



УТВЕРЖДЕНО

Протоколом заседания Совета Директоров
ЗАО «Межбанковский Процессинговый Центр»
№22/25 от 21 июля 2025 года

СОГЛАСОВАНО

Протоколом заседания Правления
ЗАО «Межбанковский Процессинговый Центр»
№31/2025 от 19 июня 2025 года

**Технический регламент
Основного оператора взаимодействия**

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ	3
2. ТЕРМИНЫ И СОКРАЩЕНИЯ	3
3. АРХИТЕКТУРА СИСТЕМЫ И СХЕМА ИНФОРМАЦИОННОГО ПОТОКА...	4
4. ТРЕБОВАНИЯ К ПРОЦЕССУ ПРОВЕДЕНИЯ ПЛАТЕЖА	5
5. ТЕЛЕКОММУНИКАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ И ТРЕБОВАНИЯ К КРИПТОГРАФИИ	6
6. СЕТЕВОЕ ВЗАИМОДЕЙСТВИЕ.....	8
7. КЛИРИНГ ПЛАТЕЖЕЙ	9
8. ЗАКРЫТИЕ ОПЕРАЦИОННОГО ДНЯ	10
9. ИНТЕГРАЦИОННЫЕ АРІ И ТРЕБОВАНИЯ К ГЕНЕРАЦИИ QR-КОДОВ	13
10. ТРЕБОВАНИЯ К ЧЕКУ И СТАТУСАМ ПЛАТЕЖЕЙ ПО QR.....	16
Приложение №1	17

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Технический регламент Основного оператора взаимодействия (далее – ТР ООВ) устанавливает основные технические условия функционирования ООВ.
- 1.2. ТР ООВ, его приложения и дополнения являются неотъемлемой частью Операционных правил ООВ и являются обязательными для исполнения всеми Участниками Системы ООВ.
- 1.3. ТР ООВ трактуется, как есть и принимается всеми Участниками без ограничения условий.
- 1.4. Неисполнение, частичное исполнение, несоответствие, неполное соответствие участников ТР ООВ влечет за собой ответственность в соответствии с Операционными правилами ООВ.

2. ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем документе для наилучшего практического применения и понимания используются следующие сокращения и термины:

Термины	Определение
Система	Согласно Операционным правилам ООВ
PSP	Payment Service Provider – платежное приложение/сервис Участников ООВ для оплаты товаров, услуг и работ.
API	Application Programming Interface — интерфейс программирования, интерфейс создания приложений
JSON	JavaScript Object Notation — формат хранения и обмена информацией, доступной для чтения человеком. Файл содержит только текст и использует расширение json.
Merchant Category Code (далее – MCC)	Код классификации торгово-сервисного предприятия
payqr.kg	web-ресурс ООВ
PSP Отправитель	Участник, предоставляющий Плательщикам сервис для отправки финансовых услуг и инициирующий проведение платежа.
PSP Получатель	Участник, предоставляющий Получателям сервис по генерации QR-кодов и получению Платежей.
Интерфейс	«Общая граница» между системами Субъектов настоящих Правил, через которую обеспечивается информационное взаимодействие, используя совокупность средств и правил.
Платёжное Ядро	Центральная часть Системы, обеспечивающая приложениям координированный доступ к ресурсам компьютера, таким как процессорное время, память, внешнее аппаратное обеспечение, внешнее устройство ввода и вывода информации. Также обычно ядро предоставляет сервисы файловой системы и сетевых протоколов.

Режим реального времени	Режим обработки платёжных документов, информации, обеспечивающий немедленное взаимодействие системы обработки платежных документов, информации с внешними процессами в темпе, соизмеримом со скоростью протекания этих процессов.
Роли	Наборы прав доступа к Панели удалённого доступа.
ОВ	Оператор взаимодействия
Основной ОВ	ЗАО «МПЦ»
PSP-ОВ	ОВ, интегрированный в систему основного ОВ

3. АРХИТЕКТУРА СИСТЕМЫ И СХЕМА ИНФОРМАЦИОННОГО ПОТОКА

3.1. Архитектура Системы ООВ включает в себя основной и резервный сайт аппаратно-программного комплекса Системы ООВ, платежных приложений/сервисов.

3.2. Аппаратно-программный комплекс Системы ООВ в архитектуре REST-системы и представляет из себя набор сервисов, предоставляющий внешние и внутренние API-интерфейсы для взаимодействия с Системой в режиме реального времени.

3.3. Аппаратно-программный комплекс Системы ООВ состоит из подсистем: Ядро, Панель удалённого доступа и SFTP.

3.4. Ядро Системы ООВ имеет следующие основные сущности обеспечивает основные процессы проведения платежа и закрытие дня:

- Участник – Прямой участник Системы с отдельным суточным лимитом для каждого из своих PSP;
- Лимит участника – информация о текущем доступном суточном балансе Прямого участника в системе ГСРРВ;
- Лимит PSP – информация о текущем доступном суточном балансе PSP на балансе Прямого участника;
- PSP – Платежное приложение/сервис Участников ООВ для оплаты товаров, услуг и работ);
- PSP Apps – набор данных для доступа PSP к API;
- Транзакция – минимальная логически осмысленная операция, содержащая учётный набор данных по движениям средств в рамках PSP Участников.

3.5. **Панель удаленного доступа** предоставляет возможность удаленного доступа к системе:

3.5.1. **Роли:**

- Оператор Прямого участника;
- Оператор Ассоциата.

