торговли (услуг), которое заранее не было зарегистрировано в службе электронных платежей (см. раздел 5.2.2.4), важно использовать соответствующий идентификатор получателя. В большинстве случаев плательщику нецелесообразно вводить IBAN, BIC и другие реквизиты получателя при использовании мобильного устройства.

В зависимости от характера взаимоотношений между двумя сторонами необходимо рассмотреть различные практические вопросы, исходя из уровня доверия потребителей товаров (услуг) и требований удобства использования платежного средства. Ниже рассмотрены данные вопросы :

1. Высокий уровень доверия, удобство не имеет значения – могут использоваться обычные SCTs. Плательщик готов ввести все реквизиты получателя. Получателю не требуется немедленное подтверждение.

2. Высокий уровень доверия, но удобство имеет значение – плательщику требуется решение, позволяющее облегчить ввод информации для идентификации получателя. Дополнительные требования для получателя отсутствуют.

3. Низкий уровень доверия, удобство важно – в данном случае, помимо требований плательщика, указанных в пункте 2, получателю требуется некоторая уверенность в проведении платежа или даже его подтверждение.

В разделе 5 будет представлен пример использования по каждому случаю с дополнительным описанием типа плательщика и получателя, являющихся потребителем или предприятием. В некоторых случаях предприятия ведут себя подобно потребителям, инициируя платежи с использованием канала мобильной связи (в частности, малые предприятия), а потребители-получатели ведут себя подобно предприятиям, т.е. им требуется подтверждение выполнения платежа.

Таблица 7. **Дистанционные кредитовые переводы в зоне SEPA посредством мобильного телефона: определение и приоритеты**

SCT	Потребитель	Предприятие
Потребитель	**C2C** • Предлагается практическое решение для быстрых персональных платежей, включая замещение чеков и денежной наличности • Требуется практическое решение для идентификации получателя (решением может быть мобильный номер или номер «псевдоним») • Может потребоваться центральный архив данных • Уверенность в результате будет способствовать выбору данной технологии • Возможность быстрого роста	**C2B** • Предлагается практическое решение для быстрых персональных платежей, включая замещение чеков и денежной наличности • Требуется практическое решение для идентификации получателя для менее крупных предприятий • Определенность результата по платежам SCT будет способствовать принятию технологии торговыми предприятиями
Предприятие	**B2C** • Маловероятно использование предприятиями и крупными компаниями, но может быть привлекательным вариантом для малых предприятий • Используя мобильный канал связи для инициирования SCTs, предприятие действует подобно потребителю • Следовательно, такой же сценарий, как в случае C2C	**B2B** • Маловероятно использование предприятиями и крупными компаниями, но может быть привлекательным вариантом для малых предприятий • Используя мобильный канал для инициирования SCTs, предприятие действует подобно потребителю • Следовательно, такой же сценарий, как в случае C2B

4. БЕСКОНТАКТНЫЕ ПЛАТЕЖИ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО ТЕЛЕФОНА ПУТЕМ ВВЕДЕНИЯ РЕКВИЗИТОВ ПЛАТЕЖНОЙ КАРТЫ

4.1. ВВЕДЕНИЕ

В настоящем разделе представлено краткое описание бесконтактных платежей в зоне SEPA (MCP) посредством мобильного телефона, которые определяются как бесконтактные платежи по картам SEPA [5], совершаемые держателем карты (потребитель) с использованием специального приложения MCP и технологии NFC. Приложение MCP предоставляется эмитентом и загружается в элемент безопасности (SE), независимо предоставляемый эмитентом SE, которым может быть эмитент MCP, MNO или другая доверенная третья сторона (TTP). Независимо от используемого SE введение бесконтактной мобильной технологии должно быть направлено на достижение такого же уровня безопасности, как в существующих (бесконтактных) платежах в зоне SEPA [5].

4.2. ПРИМЕРЫ ПРОВЕДЕНИЯ БЕСКОНТАКТНЫХ ПЛАТЕЖЕЙ В ЗОНЕ SEPA ПОСРЕДСТВОМ МОБИЛЬНОГО ТЕЛЕФОНА

В настоящем разделе описываются примеры использования MCP, приведенные в разделе 3.1. Следует отметить, что описанные действия пользователя являются только иллюстративным примером, поскольку возможны различные способы реализации по каждому примеру использования. Если упоминаются аспекты пользовательского интерфейса мобильного телефона, то также лишь в качестве примера.

В настоящем разделе описаны три основных вида бесконтактных мобильных платежей в зоне SEPA «потребитель – предприятию» (C2B), независимо от типа используемой карты (кредитная, расчетная). Вариант B2B реализуется, если потребитель является предприятием.

4.2.1. MCP 1 TAP AND GO («ПРИСОЕДИНЯЙСЯ К СЕТИ И ДЕЙСТВУЙ»)

Сценарий, представленный на рисунке 4, демонстрирует возможную кассовую процедуру в магазине продовольственных товаров при совершении платежной операции на небольшую сумму.

Перед началом исполнения сценария потребитель должен подписаться на услугу по предоставлению данного вида платежа с использованием мобильного телефона по своей платежной карте и выбрать ее в качестве платежного средства по умолчанию в меню конфигурации мобильного кошелька. В качестве опции потребитель вводит свой мобильный код, чтобы открыть приложение MCP до начала выполнения операции (режим ручной настройки).

На рисунке 4 отражены следующие действия:

1. Сначала предприятие торговли (услуг) вводит сумму операции на терминале POI.

2. Для платежа автоматически используется платежная карта, заранее выбранная потребителем в своем мобильном телефоне. Поэтому, чтобы подтвердить платежную операцию, ему достаточно поднести мобильный телефон к терминалу POI с включенной технологией NFC.

3. Затем операция обрабатывается как стандартная операция SCP.

4. Предприятие торговли (услуг) имеет возможность проверить платеж.

Рисунок 4. **MCP 1 Tap and Go**

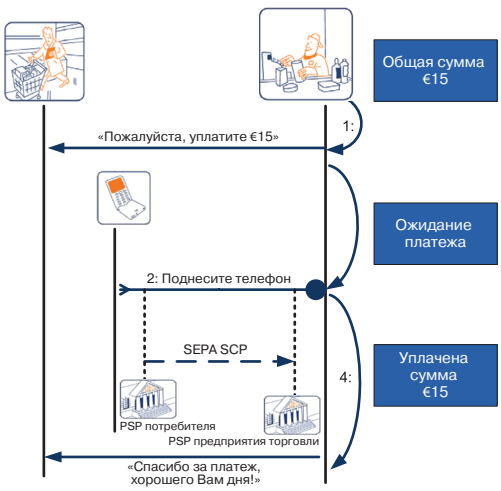


Таблица 8. **MCP 1 Tap and Go**

MCP 1 Tap and Go – характеристики	
Категория	«Потребитель – предприятию» (C2B). Также относится к B2B.
Тип связи	Бесконтактная
Платежное средство	Карта SEPA – любой тип (SCF)
Инициатор платежа	Предприятие торговли (услуг)
Необходимые условия	• Потребитель должен иметь подписку на услугу по платежам посредством мобильного телефона • Потребитель должен заранее выбрать платежную карту, используемую по умолчанию в его мобильном телефоне. В качестве опции потребитель вводит свой уникальный мобильный код, чтобы открыть приложение MCP до начала выполнения операции (режим ручной настройки) • Предприятие торговли (услуг) должно иметь терминал POI с включенной технологией NFC • Согласие предприятия торговли (услуг)
Способ подтверждения платежа	Поднести мобильный телефон к терминалу POI с включенной технологией NFC
Выгоды для предприятия торговли	• Доступ к более широкой клиентской базе • Эффективность обработки платежей • Дополнительные услуги, такие как баллы, купоны и т.д.
Выгоды для потребителя	• Удобство, мобильность • Уменьшается потребность в наличных деньгах • Замещение чеков (или наличных денег) • Уменьшение очередей
Проблемы	В канале мобильной связи по сравнению с бесконтактными платежами по картам проблемы отсутствуют

4.2.2. MCP 2 DOUBLE TAP

Сценарий, представленный на рисунке 5, демонстрирует возможную кассовую процедуру в магазине продовольственных товаров при совершении платежной операции на крупную сумму, когда потребитель вводит свой уникальный мобильный код в мобильном телефоне.

Перед началом исполнения сценария потребитель должен подписаться на услугу осуществления платежей посредством мобильного телефона по своей платежной карте и выбрать ее в качестве платежного средства по умолчанию в меню конфигурации мобильного кошелька в мобильном телефоне.

На рисунке 5 отражены следующие действия:

1. Сначала предприятие торговли вводит сумму операции на терминале POI.

2. Потребитель подносит свой мобильный телефон к терминалу POI с включенной технологией NFC.

3. Для платежа автоматически используется платежная карта, заранее выбранная в мобильном телефоне потребителя. Поэтому, чтобы подтвердить платежную операцию, потребителю достаточно ввести свой мобильный код[9] в мобильном телефоне.

4. Затем потребитель снова подносит свой мобильный телефон к терминалу POI с включенной NFC.

5. Затем операция обрабатывается, как стандартная операция SCP в зоне SEPA.

6. Предприятие торговли имеет возможность проверить платеж.

[9] По соображениям безопасности код аутентификации потребителя, так называемый «мобильный код», должен отличаться от PIN-кода карты, используемого для совершения платежных операций по карте на контактной основе. Дополнительные инструкции приведены в [5].

Рисунок 5. **MCP 2 Double Tap**

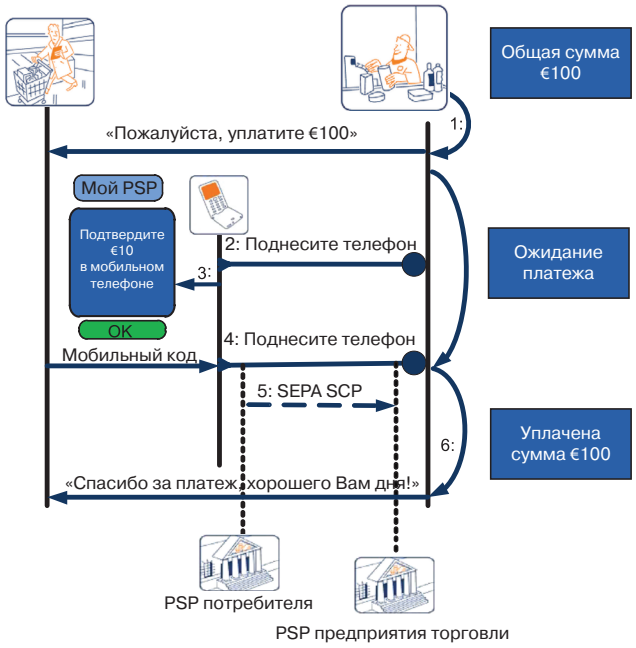


Таблица 9. **MCP 2 Double Tap**

MCP 2 Double Tap – характеристики	
Категория	«Потребитель – предприятию» (C2B). Также относится к B2B.
Тип связи	Бесконтактная
Платежное средство	Карта SEPA – любой тип (SCF)
Инициатор платежа	Предприятие торговли
Необходимые условия	• Потребитель должен иметь подписку на услугу бесконтактных платежей, совершаемых с использованием мобильного телефона • Потребитель должен заранее выбрать платежную карту, используемую по умолчанию, в своем мобильном телефоне • Торговое предприятие должно иметь терминал POI с включенной технологией NFC • Согласие предприятия торговли
Способ подтверждения платежа	• Мобильный код; поднести мобильный телефон к терминалу POI с включенной технологией NFC
Выгоды для предприятия торговли	• Доступ к более широкой клиентской базе • Эффективность обработки платежей • Дополнительные услуги, такие как баллы, купоны и т.д.
Выгоды для потребителя	• Удобство, мобильность • Уменьшается потребность в наличных деньгах • Замещение чеков (или наличных денег)
Проблемы	Обучение, готовность принять новый способ платежа со стороны потребителя и предприятия торговли

4.2.3. MCP 3 SINGLE TAP И PIN

Сценарий, представленный на рисунке 6, демонстрирует возможную кассовую процедуру в магазине продовольственных товаров при совершении платежной операции на крупную сумму, когда POI торгового предприятия – это подключенный к сети Интернет терминал и потребитель вводит свой PIN-код в POI.

Перед началом исполнения сценария потребитель должен подписаться на услугу осуществления платежей посредством мобильного телефона по своей платежной карте и выбрать ее в качестве платежного средства по умолчанию в меню конфигурации мобильного кошелька.

На рисунке 6 отражены следующие действия:

1. Сначала предприятие торговли вводит сумму операции на терминале POI.

2. Потребитель подносит свой мобильный телефон к терминалу POI с включенной технологией NFC.

3. Для платежа автоматически используется платежная карта, заранее выбранная в мобильном телефоне потребителя. Потребитель должен ввести свой PIN-код на терминале POI, чтобы завершить операцию. Информация о текущей операции (например, запрошенной онлайн-операции на заданную сумму) может также отображаться на дисплее мобильного телефона.

4. Потребитель вводит свой PIN-код[10] на терминале POI, чтобы подтвердить платежную операцию.

5. Затем операция обрабатывается как стандартная операция SCP в зоне SEPA.

6. Предприятие торговли может проверить платеж.

Рисунок 6. **MCP 3 Single Tap и PIN**

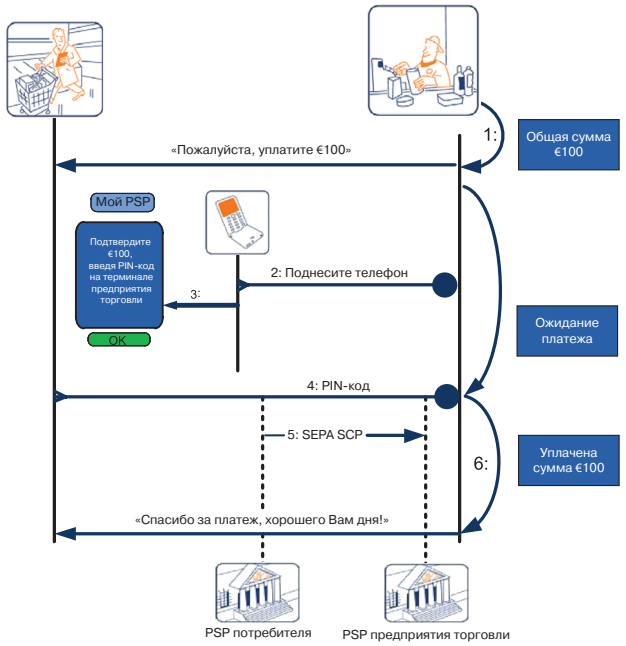


Таблица 10. **MCP 3 Single Tap и PIN**

MCP 3 Single Tap и PIN – характеристики	
Категория	«Потребитель – предприятию» (C2B). Также относится к B2B
Тип связи	Бесконтактная
Платежное средство	Карта SEPA – любой тип (SCF)
Инициатор платежа	Предприятие торговли
Необходимые условия	• Потребитель должен иметь подписку на услугу бесконтактных платежей, совершаемых с использованием мобильного телефона • Потребитель должен заранее выбрать платежную карту, используемую по умолчанию, в своем мобильном телефоне • Предприятие торговли должно иметь терминал POI с включенной технологией NFC • Согласие предприятия торговли
Способ подтверждения платежа	Ввод PIN-кода на терминале POI
Выгоды для предприятия торговли	• Доступ к более широкой клиентской базе • Дополнительные услуги, такие как баллы, купоны и т.д.
Выгоды для потребителя	• Удобство, мобильность • Уменьшение потребности в наличных деньгах • Замещение чеков (или наличных денег)
Выгоды для PSP	Это бесконтактное платежное решение может также использоваться в банкоматах
Проблемы	Особые проблемы в канале мобильной связи по сравнению с операциями, совершаемыми посредством платежной карты, отсутствуют

4.3. ЭКОСИСТЕМА

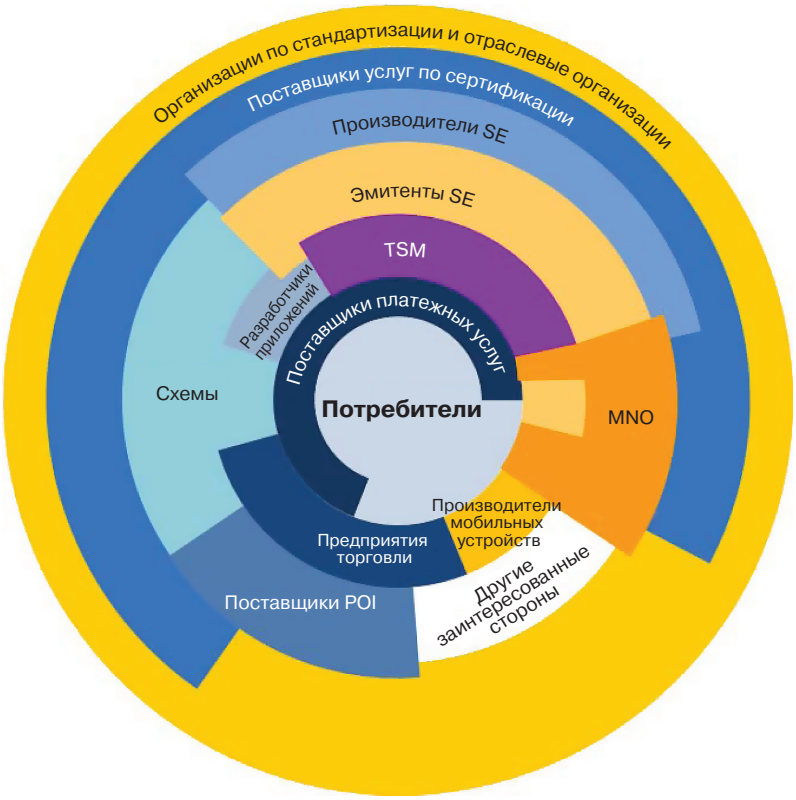
4.3.1. ВВЕДЕНИЕ

По определению любой вид экосистемы платежей, совершаемых с использованием мобильного телефона, предусматривает роль PSPs, отвечающих за сохранность информации. Несмотря на то, что доклад не предусматривает экономического обоснования по PSP на рынке платежей посредством мобильного телефона (поскольку это относится к конкурентному пространству), в нем отражено, что хорошее обоснование должно существовать.

MCP представляет новую экосистему с новыми участниками. Даже если главные участники операций на основе MCP те же, что и для «классического» платежа, MCPs должны основываться на ряде элементов технической инфраструктуры, характерных для мобильной среды. Особый интерес представляют мобильные телефоны, элементы безопасности (SE) и серверные схемы MCP.