3.5.2. **Права доступа:**

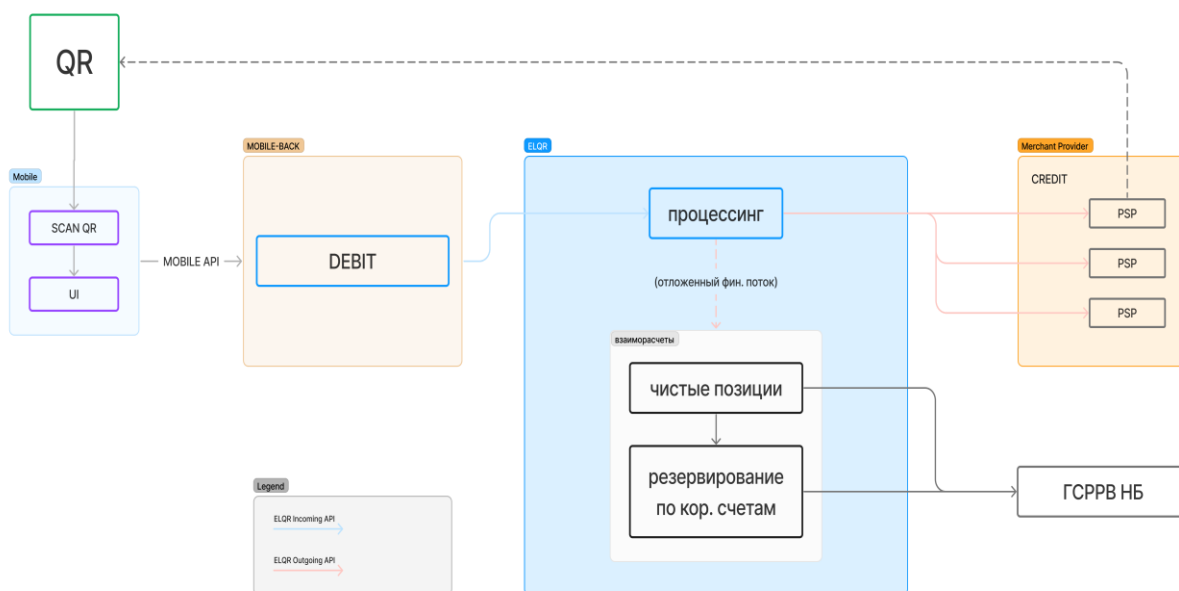
- Управление всеми участниками;
- Управление лимитами всех участников;
- Доступ к информации по платежам в режиме реального времени;
- Управление пользователями и их доступами к Системе;
- Мониторинг платежей;
- Статус платежа в Системе.

3.6. **SFTP** – протокол прикладного уровня передачи файлов, предназначенный для обмена данными с Участниками по проведённым платежам.

- В системе формируются следующие типы финансовых сообщений:

№	Тип финансовой операции	Тип транзакции
1	Платёж, проводимый физическим лицом в адрес физического лица (C2C)	«10»
2	Платёж, проводимый физическим лицом в адрес юридического лица (C2B)	«20»
3	Платёж, проводимый физическим лицом в адрес государственного органа (C2G)	«30»
4	Платёж, проводимый юридическим лицом в адрес физического лица (B2C)	«40»
5	Платёж, проводимый юридическим лицом в адрес юридического лица (B2B)	«50»
6	Платёж, проводимый юридическим лицом в адрес государственных органов	«70»
7	Установка Резерва в корреспондентских счетах Прямых участников в ГСРРВ	«60»

Рисунок 1. Общая схема информационного взаимодействия



4. ТРЕБОВАНИЯ К ПРОЦЕССУ ПРОВЕДЕНИЯ ПЛАТЕЖА

4.1. Требование для PSP получателя

4.1.1. Общее время ответа на каждый онлайн запрос к Системе PSP Получателя, в рамках интеграции, **не должен превышать – 2 (две) секунды**, т.е.

- Запрос на возможность платежа: check.request/response – не более 2 сек.
- Запрос на создание платежа: create.request/response – не более 2 сек.
- Запрос на выполнение платежа: execute.request/response – не более 2 сек.
- Запрос на уточнение статуса платежа: state.request/response – не более 2 сек.

- 4.1.2. При получении не финального статуса «В обработке» на Запрос на уточнение статуса платежа Система будет **повторять Запрос на уточнение статуса платежа в течение 45 секунд** для платежей с момента отправки Запроса на выполнение платежа, после чего Система автоматически отменяет платеж.
- 4.1.3. При получении не валидного статуса платежа:
- ответы не по протоколу – будет применено правило п.4.1.2.
 - сетевые ошибки, недоступность систем и т.д. – система в одностороннем порядке **отменяет платёж через 3600 секунд** с момента отправки Запроса на выполнение платежа.
- 4.1.4. На все отмененные платежи, указанные в п. 4.1.2. и 4.1.3., будет применено правило переноса ответственности: «финансовые риски и ответственность несет та сторона, которая не соответствует требованиям Основного оператора взаимодействия».
- 4.1.5. Участники обязаны строго соблюдать установленные в утверждённом протоколе сроки ответа на запросы. Такие ограничения защищают от "зависших" транзакций и обеспечивают согласованность состояния в системе.
- 4.1.6. Ответ на запросы должен соответствовать формату, описанному в утверждённом протоколе, включая корректный формат, обязательные поля, кодировку, структуру сообщения и формат времени;

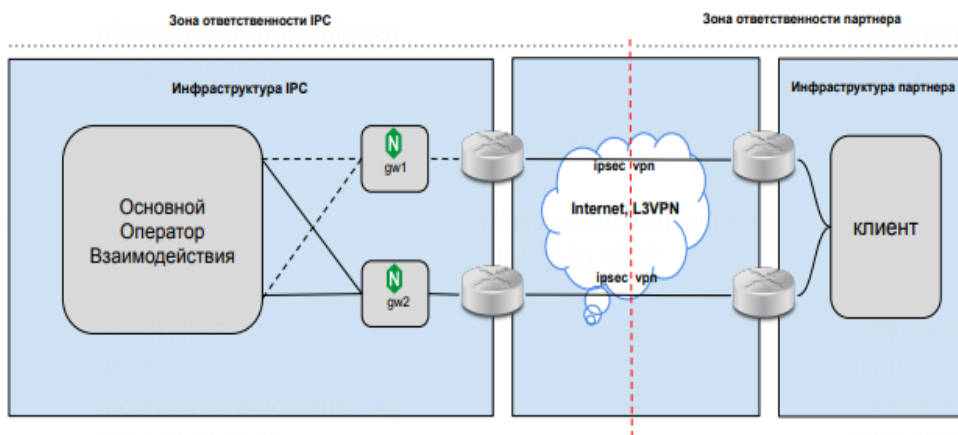
4.2. Требования для PSP отправителя

- 4.2.1. Запрашивать статус платежа у ООВ необходимо всегда после Запроса на выполнение платежа.
- 4.2.2. Если при попытке Запроса на выполнение платежа получен таймаут от ООВ, необходимо запрашивать статус платежа и ориентироваться на полученные данные о статусе от ООВ.
- 4.2.3. При запросе статуса платежа от ООВ PSP Отправитель обязан ориентироваться только на статус платежа, полученный ООВ. Отклонение и завершение платежа предусматривается только со стороны ООВ.
- 4.2.4. Время между получением запроса на Создание платежа со стороны ООВ и получением Запроса на выполнение платежа ограничено 1 минутой. После прохождения этого времени Система в автоматическом режиме переводит платеж в статус Отменен.
- 4.3. Требования к процессу проведения платежа между ОВ и ООВ будут регламентированы отдельными соглашениями.

5. ТЕЛЕКОММУНИКАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ И ТРЕБОВАНИЯ К КРИПТОГРАФИИ

- 5.1. В рамках ООВ используются следующие схемы телекоммуникационного подключения локальных и зарубежных партнеров:
- L3VPN
 - Internet-VPN

Рисунок 2. Схема сетевого взаимодействия.



5.2. Решение о выборе первичной или постоянной схемы телекоммуникационного взаимодействия, а также о количестве подключений, принимается Участником и ООВ индивидуально, с учётом типа подключения (тестовое или продуктивное) и минимальных требований, приведённых ниже для каждого типа подключения.

Промышленный контур (хосты даны для примера):

- хосты: prod-gw1.elpay.kg и prod-gw2.elpay.kg;
- протокол подключения: https;
- для работы в продуктивной среде с высокой нагрузкой;
- операции проводятся с учётом высоких требований к безопасности, доступности и производительности.

Тестовый контур (хосты даны для примера):

- хосты: test-gw1.elpay.kg и test-gw2.elpay.kg;
- протокол подключения: https;
- для разработки, тестирования и предварительной проверки взаимодействия;
- используется исключительно для непроизводственных задач и проведения тестов.

5.3. Проверка доступности хостов выполняются со стороны Участника.

5.4. Хосты работают независимо друг от друга, обеспечивая балансировку нагрузки и надёжное функционирование Системы ООВ.

5.5. Обязательные минимальные требования к подключению:

5.5.1. для продуктивного контура обязательно не менее 2-х подключений и только по схеме L3VPN.

5.5.2. использование Internet-VPN допустимо только для тестовых контуров, как локальных, так и зарубежных партнеров.

5.5.3. схема подключения Internet-VPN для продуктивного контура для зарубежных партнеров допустима в исключительных случаях и рассматривается индивидуально при невозможности реализации L3VPN через выделенные каналы связи.

5.5.4. На этапе проектных работ, допустимо применение Internet-VPN с обязательной реализацией схемы подключения L3VPN при выходе в опытно-промышленную или промышленную эксплуатацию только для зарубежных партнеров.

5.6. **Использование L3VPN через выделенные каналы связи.** Подключение к ООВ предусматривает два варианта:

5.6.1. Участник организует прямое подключение к ЦОД ООВ;

5.6.2. Участник организует подключение по выделенным каналами связи через локальных интернет-провайдеров партнеров ООВ. Список партнёров интернет-провайдера определяет ООВ.