[10] Тот же, что и PIN-код, используемый для совершения платежных операций по карте на контактной основе.

Рисунок 7. **Бизнес-экосистема MCP**

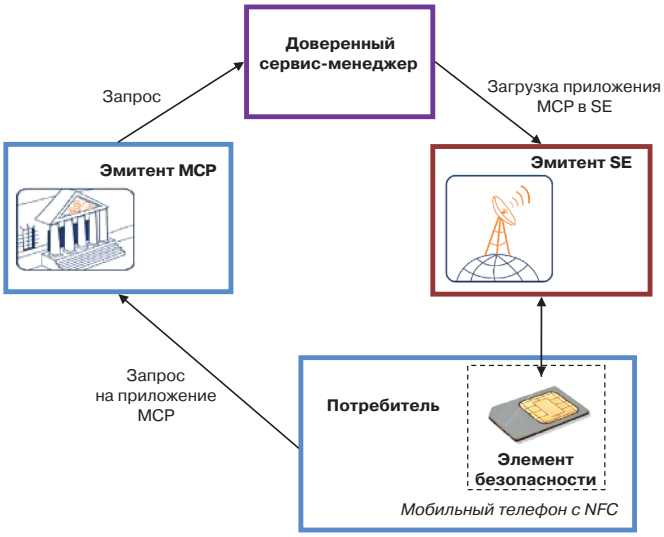


В связи со сложностью этой экосистемы контактными точками на рисунке обозначены только самые важные деловые отношения. В центре бизнес-экосистемы MCP находится потребитель. Последний является клиентом не только поставщика платежных услуг, но также предприятия торговли, MNO, производителя мобильного оборудования и потенциально эмитента SE.

4.3.2. НОВЫЕ ЗАИНТЕРЕСОВАННЫЕ СТОРОНЫ

Как сказано выше, наиболее заметной заинтересованной стороной в экосистеме MCP является эмитент SE. Это MNO в случае универсальной карты с интегральной схемой (UICC), производитель телефонов или эмитент MCP в случае встроенного SE (см. раздел 4 в [5]) и т.д. В любом случае эмитент MCP может воспользоваться услугами так называемого доверенного сервис-менеджера (TSM) для управления своим приложением. TSM является доверенной третьей стороной (TTP), обеспечивающей лучшую расширяемость, когда несколько эмитентов MCP должны осуществлять коммерческое и техническое взаимодействие с несколькими эмитентами SE. Как показано на рисунке 8, эмитенты MCP, TSMs и эмитенты SE сотрудничают по вопросу предоставления приложений MCP и их управления.

Рисунок 8. **Обеспечение приложения MCP для SE**



Чтобы экосистема была открытой, могут существовать многие TSMs, конкурирующие в области предоставления услуг для эмитентов SE и эмитентов MCP.

Другими новыми заинтересованными сторонами могут выступать:

- производители SE;
- разработчики приложений (приложение MCP, AAUI, мобильный кошелек и т.д.);
- производители мобильного оборудования;
- организации, осуществляющие сертификацию инфраструктуры (например, SEs, приложения MCP, POI и т.д.).

4.3.3. МОДЕЛИ ОБСЛУЖИВАНИЯ

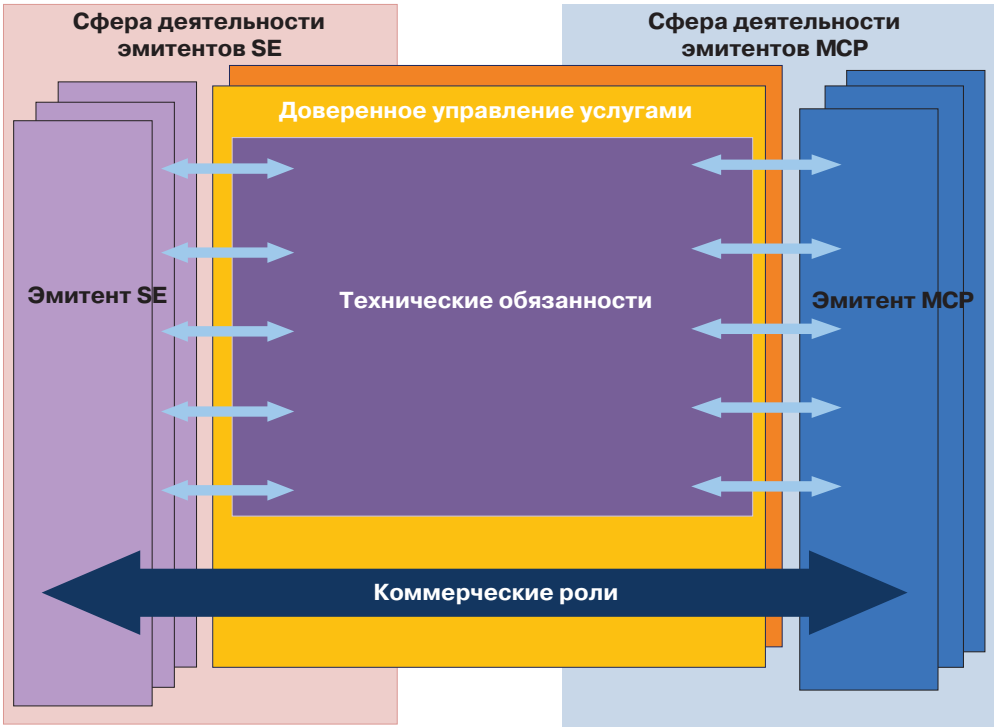
4.3.3.1. Платежная операция

MCP не меняет лежащую в основе платежную операцию по карте SEPA. Следовательно, модель обслуживания последней остается без изменений (см. также раздел 4.4).

4.3.3.2. Обеспечение и управление

Для создания обширной экосистемы поставщиков услуг, выполняющих функции TSM, EPC и GSMA совместно разрабатывают требования и технические условия по обязанностям управления услугами MCP по приложениям, находящимся в UICC [6]. В дальнейшем EPC разделил эти требования и технические условия в соответствии с двумя дополнительными типами SE: встроенными и съемными (такими, как карты SD) [5].

Рисунок 9. **Обеспечение и управление для MCP**

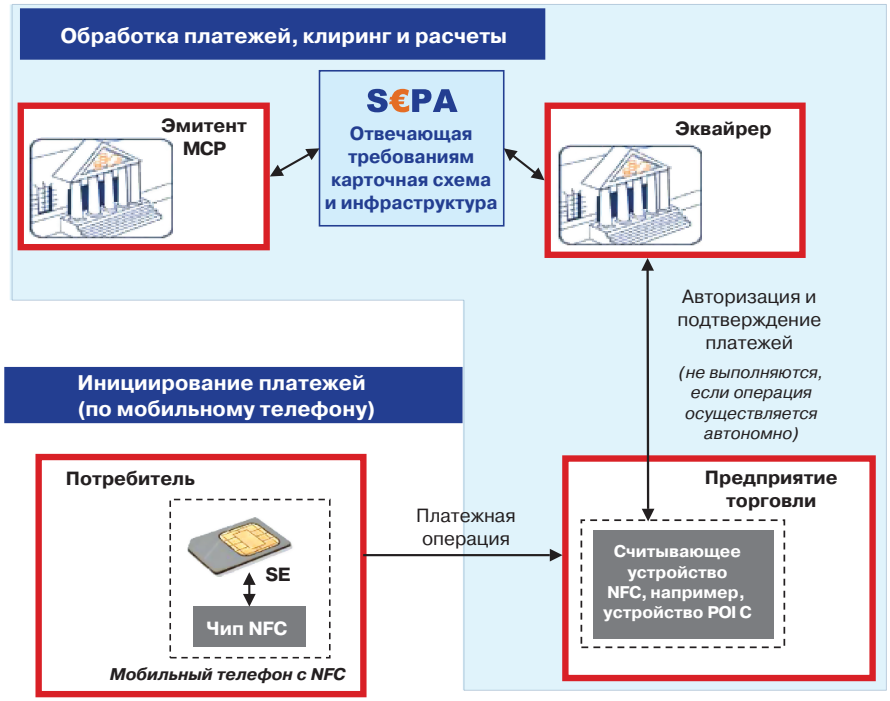


Многие модели обслуживания могут быть реализованы путем передачи различных технических и коммерческих обязанностей одному или нескольким TSMs, включая трехсторонние и четырехсторонние модели обслуживания. Более подробная информация приведена в [5] и [6].

4.4. АРХИТЕКТУРА ВЫСОКОГО УРОВНЯ

Как показано на рисунке 10, основными участниками, вовлеченными в операции на основе MCP, являются те же, что и в случае «классического» платежа путем введения реквизитов платежной карты SEPA. Платежная операция выполняется путем повторного использования существующих устройств для принятия бесконтактных платежей SEPA, а необходимые серверные приложения и операционная инфраструктура уже используются для проведения платежей путем введения реквизитов платежной карты SEPA (см. [4]).

Рисунок 10. **Операция МСР**



5. ДИСТАНЦИОННЫЕ ПЛАТЕЖИ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО ТЕЛЕФОНА

5.1. ВВЕДЕНИЕ

В контексте доклада дистанционные платежи, совершаемые с использованием мобильного телефона (MRPs), – это платежи SEPA (SCT, SDD, SCP), инициированные посредством мобильного телефона, при том что операция совершается по каналу мобильной связи (например, GSM, мобильная сеть Интернет и т.д.) и может осуществляться независимо от места нахождения плательщика (и/или его оборудования). Это означает, что платежная операция не зависит от физического контакта с POI, таким как кассовый терминал.

5.2. ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ ДИСТАНЦИОННЫХ ПЛАТЕЖЕЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО ТЕЛЕФОНА

5.2.1. ДИСТАНЦИОННЫЕ ПЛАТЕЖИ ПО КАРТАМ SEPA, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО ТЕЛЕФОНА

Следующие примеры использования основаны на SCP в качестве основного платежного средства SEPA.

5.2.1.1. Платеж по карте SEPA потребителя – предприятию посредством введения реквизитов платежной карты SEPA SCP 1 – основной (C2B)

В этом сценарии, показанном на рисунке 11, потребитель использует свой мобильный телефон, чтобы совершить платеж предприятию торговли (услуг), которое предоставляет товары (услуги) (например, мобильный контент). Схема B2B реализуется, когда потребитель является предприятием.

Последовательность действий в этом примере подобна дистанционному платежу по карте SEPA с использованием ПК по сети Интернет.

На рисунке 11 приведены следующие действия:

1. Зайдя в сеть Интернет с помощью своего мобильного телефона (так называемый «мобильный Интернет») или путем использования специального приложения MRP, потребитель переходит в расчетный раздел на сайте предприятия торговли (услуг).

2. Сайт предприятия торговли (услуг) выводит платежную информацию на дисплей мобильного телефона потребителя.

3. Потребитель вводит реквизиты своей платежной карты (например, номер карты, дату истечения срока действия и защитный код карты) и инициирует операцию SCP.

4. После авторизации платежа посредством введения реквизитов платежной карты SEPA он обрабатывается.

5. Предприятие торговли (услуг) передает потребителю товар (услуги).

Рисунок 11. **Платеж посредством введения реквизитов платежной карты SEPA потребителя – предприятию (SCP 1)**

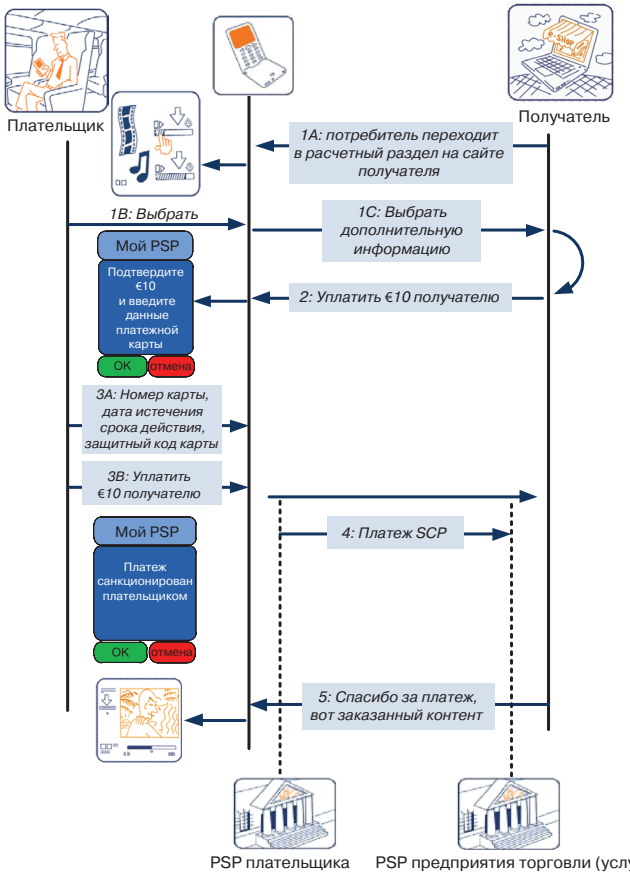


Таблица 11. **Платеж посредством введения реквизитов платежной карты SEPA потребителя – предприятию (SCP 1)**

Кредитовый перевод SEPA потребителя – предприятию торговли	
Категория	«Потребитель – предприятию» (C2B), также относится к B2B
Тип связи	Дистанционная
Платежное средство	Карта SEPA – любой тип (SCF)
Инициатор платежа	Предприятие торговли (услуг)
Необходимые условия	• Предприятие торговли (услуг) принимает дистанционные платежи посредством введения реквизитов платежной карты SEPA по данной карточной схеме • У потребителя есть карта, отвечающая требованиям SCF, в той же карточной схеме
Способ подтверждения платежа	Как в случае любой другой дистанционной операции по карте SEPA
Выгоды для предприятия торговли	• Доступ к более широкой клиентской базе • Предприятие торговли (услуг) в любой момент доступно для потребителя
Выгоды для потребителя	• Удобство, мобильность • Уменьшение потребности в наличных деньгах • Замещение чеков (или наличных денег)
Проблемы	• Отсутствуют особые проблемы в канале мобильной связи по сравнению с другими дистанционными платежами, совершенными с использованием платежных карт, в сети Интернет • Неудобство для потребителя в связи с необходимостью ввода своих удостоверительных данных в мобильный телефон (можно решить, например, путем использования мобильного кошелька[12]) • Поскольку это операция CNP, предприятие торговли (услуг) не уверено в достоверности платежа (эмитент вправе вернуть средства)

[12] Обратите внимание, что некоторую практическую информацию по мобильным кошелькам можно получить посредством специальных инициатив, осуществляемых в некоторых районах или регионах.

5.2.1.2. Кредитовый платеж по карте SEPA потребителя – предприятию (SCP 2): мобильный кошелек (C2B)

В сценарии, показанном на рисунке 12, потребитель использует свой мобильный телефон, чтобы произвести платеж предприятию, которое предоставляет услуги или осуществляет торговлю товарами (например, мобильным контентом). B2B реализуется, когда потребитель является предприятием. Отличие от указанного выше «основного» сценария в том, что потребитель-плательщик использует мобильный кошелек, чтобы получить доступ к своей платежной карте и ее реквизитам, совершая платеж предприятию торговли.

С точки зрения предприятия торговли этот сценарий очень похож на SCP 1.

Перед началом исполнения сценария потребитель должен активировать карту (карты) для совершения дистанционных платежей в меню конфигурации мобильного кошелька.

На рисунке 12 отражены следующие действия:

1. Зайдя в сеть Интернет с помощью своего мобильного телефона или с использованием специального приложения MRP, потребитель переходит в раздел расчетов на сайте предприятия торговли.

2. Сайт предприятия торговли выводит платежную информацию на дисплей мобильного телефона потребителя.

3. Реквизиты платежной карты потребителя передаются через мобильный кошелек и путем ввода потребителем защитного кода карты, после чего инициируется операция SCP.

4. После авторизации платежа по карте SEPA он обрабатывается.

5. Предприятие передает потребителю товары или оказывает услуги.

Рисунок 12. **Платеж по карте SEPA потребителя – предприятию: мобильный кошелек**

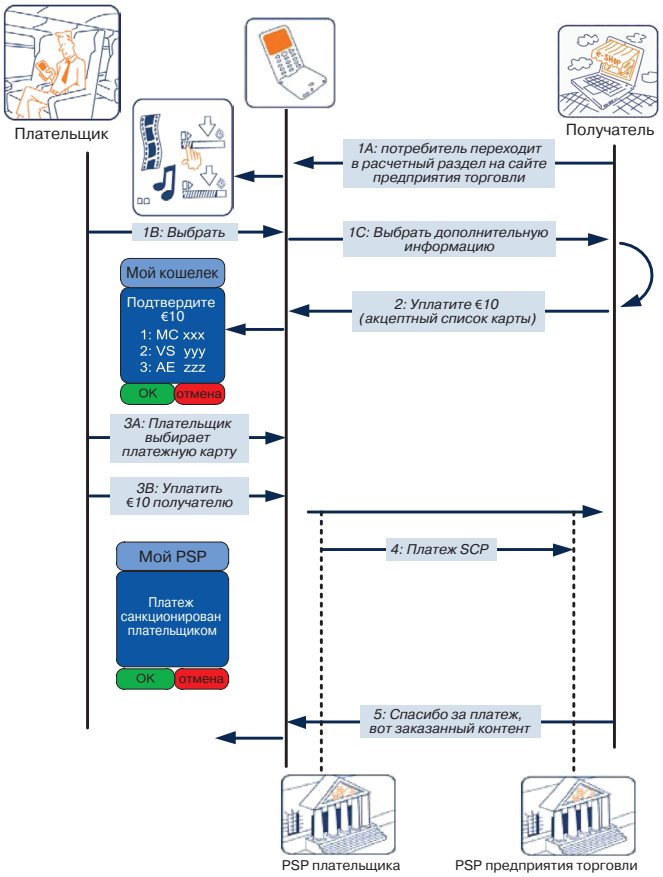


Таблица 12. **Кредитовый перевод по карте SEPA потребителя – предприятию (SCP 2): мобильный кошелек**

Кредитовый перевод по карте SEPA потребителя – предприятию (SCP 2): мобильный кошелек	
Категория	«Потребитель – предприятию» (C2B), также относится к B2B
Тип связи	Дистанционная
Платежное средство	Карта SEPA – любой тип (SCF)
Инициатор платежа	Предприятие торговли (услуг)
Необходимые условия	• Предприятие торговли (услуг) принимает дистанционные платежи, совершаемые потребителем посредством платежной карты по данной карточной схеме • У потребителя есть карта, отвечающая требованиям SCF, в той же карточной схеме
Способ подтверждения платежа	Как в случае любой другой дистанционной операции по карте SEPA
Выгоды для торгового предприятия	• Доступ к более широкой базе данных по держателям карт • Предприятие торговли (услуг) в любой момент доступно для держателей карт
Выгоды для потребителя	• Удобство, мобильность • Удобство для потребителя в выборе платежной карты с соответствующими удостоверительными данными с использованием мобильного кошелька. Снижается потребность в наличных деньгах • Замещение чеков (или наличных денег)
Проблемы	•Отсутствуют особые проблемы в мобильном канале по сравнению с другими дистанционными платежами, совершенными потребителем в сети Интернет посредством платежной карты • Аутентификация пользователя: поскольку ему не разрешается сохранять защитный код карты, потребитель должен вводить этот код, чтобы совершить операцию, что может представлять для него некоторую сложность

5.2.1.3. Кредитовый перевод по карте SEPA потребителя – предприятию (SCP 3): надежная аутентификация держателя карты (C2B)

Этот сценарий отличается от описанного выше сценария SCP 2 тем, что плательщик должен совершить дополнительные действия для аутентификации. Поскольку в дистанционных операциях по карте может использоваться карточная аутентификация, такая как CAP (Chip Authentication Program) или DPA (Dynamic Passcode Authentication), использование SE в мобильном телефоне с установленным специальным приложением аутентификации может быть очень удобным для потребителя. Это приложение аутентификации используется после ввода потребителем мобильного кода в мобильный телефон: приложение производит проверку кода. Аутентификация потребителя обеспечивает для предприятия торговли более высокую степень защиты от проведения несанкционированных операций и их отмены. Кроме того, если в мобильном телефоне уже установлено приложение MCP в SE, это может быть финансово выгодным решением.