- 5.7. Номер VLAN согласовывается между ООВ, интернет-провайдером и Участником по форме Заявки, указанной в Приложении №1 к настоящему ТР ООВ.
- 5.8. Минимальное количество подключений – 2 (Два) L3VPN, через разных интернет-провайдеров для продуктового контура.
- 5.9. Транспортный туннель создаётся с использованием двух маршрутизаторов ООВ, подключённых к разным провайдерам связи для обеспечения независимости каналов и надёжности соединения в заявке по форме, указанной в Приложении №2.
- 5.10. Участник подключается к ООВ через свои граничные для обеспечения связи с ООВ.
- 5.11. Безопасность информации при передаче данных на канальном уровне обеспечивается с использованием технологий на основе протокола шифрования IPSEC. Минимальный уровень криптостойкости:
- 5.11.1. размер блока: 128 бит;
- 5.11.2. длина ключа: 256 бит;
- 5.11.3. срок использования ключа: до 2 (двух) лет.
- 5.12. Необходимые IP-адреса межхостового соединения выделяет ООВ.
- 5.13. Безопасность информации на прикладном уровне обеспечивается с использованием протокола HTTPS (Hyper Text Transfer Protocol over TLS).
- 5.14. **Использование Internet-VPN.** В случае отсутствия других возможностей при организации взаимодействия с Международным участником на этапе тестирования допускается подключение через сеть Интернет посредством VPN.
- 5.15. Транспортный туннель создаётся с одной стороны маршрутизаторами ООВ, с другой — граничными маршрутизаторами на площадке Международного участника.
- 5.16. Безопасность информации при передаче данных по публичным каналам связи обеспечивается с использованием технологий на основе протокола шифрования IPSEC. Минимальный уровень криптостойкости:
- 5.16.1. размер блока: 128 бит;
- 5.16.2. длина ключа: 256 бит;
- 5.16.3. срок использования ключа: до 2 (двух) лет.
- 5.17. Необходимые IP-адреса межхостового соединения выделяет ООВ.
- 5.18. Безопасность информации на прикладном уровне обеспечивается с использованием протокола HTTPS (Hyper Text Transfer Protocol over TLS).

6. СЕТЕВОЕ ВЗАИМОДЕЙСТВИЕ

6.1.Онлайн взаимодействие:

- 6.1.1. Взаимодействие с API (Ядро системы), Панелью удаленного доступа осуществляется посредством HTTPS;
- 6.1.2. Обмен оффлайн-сообщениями осуществляется по посредством SFTP;
- 6.1.3. Все программные интерфейсы используют JSON API.

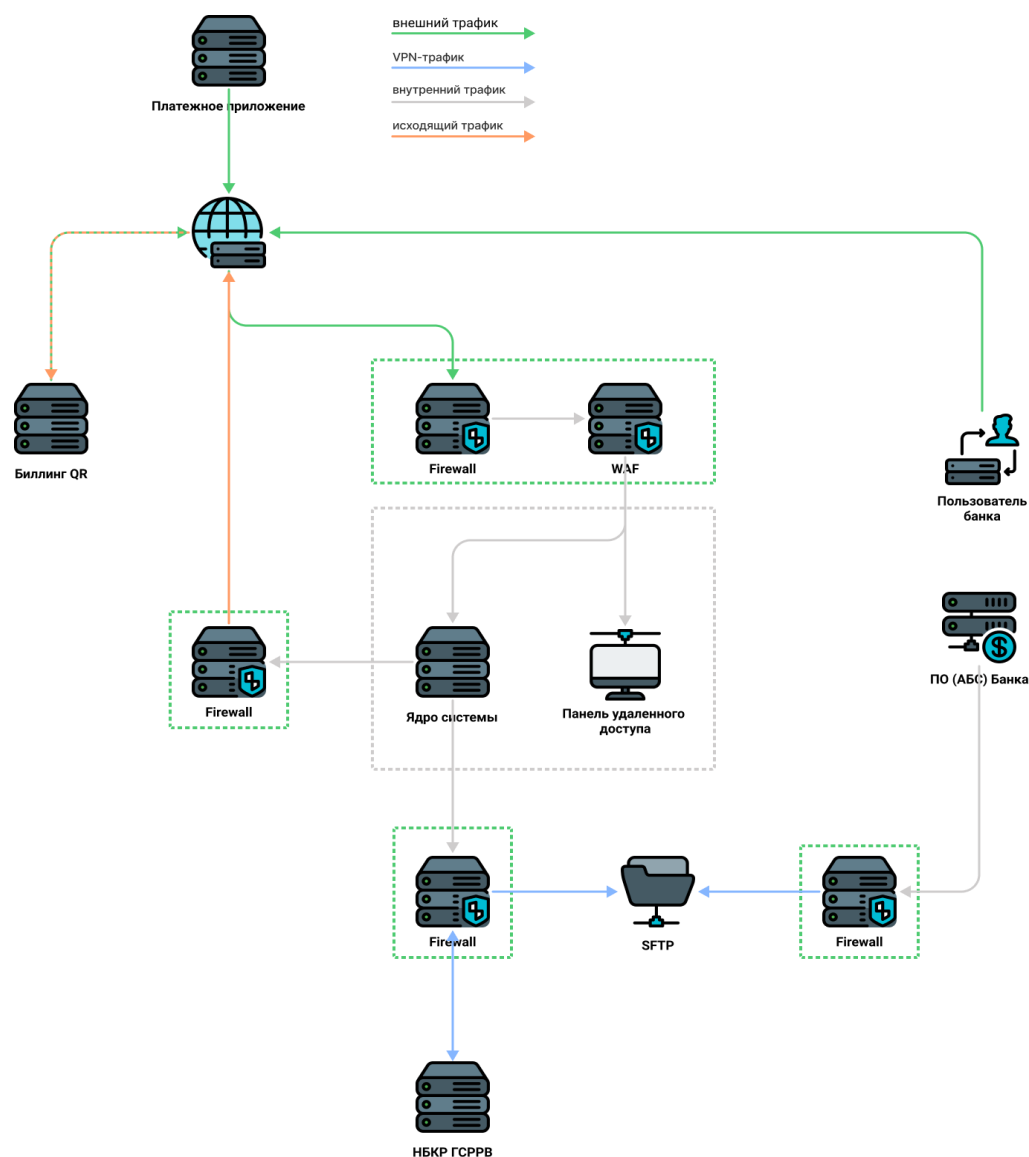


Рисунок 2. Схема сетевого взаимодействия.

7. КЛИРИНГ ПЛАТЕЖЕЙ

7.1 Процесс процессинга платежей состоит из 5-этапов:

- Этап 1: установка Участниками лимита на операции в операционной панели ООВ;
- Этап 2: резервирование ООВ денежных средств в ГСРРВ;
- Этап 3: приём, отправка и обработка платежей в течение Операционного дня в рамках лимитов;
- Этап 4: процедура Закрытия Операционного дня и отправка файлов чистых позиций в систему ГСРРВ;
- Этап 5: проведение взаиморасчетов в ГСРРВ.

7.2. В процессе проведения взаиморасчётов производится обработка и сверка полей, как в процессе проведения платежей, так и статично:

- БИК отправителя;
- расчётный счёт отправителя;
- БИК получателя;
- расчётный счёт получателя;
- дополнительные поля.

7.3. Для входящих в Систему ООВ/иного ОВ платежей/переводов дебетовый баланс в Системе ООВ/иного ОВ и кредитовый баланс Участника-получателя не изменяются.

7.4. Для исходящих из Системы ООВ/иного ОВ платежей/переводов дебетовый баланс в Системе ООВ/иного ОВ и кредитовый баланс Участника-получателя изменяются.

7.5. Алгоритм проведения Платежа состоит из следующих этапов:

1. Этап: Участник в своей информационной системе/мобильном приложении генерирует QR-код/платёжную ссылку и передает ее Плательщику/Отправителю;

2. Этап: Плательщик/Отправитель с помощью информационной системы/мобильного приложения Участника-получателя сканирует QR-код или переходит по платёжной ссылке;

3. Этап: Плательщик/Отправитель, указывает сумму платежа (там, где применимо) и заполняет дополнительные поля;

4. Этап: после заполнения и сверки платёжных данных, Плательщик/Отправитель подтверждает Платёж;

5. Этап: Участником направляются электронные сообщения в ООВ на проверку и создание платежа;

6. Этап: ООВ определяет Платёжное приложение/ Сервис и Получателя, и направляет соответствующие электронные сообщения Участнику-получателю;

7. Этап: при успешной обработке данных, ООВ создает платёж, который принимается для последующей обработки. В противном случае, возвращает Участнику соответствующую ошибку;

8. Этап: Участник-получатель направляет финальный статус платежа в ООВ для направления Участнику-отправителю;

9. Этап: после получения финального статуса и обновления статуса платежа, Участником формируется trans_ID в сформированном чеке для плательщика.

7.6. Запрещается при проведении платежей использовать любые технические уловки согласно Операционным правилам ООВ.

7.7. ООВ блокирует платежи, превышающие установленные размеры лимитов.

8. ЗАКРЫТИЕ ОПЕРАЦИОННОГО ДНЯ

8.1. Ежедневно, каждый операционный день в 09:05:00 запускается процесс закрытия Операционного дня.

8.2. Процесс закрытия Операционного дня состоит из следующих этапов:

- Этап 1: формируются сводные данные по прошедшим платежам в разрезе каждого Участника (даже при нулевых оборотах) и его Агентов.
- Этап 2: формируется и отправляется файл чистых позиций в ГСРРВ.
- Этап 3: после получения успешного ответа от ГСРРВ, в ГСРРВ отправляются файлы установки резервов по каждому Участнику.
- Этап 4: после получения успешного ответа от ГСРРВ по установке резервов по каждому Участнику, производится процесс закрытия дня:
 - обновление/пересчёт балансов Участников;
 - обновление статусов отправки Платежей на обработку;
 - формируются и передаются клиринговые отчёты для всех Участников согласно установленному формату;
 - в случае ошибок в процессе закрытия дня шаг перезапускается сначала.

Рисунок 3. Регламент закрытия дня.



8.3. При закрытии операционного дня ОВ-получатель не включает в расчёт чистой позиции платежи, полученные от другого ОВ-отправителя;

8.4. ОВ-отправитель формирует файл чистых позиций по всем платежам/переводам, включая платежи отправленные в сторону ОВ-получателя по дебетовой и кредитовой части;

8.5. ОВ отправляют сформированные файлы чистых позиций в ГСРРВ, согласно регламенту ГСРРВ Национального банка КР.

8.6. Оффлайн сообщения.

8.6.1. к оффлайн сообщениям относятся процессы осуществляемые в процессе закрытия дня;

8.6.2. обмен файлами осуществляется посредством SFTP;

8.7. Система поддерживает следующие оффлайн сообщения:

8.7.1. Interbank Settlement file – ГРОСС-файл (внутренний формат системы ГСРРВ):

файл формирует: Система ООВ.

файл принимает: ГСРРВ.

расписание: один раз в рабочий день.

назначение: файл двусторонних чистых позиций для проведения окончательного расчета между банками за проведенные транзакции.

8.7.2. Файл установки резервов – ГРОСС-файл (внутренний формат системы ГСРРВ):

файл формирует: Система ООВ.

файл принимает: ГСРРВ.

расписание: один раз в рабочий день.

назначение: файл установки резерва банка в ГСРРВ.