Эмитент карты (карт) должен установить специальное приложение аутентификации в SE в мобильном телефоне потребителя. Кроме того, потребитель должен включить это приложение аутентификации, например, в меню конфигурации мобильного кошелька.

В качестве альтернативы, если плательщик имеет мобильный телефон с NFC и бесконтактную карту, включая приложение аутентификации, такое как CAP или DPA, он может осуществить аутентификацию, вставив карту в считывающее устройство с технологией NFC в мобильном телефоне. Опять же, использование этого метода аутентификации осуществляется после ввода мобильного кода потребителем в мобильном телефоне.

На рисунке 13 отражены следующие действия:

1. Зайдя в сеть Интернет с помощью своего мобильного телефона или с использованием специального приложения MRP, потребитель переходит в раздел расчетов на сайте предприятия торговли (услуг).

2. Сайт предприятия торговли (услуг) выводит платежную информацию на дисплей мобильного телефона потребителя.

3. Реквизиты платежной карты потребителя передаются через мобильный кошелек, после чего инициируется операция SCP. Приложение аутентификации в платежной карте удостоверяет потребителя.

4. После успешной аутентификации платеж разрешается.

5. После авторизации платеж SCP обрабатывается.

6. Предприятие торговли (услуг) передает потребителю товар или оказывает услугу.

Рисунок 13. **Платеж по карте SEPA потребителя – предприятию (SCP 3): надежная аутентификация держателя карты**

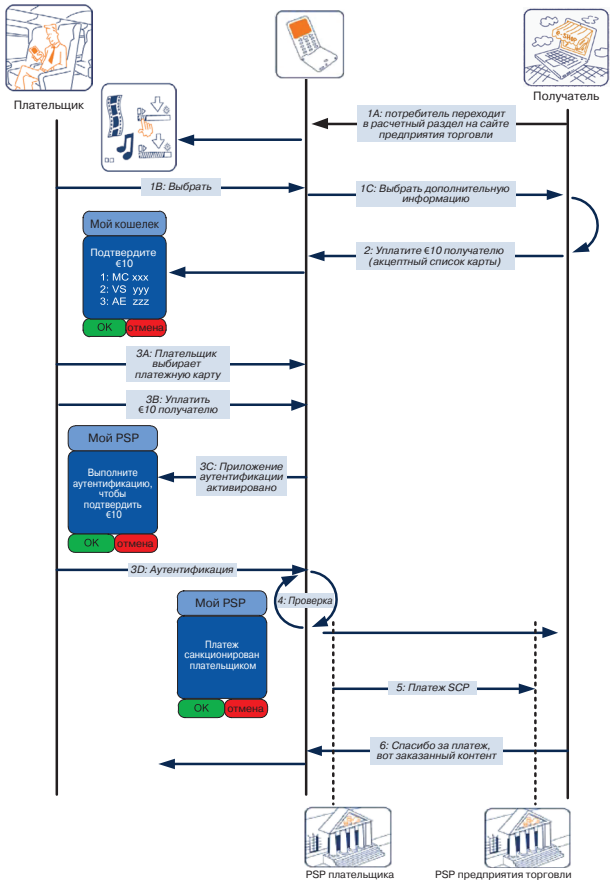


Таблица 13. **Кредитовый перевод по карте SEPA потребителя – предприятию (SCP 3): надежная аутентификация держателя карты**

Кредитовый перевод по карте SEPA потребителя – предприятию: надежная аутентификация держателя карты	
Категория	«Потребитель – предприятию» (C2B), также относится к B2B
Тип связи	Дистанционная
Платежное средство	Карта SEPA – любой тип (SCF)
Инициатор платежа	Предприятие торговли
Необходимые условия	• Предприятие торговли принимает дистанционные платежи, совершаемые потребителем посредством платежной карты по данной карточной схеме • У потребителя есть карта, отвечающая требованиям SCF, в той же карточной схеме
Способ подтверждения платежа	Как в случае любой другой дистанционной операции по карте SEPA
Выгоды для торгового предприятия	• Доступ к более широкой базе держателей карт • Предприятие торговли в любой момент доступно для держателей карт • Меньше случаев совершения несанкционированных операций с дистанционными платежами по картам
Выгоды для потребителя	• Удобство, мобильность • Удобство для клиента: более автоматизированная аутентификация • Меньше потребность в наличных деньгах • Замещение чеков (или наличных денег)
Проблемы	• Отсутствуют особые проблемы в мобильном канале связи по сравнению с другими дистанционными платежами с использованием платежной карты в сети Интернет.

5.2.1.4. Кредитовый перевод по карте SEPA потребителя – потребителю (SCP 4) (C2C)

На рисунке 14 показан возможный пример действий пользователя при совершении платежа в зоне SEPA «потребитель – потребителю», инициированного с мобильного телефона, когда потребитель (плательщик) желает произвести персональный платеж другому потребителю (получателю) с помощью своего мобильного телефона.

В данном примере главное отличие от обычного платежа в зоне SEPA в том, что операция инициирована плательщиком, а не получателем. Платеж обрабатывается в сетях карточной схемы, и сумма платежа обычным образом списывается со счета платежной карты плательщика. Получатель обычно (но не

обязательно) идентифицируется по реквизитам его платежной карты, а сумма платежа зачисляется на соответствующий платежный счет. В зависимости от правил карточной схемы существует возможность использовать псевдоним (например, номер мобильного телефона) и могут быть также альтернативные варианты идентификации получателей и зачисления им платежей (например, платежный счет). Этот сценарий может относиться и к платежам C2B, когда получателем является предприятие (которое при этом ведет себя как потребитель и подчиняется правилам карточной схемы). Плательщик и получатель могут быть клиентами разных PSPs.

Необходимое условие для этого сценария – чтобы плательщик был подписан, возможно (но не обязательно) на мобильной основе, на услуги карточной платежной системы C2C у эмитента своих карт. Многие крупные карточные схемы уже предлагают некоторые проприетарные услуги C2C, но для их широкого распространения в SEPA нужно обеспечить операционную совместимость.

На рисунке ниже отражены следующие действия:

1. Плательщик определяет сумму, которую необходимо уплатить.

2. Плательщик выбирает свое приложение MRP.

3. Плательщик вводит сумму и уникальный идентификатор получателя, подтверждает номер карты, которая будет использоваться для платежа, и разрешает операцию.

4. PSP плательщика получает идентификационные данные получателя на основе уникального идентификатора.

5. PSP плательщика отправляет платеж в PSP получателя.

6.Затем PSP получателя зачисляет платеж на основной платежный счет получателя (возможно, с уведомлением).

Можно расширить этот пример использования, рассмотрев случаи, когда требуется «срочный» или «быстрый» платеж. «Быстрый» сервис C2C SCP подойдет для сценариев, при которых:

• получатель должен использовать денежные средства незамедлительно;

• получателю требуется уверенность в получении платежа, чтобы выполнить связанную с ним операцию, например сделку купли-продажи товаров или предоставления услуг между незнакомыми лицами.

Рисунок 14. **Кредитовый перевод по карте SEPA потребителя – потребителю (SCP 4)**

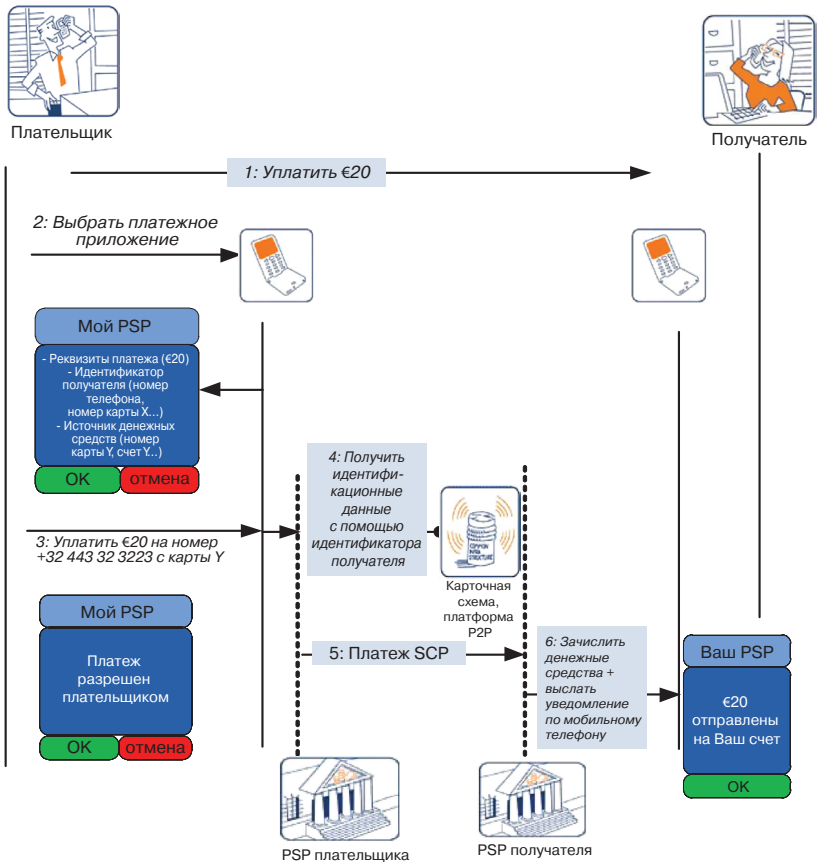


Таблица 14. **Кредитовый перевод по карте SEPA потребителя – потребителю (SCP 4)**

Кредитовый перевод по карте SEPA потребителя – потребителю	
Категория	Главным образом «потребитель – потребителю» (C2C), некоторые сценарии – «потребитель – предприятию» (например, малому) (C2B)
Тип связи	Дистанционная
Платежное средство	Карта SEPA – любой тип (SCF)
Инициатор платежа	Плательщик
Необходимые условия	• Получатель идентифицируется по уникальному идентификатору, обычно, но не обязательно – по платежной карте • Плательщик имеет карту, отвечающую требованиям SCF, и подписан на услуги мобильной карточной платежной системы C2C у своего PSP (эмитент карт)
Способ подтверждения платежа	Определяется PSP (эмитент карт)
Выгоды для потребителя	• Скорость и легкость для обоих потребителей • Плательщик имеет доступ к получателю без карты • Позволяет плательщику сохранить удостоверительные данные в тайне, а получателю не требуется раскрывать реквизиты счета
Проблемы	• Обеспечение операционной совместимости карточных схем • Управление уникальным идентификатором получателя и при необходимости его поддержка • Неудобство для держателя карты в связи с необходимостью ввода своих удостоверительных данных в мобильный телефон (можно решить, например, путем использования мобильного кошелька)

5.2.2. ДИСТАНЦИОННЫЕ КРЕДИТОВЫЕ ПЕРЕВОДЫ SEPA, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО ТЕЛЕФОНА

Следующие примеры использования основаны на SCT в качестве основного платежного средства SEPA. Обратите внимание, что в соответствии с действующими правилами SCT максимальное время обработки операции между PSPs для SCT – один рабочий день (D+1), согласно PSD.

Независимо от действий по инициированию реальная операция SCT всегда основана на использовании IBAN и BIC[13].

5.2.2.1. Кредитовый перевод SEPA потребителя потребителю (SCT 1) – C2C, SCT

На рисунке 15 показан основной пример действий пользователя по платежу SCT, инициированному с использованием мобильного телефона, когда потребитель (плательщик) производит платеж с собственного платежного счета на платежный счет другого потребителя (получателя). Плательщик и получатель могут являться и часто действительно являются клиентами разных поставщиков платежных услуг (PSP) (четырехсторонняя модель[14], см. разделы 5.4.3.2 и 5.4.3.3).

В этом сценарии не предполагается изначального доверия между плательщиком и получателем. Плательщик и получатель получают услуги одного уровня от своих PSPs, как и в случае других SCT.

Во многих обстоятельствах этот пример использования также относится к C2B, B2C и B2B (в частности, малые предприятия).

На рисунке ниже отражены следующие действия.

1. Получатель предоставляет всю необходимую информацию, включая IBAN и BIC, плательщику.

2. Плательщик предоставляет всю необходимую информацию, включая IBAN и BIC получателя, своему PSP по своему мобильному телефону. Эта информация может быть полностью введена плательщиком или может быть запрошена, если получатель заранее зарегистрирован. Обычно это делается с использованием специального приложения PSP в мобильном телефоне или через мобильный браузер.

3. Плательщик, аутентификация которого проведена его PSP, разрешает инструкцию SCT в соответствии с обычными требованиями безопасности, установленными этим PSP.

4. Затем PSP плательщика обрабатывает и передает SCT в PSP получателя, который, в свою очередь, зачисляет сумму на счет получателя.

[13] В соответствии с Положением SEPA необходимость использования BIC потребителями исчезнет самое позднее к февралю 2016 года, а в большинстве случаев – к февралю 2014 года (по внутренним операциям).
[14] Ссылка на четырехстороннюю модель не означает, что трехсторонние модели не могут быть улучшены на основе рассмотренных здесь примеров.

Рисунок 15. **Кредитовый перевод SEPA потребителя – потребителю (SCT 1)**

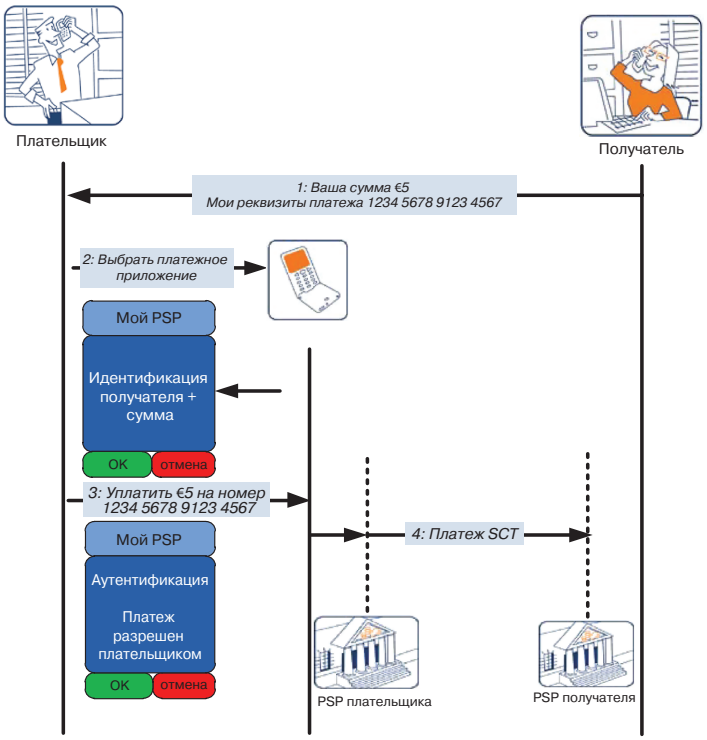


Таблица 15. **Кредитовый перевод SEPA потребителя – потребителю**

Кредитовый перевод SEPA потребителя – потребителю	
Категория	«Потребитель – потребителю» (C2C), также относится к C2B и B2B.
Тип связи	Дистанционная
Платежное средство	Кредитовый перевод SEPA
Инициатор платежа	Плательщик
Необходимые условия	Плательщик подписывается на услугу дистанционных платежей, совершаемых с использованием мобильного телефона (в зависимости от того, каким образом PSP разрешает получать инструкции от плательщика)
Способ подтверждения платежа	Определяется PSP
Выгоды для потребителя	• Мобильность для плательщика • Замещение чеков (или наличных денег)
Проблемы	• Неудобство в связи с необходимостью получения удостоверительных данных • Количество и сложность действий, требующихся для инициирования SCT • Вероятность ошибки • Получателю может быть неудобно или нецелесообразно сообщить/предоставить свой IBAN и BIC • Получатель не имеет немедленного подтверждения окончательного характера платежа • Получатель зависит от клирингового цикла SCT и услуг своего собственного PSP при выполнении платежа

5.2.2.2. Кредитовый перевод SEPA потребителя – потребителю (SCT 2): уникальный идентификатор (C2C, SCT)

На рисунке 16 показан возможный пример действий пользователя по платежу SCT, инициированному с мобильного телефона, когда потребитель (плательщик) производит платеж с собственного платежного счета на платежный счет другого потребителя (получателя). Плательщик и получатель могут являться и часто действительно являются клиентами разных PSP (четырехсторонняя модель[15], см. разделы 5.4.3.2 и 5.4.3.3).

В этом сценарии не предполагается изначального доверия между плательщиком и получателем. Имеется уникальный идентификатор получателя (например, номер его мобильного телефона), что делает ввод реквизитов получателя удобнее для плательщика.

Во многих обстоятельствах этот пример использования также относится к C2B, B2C и B2B (в частности, малые предприятия).

[15] Ссылка на четырехстороннюю модель не означает, что трехсторонние модели не могут быть улучшены на основе рассмотренных здесь примеров.

Идентификационные данные получателя должны быть зарегистрированы вместе с его уникальным идентификатором.

PSP плательщика должен допускать использование уникального идентификатора в своем процессе принятия мобильных инструкций SCT.

PSP плательщика должен быть способен определить PSP получателя и реквизиты платежного счета на основе уникального идентификатора получателя через общую инфраструктуру (см. раздел 5.4.2.3).

На рисунке 16 отражены следующие действия:

1. Получатель предоставляет плательщику свои идентификационные данные с использованием псевдонима получателя для удобства и/или безопасности.

2. Плательщик передает необходимую информацию (сумма, псевдоним получателя и т.д.) своему PSP по мобильному телефону. Обычно это делается с использованием специального приложения MRP в телефоне или через мобильный браузер.

3. Плательщик, аутентификация которого проведена его PSP, разрешает инструкцию SCT в соответствии с обычными требованиями безопасности, установленными этим PSP.

4. PSP плательщика устанавливает идентификационные данные получателя и идентифицирует PSP получателя с использованием псевдонима получателя по общей инфраструктуре.

5. Затем PSP плательщика обрабатывает и передает SCT в PSP получателя, который, в свою очередь, зачисляет сумму на счет получателя.

Рисунок 16. **Кредитовый перевод SEPA потребителя – потребителю: уникальный идентификатор**

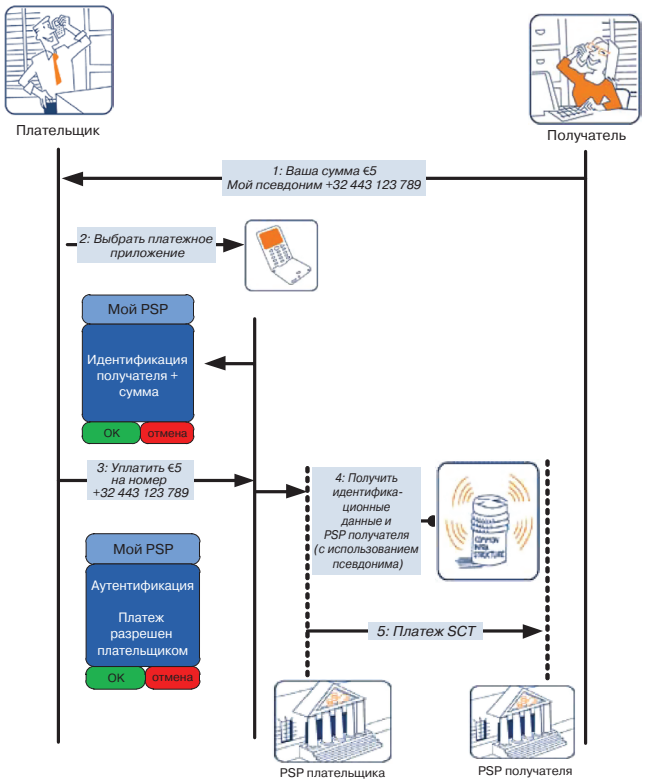


Таблица 16. **Кредитовый перевод SEPA потребителя – потребителю (SCT 2): уникальный идентификатор**

Кредитовый перевод SEPA потребителя – потребителю: уникальный идентификатор	
Категория	«Потребитель – потребителю» (C2C), также относится к C2B и B2B
Тип связи	Дистанционная
Платежное средство	Кредитовый перевод SEPA
Инициатор платежа	Плательщик
Необходимые условия	• Получатель или PSP получателя зарегистрировали свои идентификационные данные в общей инфраструктуре • PSP плательщика должен иметь доступ к общей инфраструктуре • PSP плательщика должен предлагать мобильную платежную услугу на основе использования псевдонима

Способ подтверждения платежа	Определяется PSP
Выгоды для потребителя	• Удобство, мобильность • Получателю не нужно помнить и передавать плательщику идентификационные данные (IBAN, BIC) • Замещение чеков (или наличных денег)
Проблемы	• Необходимость договоренности о формате псевдонима • Создание и эксплуатация общей инфраструктуры • Получатель не получает немедленного подтверждения окончательного характера платежа • Получатель зависит от клирингового цикла SCT и услуг своего собственного PSP при выполнении платежа.

5.2.2.3. Кредитовый перевод SEPA потребителя – предприятию (SCT 3A): подтверждение (C2B, C2C, B2B SCT)

На рисунке 17 показан возможный пример действий пользователя по платежу SCT, инициированному с мобильного телефона, когда потребитель (плательщик) производит платеж с собственного платежного счета на платежный счет получателя. Плательщик и получатель могут являться и часто действительно являются клиентами разных PSPs (четырехсторонняя модель[16], см. разделы 5.4.3.2 и 5.4.3.3).

В этом примере использования «подтверждение платежа», направляемое получателю, важно для того, чтобы SCT был приемлемой формой платежа (например, предприятию торговли требуется достаточная уверенность в проведении платежа перед передачей товаров или оказанием услуг). Обычно, но не всегда здесь реализуется сценарий «потребитель – предприятию» (предприятию торговли) C2B. Однако можно предусмотреть ситуации C2C (например, продажа автомобиля или иных ценных предметов) и B2B (например, сделки между коммерсантами).

Идеальным вариантом, хотя и не обязательным, стало бы использование универсального идентификатора согласно определению в предыдущем сценарии. Этот пример использования также относится к C2C, B2C и B2B (малые предприятия) с учетом регистрации в общей, совместно используемой службе «подтверждения платежа».

На рисунке 17 отражены следующие действия:

1. Плательщик и получатель договариваются о сумме, которая должна быть уплачена, и получатель передает плательщику свои идентификационные данные, при этом возможно использование уникального идентификатора для удобства и/или безопасности.

2. Плательщик передает необходимую информацию (сумма, псевдоним получателя и т.д.) своему PSP по своему мобильному телефону. Обычно это делается с использованием специального приложения MRP в телефоне или через мобильный браузер.

3. Плательщик, аутентификацию которого проводит его PSP, разрешает инструкцию SCT в соответствии с обычными требованиями безопасности, установленными этим PSP.

4. PSP плательщика устанавливает идентификационные данные получателя и идентифицирует PSP получателя (например, с использованием псевдонима получателя) по общей инфраструктуре.

5. PSP плательщика сообщает в службу «подтверждения платежа» о платеже SCT, в том числе идентификационные данные получателя и соответствующего PSP.

6. В качестве участника службы «подтверждения платежа» PSP получателя получает подтверждение, что SCT в безотзывном порядке произведен PSP плательщика.

7. PSP получателя передает ему подтверждение.

8. Затем PSP плательщика обрабатывает и передает SCT в PSP получателя, который, в свою очередь, зачисляет сумму на счет получателя.

[16] Ссылка на четырехстороннюю модель не означает, что трехсторонние модели не могут быть улучшены на основе рассмотренных здесь примеров.

Рисунок 17. **Кредитовый перевод SEPA потребителя – предприятию (SCT 3A): подтверждение**

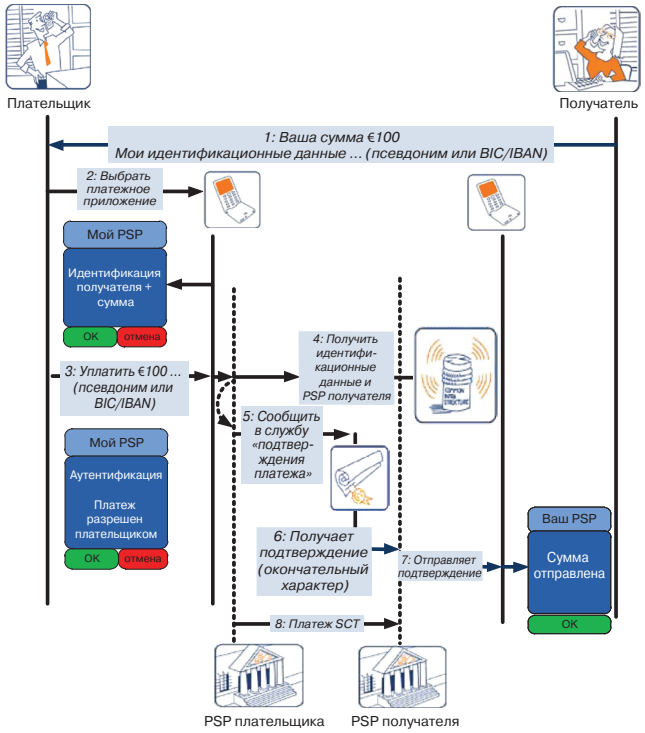


Таблица 17. **Кредитовый перевод SEPA потребителя – предприятию (SCT 3A): подтверждение**

Кредитовый перевод SEPA потребителя – предприятию: подтверждение	
Категория	«Потребитель – предприятию» (C2B), также относится к B2B.
Тип связи	Дистанционная
Платежное средство	Кредитовый перевод SEPA
Инициатор платежа	Плательщик
Необходимые условия	• Создание службы «подтверждения платежа» • PSP плательщика и PSP получателя должны участвовать в службе «подтверждения платежа» • Получатель должен быть зарегистрирован в службе уведомлений[17] своего PSP • Плательщик должен иметь возможность направить своему PSP инструкции относительно обращения в службу «подтверждения платежа».
Способ подтверждения платежа	Определяется PSP
Выгоды для потребителя	• Удобство, мобильность, оперативность • Замещение чеков (или наличных денег) • Получателю приходит немедленное подтверждение окончательного характера платежа; это позволяет получателю передать товары или оказать услуги. Хотя служба «подтверждения платежа» направляет подтверждение немедленно, платеж не является (не обязательно является) таковым
Проблемы	• Создание и эксплуатация службы «подтверждения платежа»

5.2.2.4. Кредитовый перевод SEPA потребителя – предприятию (SCT 3B): подтверждение через службу электронных платежей (C2B, SCT)

В этом сценарии как PSP плательщика, так и PSP получателя относятся к одной и той же службе электронных платежей на основе SCT, которая включает службу «подтверждения платежа». Кроме того, получатель является предприятием торговли (услуг), зарегистрированным в службе электронных платежей. Платеж проводится таким же образом, как и операция SCT, инициированная с компьютера или планшетного компьютера, но в данном случае он инициируется с мобильного телефона.

Хотя этот сценарий требует предварительной регистрации получателя (предприятия торговли (услуг)) в службе электронных платежей, его преимущество в безопасности для получателя и удобстве для плательщика, которые обеспечиваются в рамках одной и той же службы электронных платежей.

Так как реквизиты PSP (или платежного счета) получателя уже зарегистрированы в службе электронных платежей, нет необходимости использовать уникальный идентификатор. Кроме того, поскольку эта

[17] Должна работать служба передачи уведомлений между получателем (торговым предприятием) и его PSP для подтверждения последним проведения платежа до передачи товаров или услуг плательщику.

служба передает подтверждение платежа зарегистрированным в ней предприятиям торговли, организовывать отдельный процесс «подтверждения платежа» для получателей не требуется.

Совершая покупку через мобильный браузер или приложение MRP, плательщик (потребитель) просто выбирает опцию «служба электронных платежей» и свой PSP из списка участвующих PSP. Затем он получает платежные «инструкции» с указанием получателя и суммы, которые плательщик затем подтверждает в соответствии с обычными требованиями его PSP. В этом примере использования обе стороны получают подтверждение того, что платежная операция выполнена.

На рисунке 18 показаны следующие действия:

1. Плательщик, делая покупку посредством мобильного устройства (мобильный браузер или приложение), выбирает на кассе опцию «электронный платеж».

2. Плательщику передается список участвующих PSP.

3. Он выбирает своего PSP из списка.

4. В PSP плательщика через службу электронных платежей передаются реквизиты платежа. Плательщик получает платежные инструкции от своего PSP с указанием (как минимум) получателя и суммы платежа.

5. Плательщик, аутентификацию которого проводит его PSP, разрешает инструкцию SCT в соответствии с обычными требованиями безопасности, установленными этим PSP.

6. PSP плательщика сообщает в службу электронных платежей о платеже SCT, в том числе идентификационные данные получателя и соответствующего PSP. В качестве участника службы электронных платежей PSP получателя получает подтверждение, что SCT будет в безотзывном порядке произведен PSP плательщика.

7. PSP получателя передает ему подтверждение.

8. Затем PSP плательщика обрабатывает и передает SCT в PSP получателя, который, в свою очередь, зачисляет сумму на счет получателя.

Рисунок 18. **Кредитовый перевод SEPA потребителя – предприятию (SCT 3B): подтверждение через службу электронных платежей**

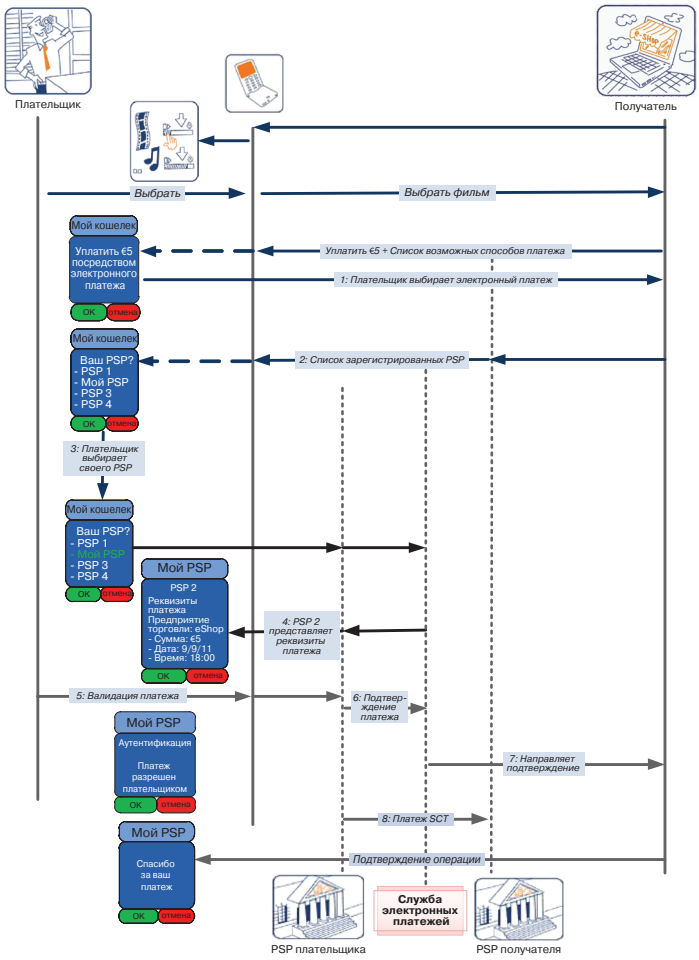


Таблица 18. **Кредитовый перевод SEPA потребителя – предприятию (SCT 3B): подтверждение через службу электронных платежей**

Кредитовый перевод SEPA потребителя – предприятию: подтверждение через службу электронных платежей	
Категория	«Потребитель – предприятию» (C2B)
Тип связи	Дистанционная
Платежное средство	Кредитовый перевод SEPA
Инициатор платежа	Получатель (через службу электронных платежей)
Необходимые условия	• Наличие службы электронных платежей • PSP плательщика и PSP получателя должны быть зарегистрированы в одной и той же службе электронных платежей • Получатель (предприятие торговли) должен быть зарегистрирован в службе электронных платежей
Способ подтверждения платежа	Определяется службой электронных платежей
Выгоды для потребителя	• Удобство для плательщика • Безопасность для получателя (предприятия торговли) • Не требуется обмен удостоверительными данными между плательщиком и получателем • Служба электронных платежей обеспечивает надежность и доверие
Проблемы	• Договоренность о подтверждении платежа со службой электронных платежей (не только для мобильной связи)

Примечание. В случае если PSPs зарегистрированы в разных службах электронных платежей, должна существовать структура, обеспечивающая операционную совместимость (см. также 5.4.3.3), которой отвечают обе службы электронных платежей. Кроме того, в данном случае эта структура также обеспечивает работу службы «подтверждения платежа».

5.2.2.5. Срочный кредитовый перевод SEPA потребителя – потребителю (C2C, uSCT)

На рисунке 19 показан возможный пример действий пользователя по срочному платежу SCT, инициированному с использованием мобильного телефона, когда потребитель (плательщик) совершает быстрый платеж со своего собственного платежного счета на платежный счет другого потребителя (получателя). Плательщик и получатель платежа могут являться и часто действительно являются клиентами разных PSPs. Этот сценарий может также относиться к операциям «потребитель – предприятию», поскольку «мгновенный» характер перевода позволяет получателю подтвердить получение денежных средств у своего PSP до передачи товаров или услуг.

Схема SCT SEPA в настоящее время не предлагает быстрого перевода платежей. Однако это не препятствует тому, чтобы в будущем «быструю» или «мгновенную» услугу предложили бы все или некоторые участники SCT.

По мере того, как все больше новых участников рынка предлагают более широкий выбор пользователям платежных услуг, весьма вероятен рост спроса на «мгновенное» выполнение всех операций, в том числе платежных. Ожидается, что PSPs должны будут разработать подобные решения, чтобы оставаться конкурентоспособными, в частности в области мобильных услуг.

Для целей данного сценария эта концепция именуется срочным кредитовым переводом SEPA (uSCT).

Во многих ситуациях этот пример использования также относится к C2B, B2C и B2B (в частности, для малых предприятий).

На рисунке ниже показаны следующие действия:

1. Получатель передает свои данные плательщику с использованием уникального идентификатора получателя для удобства и/или безопасности.