8.7.3. Клиринг файл – JSON-файл (внутренний формат Системы):

файл формирует: Система ООВ.

файл принимает: Участник.

расписание: один раз в рабочий день.

Назначение: файл содержащий список платежей, успешно принятых и попавших в закрытие дня.

8.8. Формат клирингового файла.

Клиринговые файлы формируются и направляются Участнику в рабочие дни, путём выкладывания файлов на SFTP-директорию соответствующего Участника и содержат операции, прошедшие в рамках операционного дня. Файлы формируются в формате JSON и имеют следующую схему:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    "transaction_id": {
      "type": "string"
    },
    "transaction_type": {
      "type": "string"
    },
    "amount": {
      "type": "integer"
    },
    "interchange": {
      "type": "integer"
    },
    "psp_id": {
      "type": "integer"
    },
    "psp_name": {
      "type": "string"
    },
    "aqr_bic": {
      "type": "string"
    },
    "iss_bic": {
      "type": "string"
    },
    "bic": {
      "type": "string"
    },
    "bank_account_id": {
      "type": "integer"
    },
    "bank_account": {
      "type": "string"
    },
    "executed_time": {
      "type": "string"
    },
    "created": {
      "type": "string"
    }
  },
  "required": [
    "transaction_id",
```

```

    "amount",
    "transaction_type",
    "interchange",
    "psp_id",
    "psp_name",
    "aqr_bic",
    "iss_bic",
    "bank_account_id",
    "bank_account",
    "executed_time",
    "created"
  ]
}

```

Описание полей

transaction_id – идентификатор транзакции в Системе

transaction_type – тип транзакции

amount - сумма Платежа (в тыйынах)

interchange – размер межбанковский комиссии

psp_id – уникальный идентификатор Участника

psp_name – Наименование Участника

aqr_bic – БИК банка Участника-отправителя

iss_bic – БИК банка Участника-получателя

bic – БИК банка Участника

bank_account_id – уникальный идентификатор счета Участника

bank_account – номер счета Участника

executed_time – дата и время проведения Платежа

created – дата и время создания Платежа

9. ИНТЕГРАЦИОННЫЕ API И ТРЕБОВАНИЯ К ГЕНЕРАЦИИ QR-КОДОВ

- 9.1. Платёжные приложения должны быть размещены на официальных платформах/магазинах приложений операционных систем технических устройств (Google Play, App Store и др.).
- 9.2. Платёжные приложения должны обеспечивать при запуске приложения аутентификацию пользователей посредством ввода ПИН/пароля. Допустимы альтернативные варианты аутентификации в зависимости от имеющегося функционала технического устройства (сканер отпечатка, распознавание лиц).
- 9.3. Онлайн-интеграция с Системой ООВ для осуществления платежей производится на основе внешнего входящего API, расположенного по адресу <https://api.elpay.kg:5050/docs/API-IPS-latest.html>.
- 9.4. Онлайн интеграция Системы ООВ с Участником-получателем для приёма платежей осуществляется на основе исходящего API, расположенного по адресу <https://api.elpay.kg:5050/docs/API-IPS-Outgoing-latest.html>.
- 9.5. Для приёма платежей через Систему ООВ, в соответствии со Стандартом необходимо реализовать поддержку полей.
- 9.6. Хост для QR-кодов <https://payqr.kg#> или <https://pay.payqr.kg#>.

Таблица 1. Наименование полей в рамках Стандарта¹

№	Наименование поля/пункта	Требование Стандарта	Требование Регламента
1	ID32 поле 00 (Уникальный идентификатор)	О	М
2	ID32 поле 01 (Спецификация платежной сети)	М	С
3	ID33 поле 00 (Уникальный идентификатор поставщика услуг)	-	М
4	ID33 поле 01 (Наименование услуги)	-	М

- 9.7. Поддержка полей, указанных в Таблице 1 обязательна для всех Участников.
- 9.8. Участники обязаны унифицировать формат URL-ссылок для оплаты через QR-коды в своих мобильных приложениях.
- 9.9. Приложение Участника должно корректно обрабатывать все виды платёжных ссылок в соответствии с протоколом национального QR-кода.
- 9.10. Генерация QR-кодов в приложении должна использовать хост <https://payqr.kg> или <https://pay.payqr.kg>.
- 9.11. Участники обязаны обеспечивать корректную и стабильную работу своих приложений в части обработки ссылок [payqr](https://payqr.kg).
- 9.12. В случае внесения изменений в техническую реализацию, связанную с поддержкой ссылок [payqr](https://payqr.kg), участник обязан уведомить ООВ для тестирования и актуализации данных на сайте payqr.kg.