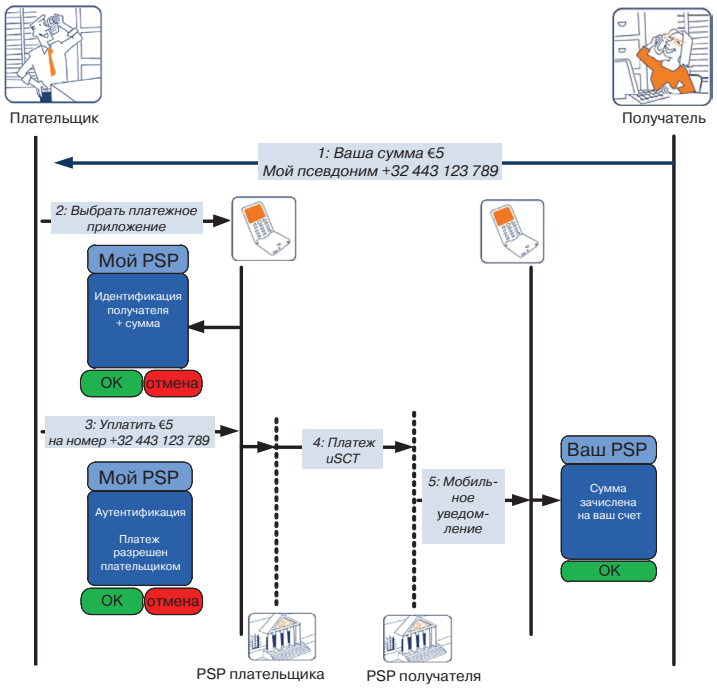
2. Плательщик передает необходимую информацию (сумма, уникальный идентификатор получателя и т.д.) своему PSP по мобильному телефону. Обычно это делается с использованием специального приложения MRP в телефоне или через мобильный браузер.

3. Плательщик, аутентификацию которого проводит его PSP, разрешает инструкцию SCT в соответствии с обычными требованиями безопасности, установленными этим PSP.

4. Затем PSP плательщика обрабатывает и передает uSCT в PSP получателя, который, в свою очередь, зачисляет сумму на счет получателя.

5. Получатель имеет возможность получить от своего PSP (почти мгновенно) подтверждение того, что платеж получен (например, мобильное уведомление), и получить доступ к денежным средствам.

Рисунок 19. **Срочный кредитовый перевод SEPA потребителя – потребителю**



Примечание. На этом рисунке не представлен механизм получения идентификационных данных получателя и его PSP по номеру мобильного телефона.

Таблица 19. **Срочный кредитовый перевод SEPA потребителя – потребителю**

Срочный кредитовый перевод SEPA потребителя – потребителю	
Категория	«Потребитель – потребителю» (C2C), также относится к B2B, C2B и B2C
Тип связи:	Дистанционная
Платежное средство	Кредитовый перевод SEPA
Инициатор платежа	Плательщик
Необходимые условия	Создание uSCT SEPA
Способ подтверждения платежа	Определяется PSP
Выгоды для потребителя	• Удобство, мобильность, оперативность • Замещение чеков (или наличных денег) • Получатель немедленно получает платеж
Проблемы	• Создание и эксплуатация uSCT

Этот пример использования фактически совпадает с примером использования SCT 2, когда платеж совершается незамедлительно с использованием срочного кредитового перевода SEPA (uSCT).

5.3. ЭКОСИСТЕМА

5.3.1. ВВЕДЕНИЕ

Одна из целей EPC – развитие платежных средств SEPA, поэтому в настоящей «Белой книге» рассмотрены только экосистемы, отвечающие требованиям SEPA[18]. Это касается как четырехсторонних, так и трехсторонних моделей (см. раздел 5.4.3), при условии, что в последних используются форматы, отвечающие требованиям SEPA. Это также означает, что для MRPs должны использоваться платежные счета.

Желательно использовать существующие инфраструктуру и бизнес-процессы платежных средств SEPA в максимально возможной степени. Это означает, что внимание должно быть сосредоточено на том, каким образом использовать мобильный телефон, чтобы инициировать операции SEPA и вписать их в существующие платежные инфраструктуры, позволив им затем обрабатывать платежи в соответствии с существующими платежными схемами SEPA.

5.3.2. ЗАИНТЕРЕСОВАННЫЕ СТОРОНЫ

• Плательщик, имея платежный счет SEPA или карту, отвечающую требованиям SEPA, и мобильный телефон, должен иметь действующую подписку на услуги MNO. Хотя в настоящей «Белой книге» рассма-

[18] Обратите внимание, что примеры использования и модели обслуживания, представленные здесь, могут также действовать за пределами зоны SEPA.

триваются платежи, инициируемые с помощью мобильного телефона, выводы могут также относиться к другим мобильным устройствам.

• Получатель имеет платежный счет SEPA и, в соответствующих случаях, карту, отвечающую требованиям SEPA. Если получатель является частным потребителем / малым предприятием, возможны ситуации, когда получателю удобнее воспользоваться мобильным телефоном для получения дополнительных услуг, таких как уведомление о проведенном платеже.

• PSP предлагает платежные услуги SEPA, отвечающие нормативно-правовым требованиям / требованиям безопасности.

• MNO отвечает за надежную маршрутизацию сообщений, эксплуатацию сети мобильной связи, присвоение и повторное использование номеров мобильных телефонов, что является важным фактором, когда номера используются в качестве псевдонимов.

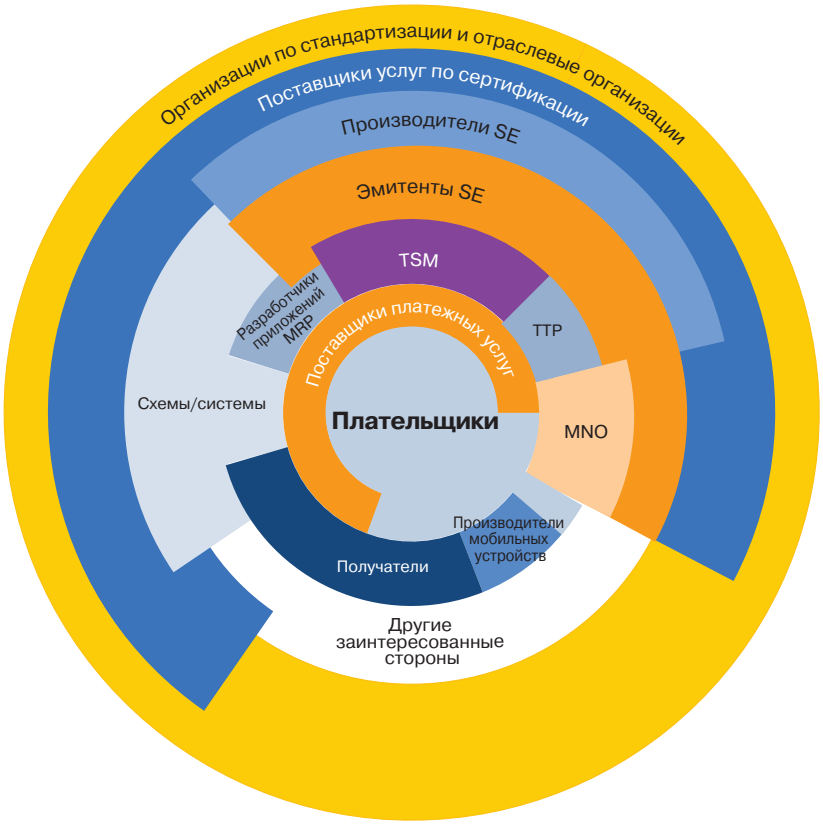
• Функции платежной системы обеспечиваются отвечающей требованиям SEPA платежной схемой и механизмом клиринга и расчетов (CSM).

• В случае если для MRP используется специальное приложение MRP в мобильном телефоне, эмитентом MRP является PSP, отвечающий за предоставление этого приложения плательщику. Обычно это приложение находится в SE в мобильном телефоне.

• Возможно участие доверенной третьей стороны (TTP), управляющей общей инфраструктурой, что повысит удобство и/или степень доверия для участвующих сторон.

• Доверенный сервис-менеджер (TSM) является TTP, действующей от имени эмитентов SE и/или эмитентов приложения MRP для формирования открытой экосистемы в случае, если SE используется для размещения приложения (приложений) MRP. Могут существовать одновременно несколько TSMs, которые предлагают взаимно конкурирующие услуги.

Рисунок 20. **Бизнес-экосистема MRP**



5.3.3. МОДЕЛИ ОБСЛУЖИВАНИЯ

5.3.3.1. Платежная операция

Дистанционные платежи по картам SEPA C2B не влияют на платежные операции по картам SEPA, на которых они основаны. Следовательно, для этих мобильных дистанционных платежей, совершаемых путем введения реквизитов платежной карты SEPA, модели обслуживания не меняются по сравнению с моделями платежных операций по картам SEPA.

Для дистанционных платежей по картам SEPA C2C требуется новая TTP, управляющая общей платформой карточной схемы P2P для получения идентификационных данных получателя (см. раздел 5.2.1.4). TTP не влияет на платежные операции по картам SEPA, на которых основываются дистанционные платежи, но может повлиять на модель обслуживания.

Основные мобильные дистанционные платежи SCT C2C, представленные в подразделе 5.2.2.1, не влияют на платежные операции SCT, на которых они основываются; следовательно, существующая модель обслуживания продолжает действовать.

Другие примеры использования, представленные в подразделах 5.2.2.2, 5.2.2.3 и 5.2.2.4, не меняют платежных операций SCT. Однако дополнительные особенности в этих примерах использования могут повлиять на существующие модели обслуживания SCT в связи с появлением новых TTP.

Заключительный пример использования C2C, представленный в подразделе 5.2.2.5, требует изменений в механизме проведения платежа SCT, на котором он основывается, в связи с незамедлительностью. Однако модель обслуживания SCT должна остаться неизменной.

5.3.3.2. Обеспечение и управление

В зависимости от конкретного MRP платежная информация, хранящаяся в мобильном телефоне, может изменяться: от одних лишь платежных реквизитов до специального приложения MRP в SE. Очевидно, обеспечение и управление по этой платежной информации будут соответствующим образом отличаться. Некоторая дополнительная информация приведена в разделе 7.3.

5.4. АРХИТЕКТУРА ВЫСОКОГО УРОВНЯ

5.4.1. ВВЕДЕНИЕ

Для дистанционных платежей архитектура высокого уровня может не зависеть от того, является ли платежное средство, на котором они основаны, картами в зоне SEPA или SCT.

Рисунок 21. **Архитектура высокого уровня для дистанционных платежей, совершаемых с использованием мобильного телефона**

На рисунке 21 можно выделить три уровня:

• Уровень 1. Возможности подключения и пользовательский интерфейс, используемые для инициирования платежа

Для инициирования дистанционного платежа посредством мобильного телефона могут использоваться различные способы, такие как мобильный браузер, SMS или специальное приложение MRP. Следовательно, возможности подключения и пользовательский интерфейс важны для обеспечения удобства действий пользователя на этом этапе, но они также относятся к конкурентному пространству.

Кроме того, важны дальнейшие сообщения между различными сторонами дистанционной платежной операции. Например, плательщику нужно знать, когда платеж был разрешен, утвержден или совершен, тогда как получателю может быть необходимо узнать о состоянии платежа, чтобы принять решение о передаче товаров (услуг) или даже подтвердить получение для завершения операции.

• Уровень 2. Общая инфраструктура, используемая для ускорения платежей

Компонент ускорения платежей помогает определить платежные средства, используемые двумя сторонами дистанционной платежной операции. Существуют различные модели. Обе стороны могут добровольно раскрыть друг другу реквизиты платежного средства (например, IBAN и BIC); они могут полагать-

ся на некоторую форму связи (через общую инфраструктуру) между мобильными идентификаторами и платежными средствами, принадлежащими различным сторонам операции.

• Уровень 3. Платежное средство для денежных переводов и движения денежных средств

Фактические денежные переводы и движение денежных средств осуществляются с использованием существующих платежных средств SEPA.

5.4.2. ВОЗВРАЩЕНИЕ НА УРОВЕНЬ 2

5.4.2.1. Введение

Главное назначение общей инфраструктуры – связать идентификатор / уникальный идентификатор с соответствующими платежными реквизитами получателя, чтобы обеспечить соответствующую маршрутизацию платежной операции (например, с платежным счетом получателя через IBAN/BIC по операции на основе SCT). В дальнейшем это может использоваться в качестве платформы для дополнительных услуг.

В зависимости от использования общей инфраструктуры (уровень 2) можно рассмотреть две основные модели для дистанционных платежей в зоне SEPA посредством мобильного телефона:

• первая модель основана на использовании существующей инфраструктуры и обеспечивает прямую операционную совместимость между плательщиками и получателями;

• вторая модель основана на создании новой централизованной общей инфраструктуры (в дополнение к существующей платежной инфраструктуре). Обратите внимание, что последняя модель может существовать в нескольких разновидностях.

Обе модели предусматривают предложение дополнительных услуг, поскольку потребители, использующие платежи, совершенные с использованием мобильного телефона, ожидают оперативности и надежности обслуживания. Особенно важным считается процесс уведомления, поскольку, например, предприятиям торговли (услуг) требуется подтверждение платежа до передачи приобретенных товаров (услуг).

5.4.2.2. Модель прямой операционной совместимости

Модель прямой операционной совместимости зависит от способности плательщиков/получателей передать все соответствующие платежные реквизиты (BIC, IBAN, наименование, адрес и т.д.) своему PSP или контрагенту. Единственное отличие между этим видом мобильных дистанционных платежей в зоне SEPA и традиционными платежами SEPA состоит в том, что платеж инициируется с помощью мобильного телефона вместо, например, ПК или бумажного документа.

Рисунок 22. **Модель прямой операционной совместимости**

Преимущества модели прямой операционной совместимости заключаются в низкой стоимости ее реализации и эксплуатации, поскольку все операции производятся с использованием уже существующих каналов, а главный ее недостаток – неудобство для потребителей. Существует возможность расширить эту модель обслуживания за счет дополнительных услуг, например услуг по уведомлению клиентов.

5.4.2.3. Модель операционной совместимости на основе централизованной общей инфраструктуры

В этой модели операционная совместимость достигается за счет использования централизованной общей инфраструктуры[19], которая может иметь различные формы и цели и может быть реализована на основе распределения. Главное назначение этой инфраструктуры – действовать в качестве службы каталога или коммутационного механизма для маршрутизации. Очевидно, централизованная общая инфраструктура может также предлагать различные дополнительные услуги, такие, как услуги по уведомлению и передаче данных, которые, однако, выходят за рамки настоящей «Белой книги».

Рисунок 23. **Модель централизованной общей инфраструктуры**

5.4.3. ВОЗВРАЩЕНИЕ НА УРОВЕНЬ 3

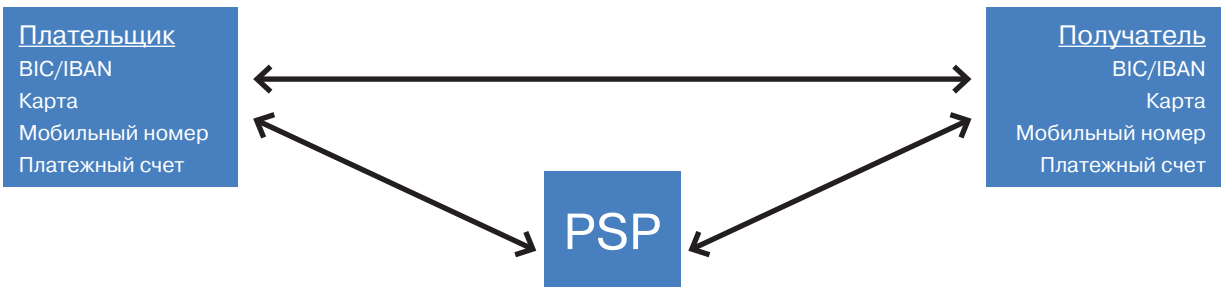
На основе этой архитектуры можно построить ряд различных моделей обслуживания в зависимости от того, относятся ли плательщик и получатель к одному и тому же PSP, и в зависимости от того, действуют ли соответствующие PSP в рамках одной или разных платежных схем. В следующих разделах рассматриваются следующие модели:

- трехсторонняя модель с участием одного-единственного PSP;
- четырехсторонняя модель с участием разных PSP в рамках одной платежной схемы;
- четырехсторонняя модель с участием разных PSP в рамках разных платежных схем.

5.4.3.1. Трехсторонняя модель

В этой модели как плательщик, так и получатель являются клиентами одного PSP, действующего в рамках данной платежной схемы. Тот факт, что участвует только один PSP, позволяет упростить реализацию примеров использования, описанных в разделе 5.2, в отношении идентификации получателя (который известен PSP), подтверждения платежа и аспекта незамедлительности.

Рисунок 24. **Трехсторонняя модель**

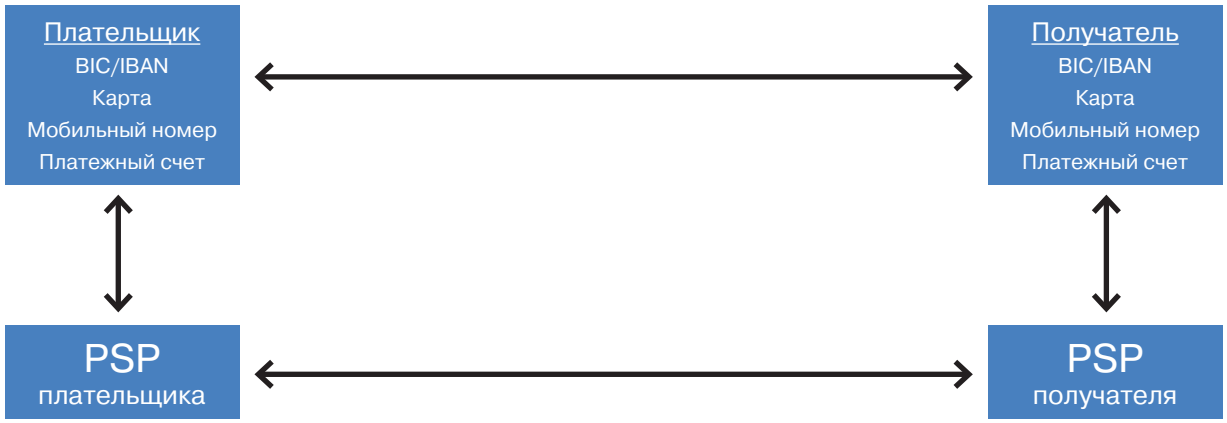


[19] Обратите внимание, что общая инфраструктура может быть проприетарной (например, может управляться карточными схемами).

5.4.3.2. Четырехсторонняя модель в рамках одной платежной схемы

В этой модели плательщик и получатель являются клиентами разных PSP, но предполагается, что оба PSP действуют в рамках одной и той же платежной схемы (карточная схема или служба электронных платежей). Эта модель также позволяет упростить некоторые аспекты, описанные в примерах использования в разделе 5.2, такие как идентификация получателя по псевдониму, подтверждение платежа и его незамедлительность.