- 9.13. Участники обязуются поддерживать актуальные данные о приложении (иконка, схема и название) в системе ООВ.
- 9.14. Иконки приложения необходимо отправлять на электронную почту согласно Операционному регламенту ООВ.
- 9.15. Приоритет переходов в приложение будет предоставлен по принципу «первого запроса», то есть приоритет отдается тем приложениям, которые первыми подали заявку на изменение.
- 9.16. Участники обязаны привести действующие ссылки к единому формату ссылок приложения (deeplink) с уникальными префиксами и корректно обрабатывать для каждого Участника. Например, ссылка вида <https://payqr.kg#...> должна вызывать [elqr-bank-deep-link://payqr.kg](https://payqr.kg#...).
- 9.17. Для соблюдения п. 9.10., необходимо изменить хост основной платежной ссылки на payqr.kg. Например: Элкарт Мобайл: [elqr-mobile://](https://payqr.kg#...), АБ24: [elqr-ab://](https://payqr.kg#...), МBank: [elqr-mbank://](https://payqr.kg#...)
- 9.18. Полное описание Спецификации по QR-кодам содержится в Приложении 1 к настоящему Техническому регламенту.
- 9.19. При вызове [elqr-bank-deep-link://payqr.kg#hash](https://payqr.kg#...) данные в хеше должны дешифроваться корректно и открывать окно перевода через Систему ООВ.
- 9.20. На сайте payqr.kg расположены иконки приложений, поддерживающих открытие ссылок, где пользователи могут выбрать приложение для оплаты.
- 9.21. Требуется добавить функцию вставки платежной ссылки вместо сканирования QR-кода.

¹ Признак М – обязательный, О – необязательный, С – зависит от других условий

- 9.22. В приложениях на базе любой операционной системы необходимо настроить связь с доменом <https://pay.payqr.kg> для автоматического запуска приложения.
- 9.23. Аналогичная связь должна быть (если применимо) настроена между мобильным приложением и собственным сайтом владельца приложения.
- 9.24. Приложение, на которое можно перейти по URI, должны быть готовы к обработке фрагментной части QR-кода (платежной ссылки).
- 9.25. На всех стадиях совершения платежа, плательщику должны быть отображены все детали выбранных (в том числе автоматически используя платежную ссылку) и заполненных полей. Например:
- название поставщика услуг;
 - лицевой счёт;
 - сумма;
 - дополнительные поля.

9.26. Требования для добавления в реестр (<https://payqr.kg>)

Должна быть заполнена заявка на добавление в реестр (сайт), содержащая:

- Иконку размером 128x128 в формате PNG или SVG;
- Название для отображения на сайте (до 50 символов);
- Акты тестирования.

9.27. Порядок размещения на сайте

- 15.13.1. Структура и порядок расположения на сайте фиксированы и не подлежат изменениям.
- 15.13.2. Иконки приложений расположены:
В сетке 4x5 на стандартных смартфонах;
В сетке 5x5 на больших экранах;
На экранах менее 360px — в сетке 3x4.

9.28. Иконки приложений расположены слева направо и сверху вниз в порядке добавления.

9.29. Уникальная схема приложения

- Каждое приложение имеет уникальную схему, которая должна:
быть не более 50 символов;
содержать только латинские буквы в нижнем регистре, цифры и дефис (-);
начинаться с `elqr-`;
быть единой для платформ iOS и Android.

9.30. Каждая схема закрепляется за приложением в базе ООВ и не может использоваться другим приложением.

9.31. Окно вставки ссылки в приложении

- Реализация окна вставки ссылки остается на усмотрение дизайна и функционала приложения.
- Интерфейс приложения должен поддерживать вставку ссылки из буфера обмена.
- Ссылка из буфера обмена может быть любой схемы или хоста.

9.32. Требования к ссылке

- При генерации ссылки не допускается использование специальных символов разметки сообщений (например, «*», «_», «'», «`», «~»).

9.33. Исключение из реестра и восстановление

- ЗАО «МПП» оставляет за собой право скрыть иконку приложения с сайта и приостановить переходы по ссылкам в следующих случаях:
 - Приложение неоднократно не выполняет требования, указанные в данном документе, или не соблюдает технические условия.

- В случае выявления некорректной работы приложения, затрудняющей пользователям проведение платежей через ELQR.
- В случае, если Участник нарушает обязательства по своевременной подаче актуальной информации.
- Восстановление доступа осуществляется по запросу участника после устранения причин, вызвавших исключение.