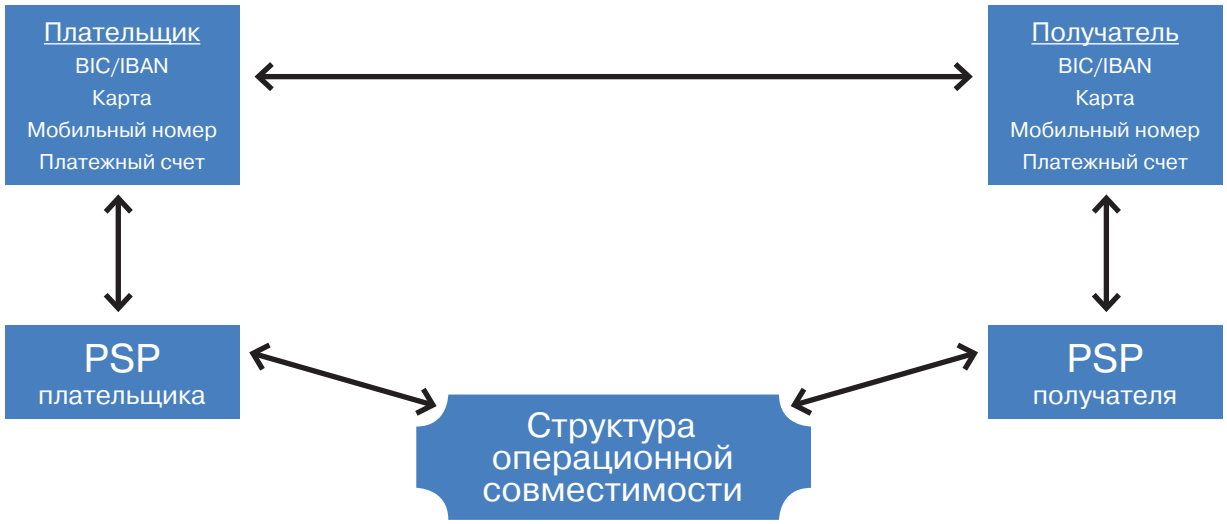
Рисунок 25. **Четырехсторонняя модель в рамках одной платежной схемы**



5.4.3.3. Четырехсторонняя модель в рамках различных платежных схем

В этой модели плательщик и получатель являются клиентами разных PSPs, которые действуют по разным платежным схемам. Очевидно, обе схемы должны иметь некоторую операционную совместимость (т.е. должно существовать соглашение между этими платежными схемами). Это наиболее общая модель, которая может существовать.

Рисунок 26. **Четырехсторонняя модель в рамках различных платежных схем**



6. БЕЗОПАСНАЯ ПОДПИСКА НА ПЛАТЕЖИ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО ТЕЛЕФОНА

Примеры использования, описывающие безопасную подписку на услуги проведения платежей, совершаемых с использованием мобильного телефона, которые приведены в настоящем разделе, основаны не на платежных средствах SEPA и не стандартизируются EPC. Они представлены здесь только для того, чтобы продемонстрировать, каким образом можно легко и удобно организовать подписку на данный вид услуг, и являются исключительно иллюстративными.

Мобильное подключение обеспечивает возможность почти немедленного предоставления новой мобильной платежной услуги. Однако эта незамедлительность сильно зависит от времени, необходимого для проверки и первичной обработки данных.

Регистрация и обеспечение приложения для платежей посредством мобильного телефона должны осуществляться в защищенной среде. Доступ клиентов к этому приложению будет облегчен, если они смогут воспользоваться существующими проверенными связями между ними и их PSP.

См. [3], где даны конкретные рекомендации по реализации услуг по регистрации клиентов с выполнением требований PSD [19].

6.1. ДИСТАНЦИОННАЯ ПОДПИСКА

В этом сценарии, показанном на рисунке 27, клиент PSP (потребитель) подписывается на услуги, позволяющие оплачивать товары (услуги) посредством мобильного телефона через существующую платежную услугу с использованием сети Интернет. При этом потребитель уже аутентифицирован и работает в защищенной среде.

В этом сценарии сделаны следующие исходные предположения:

• действующий договор между потребителем и PSP допускает дистанционную подписку (например, через систему электронных банковских услуг) на новые дополнительные услуги;

• у мобильного телефона есть необходимые технические возможности для использования желаемого вида услуг по проведению платежей посредством мобильного телефона.

Этот сценарий может выполняться следующим образом:

1. Сначала потребитель выполняет аутентификацию в PSP в рамках обычного открытия дистанционного сеанса работы.

2. Затем потребитель инициирует подписку на мобильные услуги, введя свой номер мобильного телефона и обозначив конкретную услугу, которую он намерен использовать.

3. После этого PSP проверяет технические возможности мобильного телефона (включая UICC или другой SE), напрямую или с использованием услуг, предоставляемых TSM.

4. Затем потребитель получает SMS об этом от PSP на свой мобильный телефон.

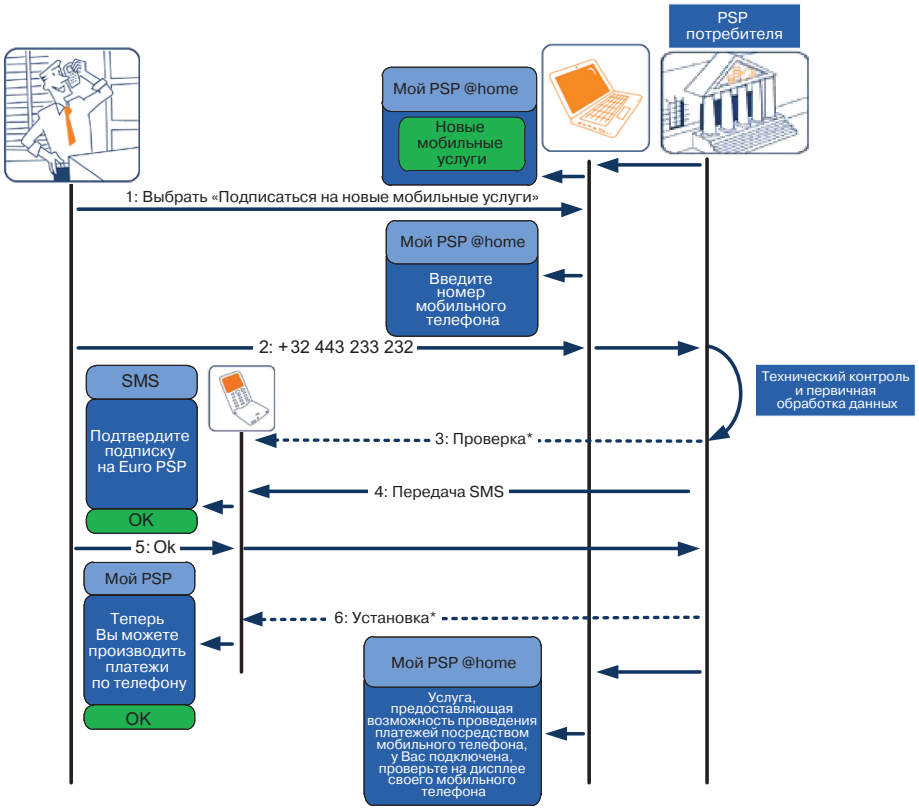
5. Он открывает SMS и подтверждает, что намерен подключить данную услугу, с мобильного телефона, на который поступило сообщение.

6. После того как потребитель отправил свое подтверждение, услуга подключается, и на дисплее мобильного телефона он видит подтверждение подключения.

Подключение услуги может быть связано с дополнительными особенностями, такими как несколько приложений, которые могут быть скачаны и установлены в SE (например, платежное приложение) и в самом мобильном телефоне (например, интерфейс конечного пользователя).

Дополнительные рекомендации будут представлены в готовящихся EPC методических рекомендациях по внедрению платежей с использованием мобильного телефона.

Рисунок 27. **Пример дистанционной подписки на платежи, совершаемые с использованием мобильного телефона**



Примечание. Операции, помеченные звездочкой, могут потребовать дополнительных действий потребителя.

6.2. ПОДПИСКА ЧЕРЕЗ УСТРОЙСТВО САМООБСЛУЖИВАНИЯ

В этом сценарии, представленном на рисунке 28, клиент PSP (потребитель) подписывается на услуги мобильных платежей через устройство самообслуживания (например, банкомат). При этом потребитель уже аутентифицирован и работает в защищенной среде.

В этом сценарии сделаны следующие исходные предположения:

• действующий договор между потребителем и PSP допускает подписку на новые дополнительные платежные услуги через устройство самообслуживания;

• у мобильного телефона есть необходимые технические возможности для использования желаемого вида услуг по проведению платежей посредством мобильного телефона.

Этот сценарий выполняется следующим образом:

1. Сначала потребитель выполняет аутентификацию в банкомате в рамках обычного открытия сеанса работы.

2. Затем потребитель инициирует подписку, введя свой номер мобильного телефона и обозначив услугу, которую он намерен использовать.

3. После этого PSP проверяет технические возможности мобильного телефона (включая UICC или другой SE), напрямую или с использованием услуг, предоставляемых TSM.

4. Затем потребитель получает SMS об этом от PSP на свой мобильный телефон.

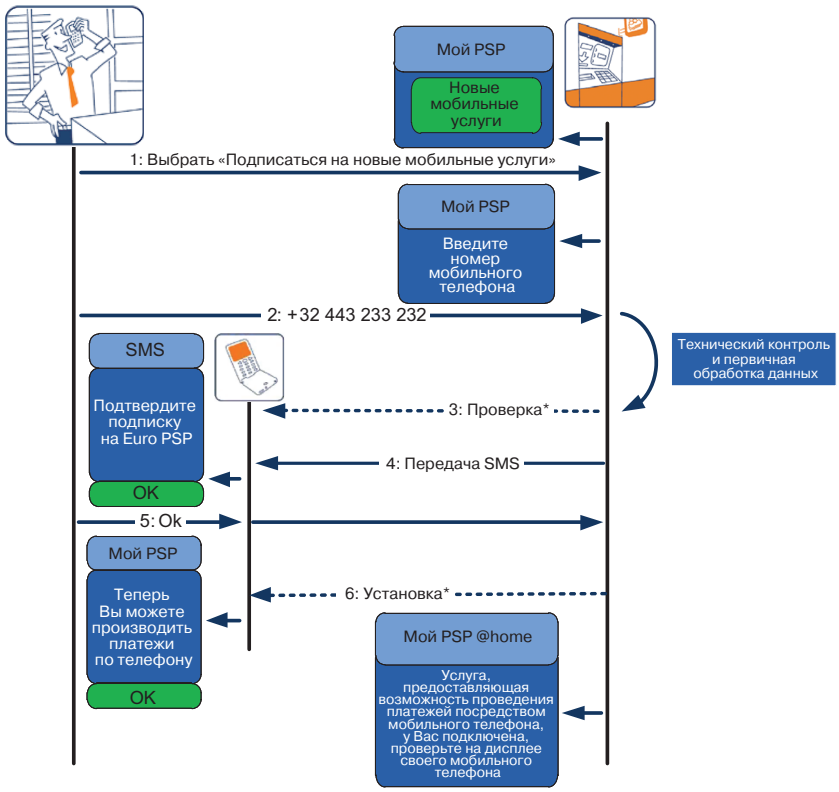
5. Он открывает SMS и подтверждает, что намерен подключить услугу, с мобильного телефона, на который поступило сообщение.

6. После того как потребитель отправил свое подтверждение, услуга подключается, и на дисплее мобильного телефона потребитель видит подтверждение подключения.

Подключение услуги может быть связано с дополнительными особенностями, такими как несколько приложений, которые могут быть скачаны и установлены в SE (например, платежное приложение) и в самом мобильном телефоне (например, интерфейс конечного пользователя).

Дополнительные рекомендации будут представлены в готовящихся EPC методических рекомендациях по внедрению платежей с использованием мобильного телефона.

Рисунок 28. **Пример подписки через банкомат на платежи, совершаемые с≈использованием мобильного телефона**



Примечание. Операции, помеченные звездочкой, могут потребовать дополнительных действий потребителя.

6.3. ПОДПИСКА В ФИЛИАЛЕ PSP

В этом сценарии, представленном на рисунке 29, подписка на услуги мобильных платежей оформляется, когда потребитель приходит в свой филиал PSP.

В этом сценарии сделано исходное предположение о том, что у мобильного телефона есть необходимые технические возможности для использования желаемого вида услуг по проведению платежей посредством мобильного телефона.

Этот сценарий выполняется следующим образом:

1. Потребитель сообщает сотруднику филиала о своем намерении подписаться на услугу по проведению платежей посредством мобильного телефона.

2. Затем потребитель сообщает номер мобильного телефона, который фиксируется в числе прочей регистрационной информации.

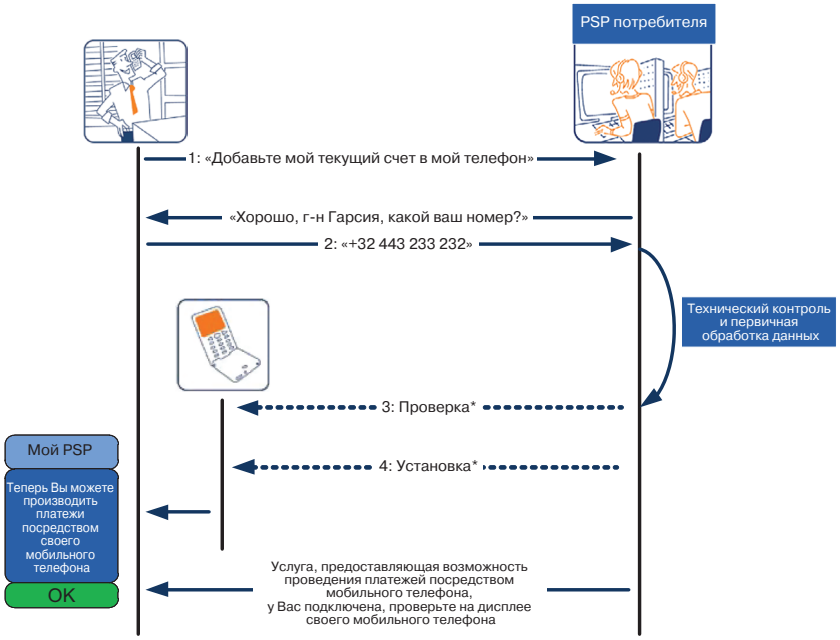
3. После этого PSP проверяет технические возможности мобильного телефона (включая UICC или другой SE), напрямую или с использованием услуг, предоставляемых TSM.

4. Новая функциональная возможность включается в мобильном телефоне дистанционно, и потребитель видит, что в его мобильном телефоне установлено новое платежное приложение.

Подключение услуги может быть связано с дополнительными особенностями, такими как несколько приложений, которые могут быть скачаны и установлены в SE (например, платежное приложение) и в самом мобильном телефоне (например, интерфейс конечного пользователя).

Дополнительные рекомендации будут представлены в готовящихся EPC методических рекомендациях по внедрению платежей с использованием мобильного телефона.

Рисунок 29. **Пример подписки на персональные платежи, совершаемые с использованием мобильного телефона**



Примечание. Операции, помеченные звездочкой, могут потребовать дополнительных действий потребителя.

7. ИНФРАСТРУКТУРА

7.1. ОБЩИЕ ПОЛОЖЕНИЯ

В настоящем разделе рассматриваются различные инфраструктурные компоненты, которые используются для MCP и MRP.

7.1.1. МОБИЛЬНЫЕ ТЕЛЕФОНЫ

В SEPA все используемые мобильные телефоны общего назначения работают в стандарте GSM или UMTS (также именуется 3G). Все мобильные телефоны UMTS обеспечивают мобильный широкополосный доступ, и практически все новые мобильные телефоны GSM, поступающие в продажу, также поддерживают GPRS или EDGE, которые также обеспечивают уверенный доступ в сеть Интернет, хотя и с невысокой скоростью передачи данных. Они поддерживают UICC (вместо SIM): устойчивое к постороннему вмешательству устройство идентификации, принадлежащее MNO, предоставляемое MNO и полностью стандартизированное ETSI. UICC управляет необходимыми конфиденциальными криптографическими данными в целях идентификации пользователя сети мобильной связи. Кроме того, в UICC также можно установить приложения MCP под контролем PSPs.

Мобильный телефон может использоваться как для MCPs, так и для MRPs, в зависимости от требований к телефону. Например, PSP, предоставляющий услугу MRP, может требовать только того, чтобы телефон поддерживал SMS, тогда как другой PSP может требовать загрузки своего платежного приложения в мобильный телефон со специальной платформой. Для MCP требования к мобильным телефонам выше: должны присутствовать контроллер NFC, SE и интерфейсы для защищенных приложений MCP. В отсутствие SE (см. раздел 7.1.3) для MRP можно использовать средства безопасности мобильных телефонов, такие как SIMs и TEEs[20]. В настоящее время считается, что для MCP они недостаточно безопасны.

Мобильные телефоны постоянно совершенствуются и получают все более широкие функциональные возможности. Современные телефоны, так называемые «смартфоны», основаны на (открытых) компьютерных платформах общего назначения, которые могут выполнять очень сложные задачи, они поддерживают цветные дисплеи все большего размера и обеспечивают доступ в сеть Интернет, подобно ПК. Существенно, что смартфоны – основная категория мобильных устройств, доля которых на рынке в настоящее время растет, причем быстрыми темпами [11].

Технология NFC, используемая для бесконтактных платежей, совершаемых посредством мобильного телефона, совместима с протоколами для бесконтактных карт[21]. Телефоны со встроенным модулем NFC могут работать со стандартными считывающими устройствами NFC (например, POI), а также с другими устройствами с NFC. Поэтому они могут использоваться в существующей инфраструктуре по бесконтактным платежным услугам на основе карт.

Следовательно, можно считать, что в SEPA существующие и будущие платежные приложения будут основываться на широкой базе мобильных телефонов с большими возможностями дистанционного управления, доступом в сеть Интернет и цветными дисплеями высокого разрешения, способными обеспечить расширенные функции для пользователя.

7.1.2. ИНТЕРФЕЙС КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ

Управление платежами, совершаемыми посредством мобильного телефона, осуществляется с помощью пользовательского интерфейса на мобильном устройстве. Этот интерфейс включает, например, приложение SMS или USSD, браузер или скачиваемое клиентское приложение, предоставляемое PSP. Мобильные кошельки (см. раздел 8) предусматривают такой интерфейс и могут управляться PSP, но их могут также предоставлять TTPs, и тогда PSPs могут участвовать посредством своих платежных приложений AAUIs.

Хотя самые современные смартфоны имеют очень большие цветные дисплеи и сенсорные интерфейсы, их использование все равно затрудняется неизбежно малым формфактором. Например, формфактор мобильного телефона действительно ограничивает объем информации, которая может выводиться на экран в данный момент времени, и способность пользователя ввести сложный текст. Поэтому важно предоставить простые в использовании интерфейсы мобильного телефона с последовательными действиями пользователя по всем поддерживаемым реализациям для мобильных телефонов.

---

[20] TEE означает «безопасная среда выполнения». Это защищенная область в центральном процессоре телефона для хранения, обработки и защиты важных данных в безопасной среде.

[21] Главное отличие в том, что бесконтактная карта работает «пассивно» т.е. без необходимости в собственном источнике питания, тогда как в мобильном телефоне с технологией NFC может использоваться его аккумулятор для обеспечения дополнительных функциональных возможностей.

7.1.3. ЭЛЕМЕНТЫ БЕЗОПАСНОСТИ

Повышенная безопасность достигается с помощью так называемого элемента безопасности (SE) (сертифицированная устойчивая к постороннему вмешательству отдельная интегральная схема, т.е. «микрочип») для хранения личных данных потребителя и его платежных реквизитов. Опыт использования платежных карт при расчетах показывает, что технология микрочипов является эффективным и недорогим способом повышения безопасности. Кроме того, для SE может использоваться существующая инфраструктура практики оценки и сертификации микрочипов и карт.

Есть несколько альтернативных вариантов использования SEs (см. Приложение II. Элемент безопасности) в мобильном телефоне для поддержания платежей, совершаемых с использованием мобильного телефона. Основные факторы выбора SE в этом контексте следующие:

• контроль и управление SE;

• внутренние характеристики безопасности;

• возможность официальной сертификации по безопасности;

• интеграция в мобильном телефоне и соединение с внешними интерфейсами, такими как бесконтактные или дистанционные протоколы;

• доступность (сроки поставки и географический рынок);

• поддерживающая инфраструктура (средства персонализации);

• возможность использования в существующих коммерческих цепочках поставки по мобильным телефонам;

• экономическая эффективность и экономия за счет роста масштабов.

Выбор типа SE влияет на модель обслуживания по платежам, совершаемым с использованием мобильного телефона. Поэтому EPC сосредоточил внимание на трех типах SE: UICC, вложенный SE и съемный SE (такой как карта микро-SD) и подробно проанализировал различные аспекты модели обслуживания каждого из них (см. [5], раздел 4).

Дополнительная информация по этому вопросу приведена в специальном приложении (см. Приложение II. Элемент безопасности).

Как сказано в разделе 4, для важных операций в MCP требуется использование SE. По MRP плательщик напрямую аутентифицируется на платежном сервере в соответствии с выбранным его PSP методом аутентификации, и это не обязательно требует использования SE. Однако если SE уже имеется для поддержки MCPs, его можно использовать и для MRP, чтобы обеспечить большее удобство для потребителя. Кроме того, использование SE для MRP может повысить безопасность.

7.2. ИНФРАСТРУКТУРА ДЛЯ MCP

В настоящем разделе рассматриваются различные инфраструктурные компоненты, которые используются только для MCP.

7.2.1. ОПЕРАЦИОННАЯ ИНФРАСТРУКТУРА

В инфраструктуре, необходимой для платежной операции MCP, полностью используется уже существующая инфраструктура для осуществления платежей посредством платежной карты. Инвестиции в инфраструктуру для принятия бесконтактных карт также могут использоваться для бесконтактных платежей в зоне SEPA, совершаемых с использованием мобильного телефона.

7.2.2. ОБЕСПЕЧЕНИЕ И УПРАВЛЕНИЕ

В SE должно быть установлено приложение для бесконтактных платежей в зоне SEPA, совершаемых с использованием мобильного телефона (см. раздел 7.1.3). Это означает, что следует определить специальные процессы для обеспечения и управления указанным платежным приложением, которые могут различаться в зависимости от выбранного SE. Ожидается, что для персонализации платежного приложения будут использоваться существующие системы персонализации карт. С этой целью могут быть привлечены TSMs. Дополнительные рекомендации по этому вопросу приведены в [5] и [6].

7.2.3. ПРИЛОЖЕНИЕ MCP

Приложение MCP представляет собой программное обеспечение, установленное в SE, которое реализует функциональные возможности платежной карты в мобильном телефоне под контролем эмитента MCP в соответствии с карточной системой SEPA. Оно имеет прямой доступ к интерфейсу NFC и поэто-

му связано непосредственно с POI. Приложения MCP персонализируются и управляются дистанционно эмитентом MCP или TSM от имени эмитента MCP (см. [5], раздел 5).

Эмитенты MCP могут конкурировать в предложении своих услуг путем настройки приложения MCP, пользовательских функций конфигурации и операций (дистанционного) управления.

Дополнительные рекомендации по приложению MCP приведены в разделе 6 в [5].

7.2.4. ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС ПРИЛОЖЕНИЯ MCP

Приложение MCP может поддерживаться дополнительными приложениями, находящимися в «основной памяти» мобильного телефона, которые называются приложениями пользовательского интерфейса MCP (AAUI) и предназначены для взаимодействия с потребителем (см. [5], раздел 7.3, где приведены дополнительные соображения по этому вопросу). Эмитент MCP отвечает за это приложение, его характеристики безопасности и безопасную связь с приложением MCP.

7.2.5. ТОЧКА ВЗАИМОДЕЙСТВИЯ

POI – это аппаратный и/или программный компонент оборудования торговой точки, который позволяет потребителю использовать карту для совершения покупки в магазине. Кассовый терминал может быть обслуживаемым или необслуживаемым. Новые поколения систем POI позволяют использовать для совершения платежей другие устройства, помимо карт (например, мобильные телефоны или карманные компьютеры).

Однако в основном инфраструктура POI еще не поддерживает NFC и потому требует обновления, которое должно включать потенциально необходимые требования, кроме уже определенных для бесконтактных платежей по картам SEPA, чтобы добиться максимальной эффективности инвестиций. Например, в то время как требования по аппаратным компонентам должны быть одинаковыми, встроенное программное обеспечение может потребовать обновления для поддержки, например правильной обработки мобильных кодов. EPC уже активно участвует в решении этого вопроса вместе со всеми соответствующими организациями по стандартизации и заинтересованными сторонами.

7.3. ИНФРАСТРУКТУРА ДЛЯ MRP

В настоящем разделе рассматриваются различные инфраструктурные компоненты, которые используются только для MRPs.

7.3.1. ОПЕРАЦИОННАЯ ИНФРАСТРУКТУРА

В инфраструктурах, необходимых для дистанционных платежных операций, совершаемых с использованием мобильного телефона, может использоваться уже существующая инфраструктура для дистанционных платежей по картам или платежей SCT (например, торговые интернет-браузеры, 3D secure, дистанционные кошельки и т.д.). Однако, как сказано в главе 5.2, некоторые примеры использования связаны с реализацией общей инфраструктуры.

Как уже отмечено, главное назначение общей инфраструктуры – связать уникальный идентификатор с соответствующими платежными реквизитами получателя, чтобы обеспечить правильную маршрутизацию платежной операции. Она может также использоваться в качестве платформы для дополнительных услуг.

В зависимости от использования общей инфраструктуры (уровень 2) в разделе 5.4.2 показано, что для MRPs в SEPA могут быть рассмотрены две основные модели. Обе модели допускают предложение дополнительных услуг, поскольку пользователи платежей, совершаемых посредством мобильного телефона, ожидают быстрого и надежного обслуживания. Процесс предоставления уведомления считается особенно важным, поскольку, например, предприятиям торговли (услуг) нужно подтверждение платежа перед поставкой купленных товаров или предоставлением услуг.

В обеих моделях эмитенты MRP отвечают за регистрацию клиентов в различных платежных службах MRP.

Итак, главное назначение централизованной общей инфраструктуры – связать уникальный идентификатор с соответствующими платежными реквизитами получателя, чтобы обеспечить правильную маршрутизацию платежной операции. Как минимум, в общей инфраструктуре должны храниться уникальный идентификатор и наименование, IBAN и BIC получателя. Она может также использоваться в качестве платформы для дополнительных услуг.

Эта централизованная общая инфраструктура может быть реализована в различных формах, в том числе следующими способами.

• Как центральный каталог или база данных, позволяющая PSP плательщика после получения уникального идентификатора получателя получить соответствующие реквизиты PSP получателя/счета/карты

(например, наименование, IBAN и/или BIC в случае SCT). При этом PSP плательщика способен отправить платежную операцию в PSP получателя / на счет получателя.

Реквизиты получателя можно получить двумя способами.

- Уникальный идентификатор получателя указывает на URL PSP получателя. В этом случае сопоставлением псевдонима / уникального идентификатора и реквизитов получателя занимается PSP получателя.

- Уникальный идентификатор получателя непосредственно указывает на реквизиты получателя.

• В качестве центрального коммутатора, позволяющего PSP плательщика после получения уникального идентификатора получателя отправить эту информацию в центральный коммутатор. Центральный коммутатор связывает эту информацию с соответствующими реквизитами PSP получателя / счета карты (например, IBAN и/или BIC в случае SCT) и затем направляет платежную операцию в PSP получателя / на счет получателя.

С точки зрения безопасности понятно, что общая инфраструктура должна обеспечивать соответствующий контроль доступа, конфиденциальность, безошибочность и доступность. Сюда может быть включено соблюдение правовых норм, касающихся личной тайны. Кроме того, общая инфраструктура должна надежно обслуживаться, чтобы гарантировать достоверность и актуальность информации.

7.3.2. УНИКАЛЬНЫЙ ИДЕНТИФИКАТОР

Концепция псевдонима представлена в ряде примеров использования в разделах 4 и 5. Псевдоним позволяет однозначно идентифицировать платежный счет получателя. В случае SCT он позволяет связать наименование, BIC и IBAN получателя. В случае дистанционных платежей, совершаемых с использованием мобильного телефона посредством ввода реквизитов платежной карты, он обеспечивает однозначную идентификацию платежного счета получателя (например, с использованием номера мобильного телефона). Обратите внимание, что псевдоним может также служить идентификатором плательщика.

7.3.3. ХРАНЕНИЕ ДАННЫХ MRP И ПРИЛОЖЕНИЕ В МОБИЛЬНОМ ТЕЛЕФОНЕ

В нижеследующем разделе проводится различие между хранением данных / удостоверительных данных, относящихся к дистанционным платежам, и установкой приложения для дистанционных платежей в мобильном телефоне. Хранение данных, относящихся к дистанционным платежам, означает хранение данных в мобильном телефоне для удобства потребителя, чтобы не вводить их вручную при совершении операции. Приложение MRP, по аналогии с приложением MCP, является специальным пакетом программного обеспечения, динамически генерирующим операционные данные.

7.3.3.1. Хранение данных / удостоверительных данных, относящихся к дистанционным платежам

В мобильном телефоне можно хранить статические данные / удостоверительные данные для дистанционных платежей SCT и платежей SCP. Если для этих данных установлены требования по безопасности (безошибочность и/или конфиденциальность), они должны храниться в безопасной среде, например SE. Эти данные могут храниться плательщиком или его PSP. Если они хранятся в безопасной среде, обычно требуется некоторый контроль доступа, например некоторая форма аутентификации, такая как специальный код плательщика или функция управления приложением MRP в PSP.

7.3.3.2. Установка приложения MRP

Для некоторых вариантов реализации MRP может потребоваться установка специального приложения MRP в мобильном телефоне. Если это приложение имеет активные функции безопасности (например, криптографические функции), оно устанавливается в SE. Как и в случае MCP, это приложение MRP требует от PSP плательщика управления всем жизненным циклом, включая обеспечение, активацию, персонализацию и т.д. (см. [21]).

PSP плательщика может передать TSM некоторые из этих функций. Как и в случае MCP, действуют разные требования к ролям, исполняющим эти функции (см. [15] и [18].

7.3.3.3. Обеспечение и управление

Дистанционный платеж SEPA посредством мобильного телефона может потребовать установки специального приложения в SE (см. раздел 7.1.3). Это означает, что необходимо определить специальные процессы по обеспечению и управлению указанным платежным приложением, которые могут различаться в зависимости от выбранного SE. Для этого могут быть привлечены TSM. Дополнительные рекомендации по этому вопросу будут приведены в готовящихся Методических рекомендациях по реализации операционной совместимости MRP.

7.3.4. ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС ПРИЛОЖЕНИЯ MRP

Хотя самые современные смартфоны имеют очень большие цветные дисплеи и сенсорные интерфейсы, их использование все равно затрудняется неизбежно малым формфактором. Например, формфактор мобильного телефона действительно ограничивает объем информации, которая может выводиться на экран в данный момент времени, и способность пользователя ввести сложный текст. Обратите внимание, что для инициирования дистанционных платежей, совершаемых с использованием мобильного телефона, могут применяться различные средства, такие как мобильный браузер, SMS или специальный AAUI.

EPC рассмотрит этот вопрос более подробно в готовящихся Методических рекомендациях по реализации операционной совместимости MRP.

7.3.5. ТОРГОВЫЙ ИНТЕРФЕЙС

В целом предприятия торговли (услуг) предлагают клиентам разные способы совершения покупок, именуемые в настоящем документе «контексты покупки». Например, предприятие торговли (услуг) может предложить использовать SMS, создать мобильный сайт в сети Интернет, предложить специальное мобильное приложение (например, для игр) или принять заранее зарегистрированный псевдоним (например, номер мобильного телефона), подобно традиционной среде POI.

Важное требование с точки зрения предприятия торговли (услуг) и потребителя состоит в том, что процессы покупки и оплаты должны быть удобными для пользователя. Для этого нужно обеспечить, чтобы сочетание платежного средства MRP и мобильного телефона подходило бы для конкретного контекста покупки.

PSP устанавливает некоторые требования к мобильному телефону потребителя исходя из реализации MRP. В простейших случаях достаточно, чтобы потребитель имел возможность использовать SMS или интернет-браузер мобильного телефона (мобильный браузер). В других случаях PSP может потребовать, чтобы потребители загрузили мобильное приложение, например для выбора платежного средства, аутентификации и других подобных целей.

7.3.6. РАСПРЕДЕЛЕНИЕ ПРИМЕРОВ ИСПОЛЬЗОВАНИЯ MRP В ИНФРАСТРУКТУРЕ

В настоящем разделе примеры использования, указанные в разделе 5.2, распределяются по трехсторонней архитектуре, представленной в разделе 5.4.1. В зависимости от примеров использования платеж может быть инициирован на уровне 1 разными способами (см. раздел 5.4.1), такими как платеж посредством мобильного телефона через браузер или мобильные кошельки, в том числе с использованием надежной аутентификации.

По каждому примеру использования в нижеследующей таблице указаны компоненты, которые должны быть добавлены на уровне 2 (например, общая инфраструктура), и возможности предоставления новых услуг на уровне 3 (например, подтверждение платежа, незамедлительность платежа). Обратите внимание, что уровни 2 и 3 находятся в кооперативном пространстве, тогда как уровень 1 остается в конкурентном пространстве.

Таблица 20. **Распределение примеров использования по трем уровням архитектуры MRP**

Три уровня / Примеры использования	Уровень 1: инициирование платежа Возможности подключения и пользовательский интерфейс	Уровень 2: совершение платежа Общая инфраструктура	Уровень 3: переводы денег и движение денежных средств Платежное средство
SCT 1	Например, через мобильный браузер или через специальное приложение MRP	Нет	Существующий SCT
SCT 2	Например, через мобильный браузер или через специальное приложение MRP	Да Общая инфраструктура	Существующий SCT
SCT 3A	Например, через мобильный браузер или через специальное приложение MRP	Да Если используется псевдоним	Существующий SCT + подтверждение платежной услуги
SCT 3B	Например, через мобильный браузер или через специальное приложение MRP	Да Если используется псевдоним	Существующий SCT + подтверждение платежной услуги через службу электронных платежей
SCT 4	Например, через мобильный браузер или через специальное приложение MRP	Да Если используется псевдоним	Существующий SCT + немедленный платеж
SCP 1	Например, через мобильный браузер	Нет	Существующая SCF
SCP 2	Через мобильный кошелек	Нет	Существующая SCF
SCP 3	С надежным механизмом аутентификации при инициировании платежа, например, с использованием специального приложения через мобильный кошелек	Нет	Существующая SCF
SCP 4	Возможно использование мобильного кошелька	Да Общая инфраструктура	Существующая SCF

8. МОБИЛЬНЫЕ КОШЕЛЬКИ

8.1. ОПРЕДЕЛЕНИЕ

Как и обычный кошелек, «цифровой» кошелек, в сущности, содержит идентификационные данные владельца кошелька, данные о платежных средствах, доступных владельцу кошелька, и в некоторых случаях – личные данные его владельца (изображения, документы и т.д.). Это может включать информацию об удостоверениях личности, цифровые подписи и сертификаты, информацию для входа в систему, адреса для выставления счетов и передачи, а также информацию о платежных средствах, таких как продукты SCT и SDD и платежные карты (предварительно оплаченные, дебетовые, кредитные). Кроме того, он может также включать другие приложения, например бонусные баллы, билеты или проездные билеты.

«Цифровой» кошелек будет основан на технической инфраструктуре (аппаратное и программное обеспечение), обеспечивающей безопасное хранение, обработку и передачу указанной выше информации, предоставленной владельцем кошелька, и/или поставщиком услуг, и/или поставщиком (платежного) приложения.

«Цифровой» кошелек позволяет владельцу использовать приложения и данные без ущерба для их безопасности и сохранять в кошельке различные приложения. Кроме того, владелец кошелька ожидает, что услуги, связанные с «цифровым» кошельком, будут хорошо доступны.

«Цифровой» кошелек обычно реализуется в оборудовании, используемом владельцем кошелька. Таким образом, владелец непосредственно контролирует свой кошелек. Однако «цифровой» кошелек может также быть реализован в качестве дистанционного кошелька в схеме передачи «программное обеспечение в качестве услуги».

Помимо технических требований и требований безопасности, которые должны выполняться при использовании/предложении услуг, связанных с «цифровым» кошельком, следует решить вопрос права собственности в отношении «цифрового» кошелька, поскольку это будет зависеть от его реализации.

Следовательно, можно принять следующие определения.

«Цифровой кошелек – это услуга, позволяющая владельцу безопасно получать доступ к идентификационным данным и платежным средствам, управлять ими и использовать их для инициирования платежей[22]. Эта услуга может быть встроена в устройство, принадлежащее владельцу, например мобильный телефон или ПК, или может быть установлена на удаленном сервере, но в любом случае контролируется владельцем».

«Мобильный кошелек – это цифровой кошелек, находящийся в мобильном телефоне».

Дальнейшее развитие концепции и обсуждение основных вопросов, касающихся мобильного кошелька, можно найти в [17].

8.2. МОБИЛЬНЫЕ КОШЕЛЬКИ И ПЛАТЕЖИ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО ТЕЛЕФОНА

В контексте настоящего документа самым важным является вопрос о взаимосвязи между мобильными кошельками и платежами, совершаемыми с использованием мобильного телефона, а конкретнее – влияние мобильных кошельков на действия потребителя в качестве пользователя.

При этом на начальном этапе рассмотрения платежей посредством мобильного телефона важно проанализировать различные ситуации: от более простых, когда в мобильном телефоне имеется одно платежное приложение, до сложных, когда в мобильном телефоне хранятся несколько платежных приложений разного характера (SE с данными карты по платежам NFC, данные карты по дистанционным платежам, виртуальный счет и т.д.).

8.3. ИСПОЛЬЗОВАНИЕ МОБИЛЬНЫХ КОШЕЛЬКОВ ДЛЯ БЕСКОНТАКТНЫХ И ДИСТАНЦИОННЫХ ПЛАТЕЖЕЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО ТЕЛЕФОНА

С точки зрения потребителя кошелек, в сущности, является приложением (или его частью), позволяющим владельцу безопасно получать доступ к данным, управлять данными или даже регистрировать данные, относящиеся к платежу (платежам) (в основном это личные данные, необходимые для идентификации владельца, и данные, необходимые для идентификации и использования платежного средства

[22] Это определение позволяет отличить цифровой кошелек от электронного кошелька, являющегося лишь одним из приложений / платежных средств, которые могут содержаться в цифровом кошельке.

(платежных средств)), а также безопасно сохранять эти данные. Соответствующая информация должна быть доступна в любое время, когда потребитель захочет совершить платеж.

Кошелек должен иметь как минимум следующие функциональные возможности:

• интерфейс для регистрации личных данных и данных по платежным средствам (в мобильном телефоне);

• архив данных для хранения этих данных (в мобильном телефоне);

• интерфейс, позволяющий пользователю выбрать платежное средство;

• интерфейс, позволяющий пользователю использовать платежное средство (один интерфейс, управляющий всеми платежными средствами, или несколько интерфейсов для разных платежных средств);

• интерфейс для управления сохраненными данными и их обновления (обновление, аннулирование и т.д.).

Как сказано выше, приложение для мобильного кошелька может быть очень простым – в случае если оно предназначено для хранения данных и управления ими по одному-единственному платежному средству, или более сложным – в случае нескольких разных платежных средств. Если в кошельке хранятся несколько разных платежных средств, кошелек должен, как минимум, позволять потребителю в любой момент выбрать платежное средство, которое он намерен использовать.

Кроме того, желательно, чтобы кошелек позволял определить платежное средство, используемое по умолчанию – одно для всех видов платежей или, что будет лучше, одно для каждого вида платежей (например, предварительно оплаченная карта X для бесконтактных платежей, кредитная карта Y для дистанционных платежей и т.д.).

В принципе, мобильный кошелек может быть предоставлен PSP, выпускающим платежные средства, и позволит управлять как конкретным платежным средством, так и разными платежными средствами данного PSP. С другой стороны, мобильный кошелек может быть предоставлен TTP, но тогда должна присутствовать возможность управления платежными средствами, выпускаемыми несколькими поставщиками платежных услуг.

Можно ожидать различных вариантов: потребители могут устанавливать в своем мобильном телефоне разные приложения для управления разными платежными средствами или могут управлять разными платежными средствами с помощью одного приложения.

Желательно, чтобы потребитель мог выбирать, каким образом он предпочитает создать и использовать свой кошелек; поставщики платежных услуг должны позволять потребителям управлять (регистрировать и использовать) своими платежными средствами в каждом кошельке[23].

EPC планирует работать над различными аспектами мобильных кошельков.

[23] При условии, что выполняются соответствующие требования (например, по безопасности).

9. СТАНДАРТИЗАЦИЯ И ОТРАСЛЕВЫЕ ОРГАНИЗАЦИИ

Мобильные платежи SEPA требуют тщательной координации стандартов и спецификаций, определенных в нескольких дисциплинах и выпущенных разнородной группой организаций по стандартизации и отраслевых организаций. После EPC наиболее значимыми в данном контексте являются следующие организации.

• ISO

Международная организация по стандартизации (ISO) – крупнейший в мире разработчик международных стандартов. В ISO существуют различные комитеты, которые устанавливают технические стандарты, используемые при осуществлении платежей посредством мобильного телефона, такие как стандарты карт с интегральными схемами, протоколы обмена данными, технология NFC, механизмы безопасности. ISO также решает вопросы в рамках Рабочей группы по платежам, совершаемым с использованием мобильного телефона в ISO TC68 SC7 WG10 (http://www.iso.org).

• ETSI

Европейский институт по стандартам в области телекоммуникаций (ETSI) разрабатывает действующие во всем мире стандарты по информационным и коммуникационным технологиям, включая технологии стационарной связи, мобильной связи, радиосвязи, объединенные технологии, технологии радиовещания и интернет-технологии. ETSI определяет протоколы обмена данными GSM, UMTS и UICC, включая все протоколы доступа (http://www.etsi.org).

• EMVCo

EMVCo осуществляет деятельность по управлению, поддержке и расширению спецификаций карт с интегральными схемами (EMV® Integrated Circuit Card Specifications) для платежных карт на основе микрочипов и приемных устройств, включая терминалы в торговых точках (POS) и банкоматы. EMVCo также устанавливает процедуру испытаний и одобрения в рамках оценки соблюдения спецификаций EMV и управляет этой процедурой. EMVCo в настоящее время принадлежит компаниям «American Express», JCB, «MasterCard» и «Visa» (http://www.emvco.com).

• IETF

Рабочая группа проектирования сети Интернет (IETF) – это крупное открытое международное объединение проектировщиков, операторов, поставщиков и исследователей сетей, занимающееся развитием интернет-архитектуры и обеспечением бесперебойной работы сети Интернет. IETF определяет основу всех интернет-протоколов (http://www.ietf.org).

• GlobalPlatform

GlobalPlatform (GP) – это ведущая международная ассоциация, занимающаяся созданием и обслуживанием совместимой устойчивой инфраструктуры для использования микропроцессорных карт (смарт-карты). Ее технологии поддерживают реализацию нескольких приложений, нескольких действующих субъектов и нескольких моделей обслуживания, что выгодно для эмитентов, поставщиков услуг и поставщиков технологий (http://www.globalplatform.org).

• GSMA

GSMA представляет интересы мирового сектора мобильной связи. Охватывая более 200 стран, GSMA объединяет почти 800 мировых операторов мобильной связи, а также более 200 компаний в более широкой экосистеме мобильной связи, включая производителей телефонов, компании по разработке программного обеспечения, поставщиков оборудования, интернет-компании, средства массовой информации и компании по организации зрелищных мероприятий. Деятельность GSMA сосредоточена на инновациях, развитии и создании новых возможностей для ее членов с конечной целью стимулирования роста сектора мобильной связи (http://www.gsmworld.com).

• Mobey Forum

Mobey Forum – это мировой форум финансового сектора, задачей которого является стимулирование предложения банками мобильных финансовых услуг за счет опыта реализации пилотных проектов, межотраслевого сотрудничества, анализа, обмена опытом, экспериментов, а также сотрудничества и связей с соответствующими внешними заинтересованными сторонами (http://www.mobeyforum.org).

• **NFC Forum**

Near Field Communication Forum – это некоммерческая отраслевая ассоциация, ставящая своей целью расширение использования связи в ближней зоне NFC в потребительской электронике, мобильных устройствах и ПК (http://www.nfcfbrum.org).

• **PCI**

Совет по стандартам безопасности PCI – это открытый всемирный форум, действующий с 2006 года, который отвечает за деятельность по разработке, управлению, образованию и информированию по стандартам безопасности PCI, включая стандарт защиты данных (PCI DSS), стандарт защиты данных в платежных приложениях (PA-DSS) и требования операционной безопасности PIN (PTS) (https://www.pcisecuritystandards.org).

• **W3C**

World Wide Web Consortium (W3C) – это международное сообщество, разрабатывающее стандарты сети Интернет и ставящее своей задачей полное использование ее возможностей (www.w3.org).

10. ЗАКЛЮЧЕНИЕ

Роль EPC

Роль EPC заключается в участии в развитии единого рынка платежей в Европе путем помощи или содействия в разработке и внедрении стандартов, передовой практики и схем. В секторе мобильной телефонной связи достигнуты полное проникновение на рынок и высокий уровень обслуживания, что обеспечивает идеальный канал расширения использования платежных средств SEPA.

В настоящем втором издании «Белой книги» представлен общий обзор мобильных платежей, включая:

- бесконтактные платежи, совершаемые с использованием мобильного телефона;
- дистанционные платежи, совершаемые с использованием мобильного телефона.

Для инициирования платежей главным образом используется мобильный телефон, тогда как EPC использует существующие платежные средства SEPA для самого платежа.

Анализ и распределение приоритетов

Проанализировав различные категории «бесконтактных» (в ближней зоне) и «дистанционных» мобильных платежей, EPC считает приоритетными в области платежей, совершаемых с использованием мобильного телефона, следующие виды платежей:

- бесконтактные платежи в зоне SEPA;
- дистанционные платежи в зоне SEPA;
- дистанционные кредитовые переводы SEPA.

Бесконтактные платежи, совершаемые с использованием мобильного телефона

В бесконтактных платежах по картам SEPA, совершаемых с использованием мобильного телефона, выбор SE сильно влияет на модель обслуживания и роли различных заинтересованных сторон.

В помощь этим заинтересованным сторонам EPC опубликовал Методические рекомендации по реализации операционной совместимости MCP [5].

Дистанционные платежи, совершаемые с использованием мобильного телефона

Определены три основные цели:

- удобство инициирования трансакции и идентификации получателя по платежам, инициируемым плательщиком;
- определенность результата платежа для получателя;
- немедленные (или очень быстрые) платежи.

Последующие действия

Хотя многие из указанных задач не являются специфичными для мобильного канала, их раннее определенное решение важно для того, чтобы платежные средства SEPA стали успешными в мобильном канале. В этом отношении EPC намерен сосредоточить усилия на разработке Методических рекомендаций по операционной совместимости мобильных дистанционных платежей.

Приложение I. Платежные средства SEPA

Платежные средства, развиваемые EPC:

• Кредитовый перевод SEPA (SCT)

Схема SCT позволяет поставщикам платежных услуг предложить основную базовую услугу кредитовых переводов в зоне SEPA как по отдельным, так и по валовым платежам. Стандарты этой схемы облегчают инициирование, обработку и выверку платежей на основе сквозной обработки. Предмет схемы ограничивается платежами в евро в странах SEPA независимо от валюты задействованных счетов. Кредитные организации, осуществляющие кредитовые переводы, должны быть участниками этой схемы, т.е. обе организации должны официально выполнять требования схемы SCT. Ограничения на сумму платежа, совершаемого по этой схеме, отсутствуют.

Свод правил схемы SCT [SCT] и прилагаемые Методические рекомендации по реализации являются окончательными источниками информации о правилах и обязательствах в этой схеме. Кроме того, имеется документ «Быстрый доступ к схемам кредитового перевода в зоне SEPA» («Shortcut to the SEPA Credit Transfer Scheme»), в котором представлена основная информация о характеристиках и преимуществах схемы SCT.

• Безакцептное списание SEPA (SDD)

Основная схема SDD – подобно любой другой схеме безакцептного списания – основана на следующей концепции: «Мне требуется денежный перевод от другого лица с его предварительного согласия, и я зачисляю сумму перевода на свой счет».

Основная схема SDD [SDD] распространяется на операции в евро. Дебитор и кредитор должны иметь счета в кредитной организации, находящейся в зоне SEPA. Кредитные организации, совершающие операцию безакцептного списания, должны быть участниками схемы, т.е. обе организации должны официально выполнять требования схемы SDD. Эта схема может использоваться для однократного (единовременного) или периодического безакцептного списания; ограничения на суммы отсутствуют.

• Карточная система SEPA (SCF)

SCF [SCF], разработанная EPC, – документ, определяющий политику в отношении того, каким образом участники рынка платежных карт (такие как карточные схемы, эмитенты карт, предприятия торговли (услуг), принимающие платежные карты, и другие поставщики услуг) должны адаптировать свою текущую деятельность для приведения ее в соответствие с концепцией SEPA по платежам в евро, совершаемым с использованием банковских карт. Хотя участник рынка сам определяет, приводить ли ему свои системы в соответствие с требованиями SCF, члены EPC обязуются выполнять условия SCF в качестве эмитентов и эквайреров.

Приложение II. Элемент безопасности

Элемент безопасности – это сертифицированный, устойчивый к постороннему вмешательству модуль (устройство или компонент интегральной схемы), способный безопасно сохранять и выполнять приложения и их криптографические данные (например, ключи) в соответствии с политикой и требованиями безопасности, установленными соответствующими организациями (например, эмитентом приложения MCP, эмитентом SE). SE обеспечивает защиту приложений, включая разделение приложений.

Особые ограничения, связанные с формфактором мобильных телефонов

Независимо от окончательного типа используемых SE и в противоположность физическим платежным картам следует предусмотреть особые условия в связи с тем, что в большинстве случаев PSPs, предоставляющие приложение для платежей, совершаемых с использованием мобильного телефона, не отвечают за распространение мобильных телефонов и SE. Основные причины этого следующие.

• В мобильном телефоне в любой определенный момент времени может быть установлено только ограниченное количество SE. Замена SE пользователем в мобильном телефоне часто очень неудобна.

• Сам мобильный телефон обычно не предоставляется PSP и, в противоположность ситуации с платежными картами, принадлежит непосредственно потребителю. Выбор мобильных телефонов потребителями напрямую основан на характеристиках устройства (технические возможности, дизайн, стоимость и т.д.), а не на требованиях поставщиков приложений. Поэтому поставщик приложения, пытающийся распространять свои собственные мобильные телефоны, будет вынужден предлагать широкий выбор доступных моделей от хорошо известных производителей мобильных телефонов (подобно тому, как уже делают все MNO по спонсируемым ими устройствам), что означает чрезмерные операционные расходы.

• Поскольку обычно потребитель пользуется только одним мобильным телефоном, этот телефон должен быть пригоден для различных поставщиков приложений, чтобы обеспечить конкурентное справедливое рыночное пространство для мобильных услуг.

Элементы безопасности для платежей, совершаемых с использованием мобильного телефона

EPC участвовал в подготовке документа Mobey Forum «Альтернативы для банков при предоставлении услуг по безопасным платежам, совершаемым посредством мобильного телефона», в котором представлен обзор существующих предложений для SE [16]. В нем рассматриваются следующие типы устройств:

• Стикеры

Бесконтактные карты, изготавливаемые в виде стикера, которые могут быть персонализированы и могут обрабатываться с помощью существующей платежной инфраструктуры. Потребители могут разместить стикер в своем мобильном телефоне для платежей с использованием технологии NFC.

• Карта Secure Micro SD

Карты памяти с встроенным микрочипом, которые могут использоваться в качестве SE (устанавливаются в мобильном телефоне или отдельно). Эти карты Secure Micro SD могут также иметь антенну NFC.

• Universal Integrated Circuit Card (UICC)

Универсальный стандартизированный SE, принадлежащий MNO и предоставляемый MNO.

• Встроенный SE

SE, встроенный в мобильный телефон при его изготовлении.

• Trusted Mobile Base

Защищенный изолированный раздел центрального процессора мобильных телефонов, в котором могут храниться защищенные приложения.

EPC дополнительно проанализировал эти различные типы SE и установил в своей последующей работе (см. [5]) такие приоритетные формфакторы SE:

• UICC;

• встроенный SE;

• съемный SE, такой как карта Secure Micro SD.

Ссылки и библиография

[1]	Little, Arthur D. «Global M-Payment Report Update, 2009»: http://www.adlittle.com/reports.html?view=389
[2]	EMVCo: http://www.emvco.com/
[3]	Европейский платежный совет. «EPC397-08 Customer-to-Bank Security Good Practices Guide»: http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=225
[4]	Европейский платежный совет. «EPC 020-08 SEPA Cards Standardisation (SCS) Volume – Book of Requirements»: http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=521
[5]	Европейский платежный совет. «EPC 178-10 Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines»: http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=557
[6]	Европейский платежный совет – Ассоциация GSM. «EPC 220-08 Mobile Contactless Payments Service Management Roles – Requirements and Specifications»: http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=423
[7]	Европейский институт по стандартам в области телекоммуникаций: http://www.etsi.org
[8]	Европейский институт по стандартам в области телекоммуникаций TS 102 221, TS 102 223, TS 102 22 и TS 102 226.
[9]	Global Platform: http://www.globalplatform.org
[10]	Ассоциация GSM: http://www.gsmworld.com
[11]	Пресс-релиз IDC от 30 июля 2009 года «Smartphone Growth Encouraging, Yet the Worldwide Mobile Phone Market Still Expected To Shrink in 2009»: http://www.idc.com/about/viewpressrelease.jsp?containerId=prUS21950309&sectionId=null&elementId=null&pageType=SYNOPSIS
[12]	Международная организация по стандартизации: http://www.iso.org
[13]	Рабочая группа проектирования Интернета: http://www.ietf.org
[14]	Международный союз электросвязи. «World Telecommunication/ICT Indicators Database 2010 (15th Edition)»: http://www.itu.int/ITU-D/ict/publications/world/world.html
[15]	Mobey Forum: http://www.mobeyforum.org
[16]	Mobey Forum. «Alternatives for Banks to offer Secure Mobile Payments (version 1.0)»: http://www.mobeyforum.org/Press-Documents/Press-Releases/Alternatives-for-Banks-to-offer-Secure-Mobile-Payments
[17]	Mobey Forum. «Mobile wallet – Definition and vision – Part 1»: http://www.mobeyforum.org/Press-Documents/Press-Releases/Mobey-Forum-White-Paper-Provides-a-New-Perspective-on-Market-Development
[18]	NFC Forum: http://www.nfc-forum.org/home
[19]	Директива по платежным услугам: Директива 2007/64/ЕС Европейского парламента и Совета от 13 ноября 2007 года по платежным услугам на внутреннем рынке
[20]	Ассоциация производителей карт SD: https://www.sdcard.org/developers