- Для восстановления доступа участник должен пройти повторное тестирование, подтвердив соответствие требованиям ЗАО «МПЦ».

10. ТРЕБОВАНИЯ К ЧЕКУ И СТАТУСАМ ПЛАТЕЖЕЙ ПО QR

10.1. Участники должны использовать стандартизированные статусы платежей для унифицированного отображения и обработки плательщикам/получателям.

10.2. Обязательный единый перечень статусов для отображения плательщикам/отправителям в чеке платежного приложения включает:

- «В обработке» - платёж инициирован, но ещё не завершён. Ожидается подтверждение;
- «Успешно» - финальный статус, присвоенный Участником-получателем, переданный в ООВ, далее Участнику-отправителю для отображения плательщику/получателю об успешности платежа в платежном приложении;
- «Ошибка» - финальный статус, присвоенный Участником-получателем, переданный в ООВ, далее Участнику-отправителю для отображения плательщику/получателю о неуспешности платежа в платёжном приложении.

10.3. Финальный статус для плательщика должен быть отображен исключительно после получения подтверждения от ООВ.

10.4. В чеке платёжного приложения для плательщиков/получателей должен быть отображен transaction_ID из Системы ООВ.

Спецификация платежного QR-кода Основного оператора взаимодействия

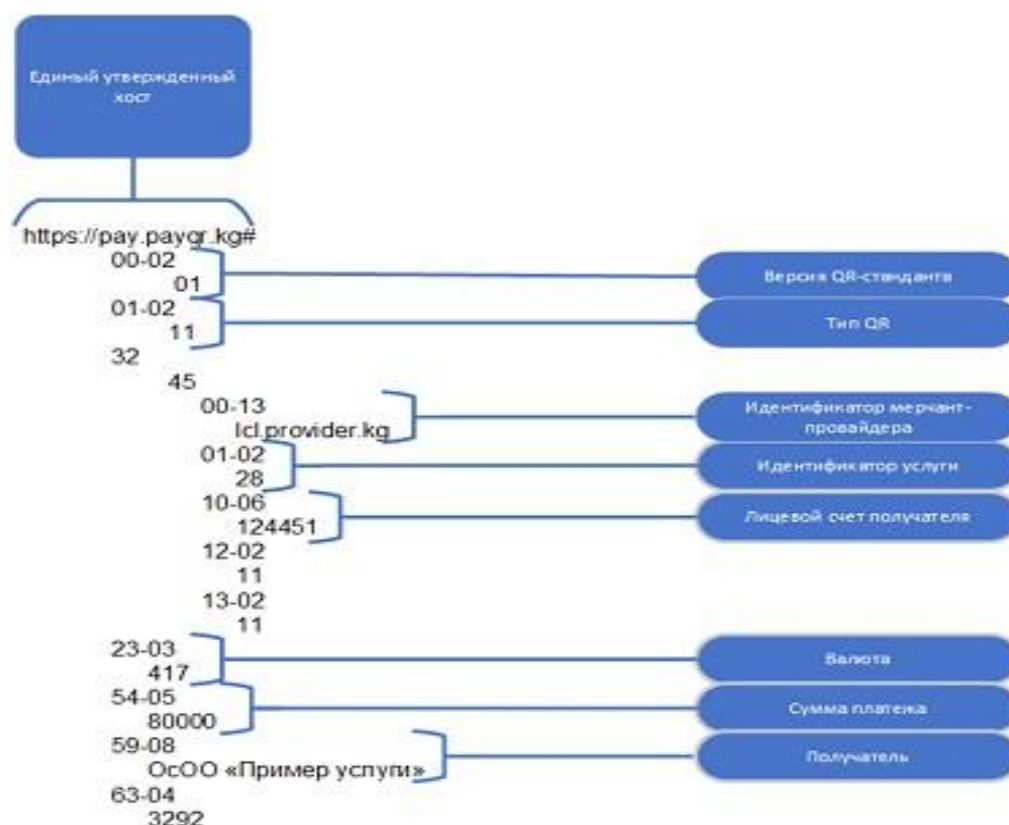
1. Описание принципа работы

1.1. Спецификация платежного QR-кода Основного оператора взаимодействия разработана в соответствии с Стандартом.

1.2. QR-код, использующийся для совершения платежей в рамках данной спецификации, содержит платежную ссылку, которая представляет собой URI (Uniform Resource Identifier) — унифицированный (единообразный) идентификатор ресурса), и имеет вид: схема://хост провайдера платежей#фрагмент, где:

- имя схемы по умолчанию содержит `https` (имя схемы может быть любым);
- имя хоста провайдера платежей по умолчанию содержит `payqr.kg23` (имя хоста провайдера платежей может быть любым), но для создания единой поддержки всеми Участникам необходимо использовать один утвержденный домен.
- фрагмент содержит детали платежа.

2. Схема данных платежной ссылки/QR-кода



3. Структура данных фрагмента URI - деталей платежа.

1.3. Данные деталей платежа организованы в виде последовательности объектов. Объект содержит идентификатор (ID), длину и данные о платеже:

- ID закодирован двумя цифрами в диапазоне от “00” до “99”;

²³ Если у платящего нет приложения, которое умеет обрабатывать фрагментную часть ссылки (детали платежа), то он будет перенаправлен на хост провайдера платежей (по умолчанию на `https://pay.payqr.kg`), где ему будет предоставлен канал оплаты по QR-коду или предложен список приложений, которые могут осуществлять обработку фрагментной части ссылки.

- длина так же закодирована двумя цифрами в диапазоне от “01” до “99”;
- данные представлены последовательностью символов, минимальная последовательность равна одному символу, максимальная – 99 символов.

1.4. Данные деталей платежа имеют древовидную структуру. Начиная от корневого объекта, данные могут содержать примитивные объекты (элементы) или шаблоны. Шаблоны могут включать в себя другие шаблоны или примитивные объекты.

Пример:

→ Корневой объект:

- Примитивный объект;
- Шаблон;
- Примитивный объект;
- Шаблон;

1.4.1. Объекты.

Объекты, которые должны обязательно присутствовать в деталях платежа, обозначены символом “М”, если присутствие объекта в коде зависит от неких условий, то такие объекты помечены символом “С”, все необязательные объекты помечены символом “О”.

1.4.2. Идентификатор - ID.

Идентификатор кодируется двумя цифрами в диапазоне от “00” до “99”.

1.4.3. Длина.

Представлена двумя цифрами в диапазоне от “01” до “99” и должна равняться длине поля данных.

1.4.4. Данные.

Данные могут быть:

- цифровыми (N);
- алфавитно-цифровыми с ограниченным набором символов (ans);
- строковыми (S). Цифровые данные – это подмножество алфавитно-цифровых с ограниченным набором символов, а алфавитно-цифровые – это подмножество строковых.

1.4.5. Организация данных.

Данные для формирования деталей платежа должны начинаться корневым элементом (корневые объекты) с идентификатором “00” и заканчиваться элементом с идентификатором “63”.

1.4.6. Используемые символы.

В случае, если во фрагменте используются символы выходящие за пределы кодировки ASCII, а именно:

":", "/", "?", "#", "[", "]", "@", "!", "\$", "&", "", " ", "(", ")", "*", "+", ",", ";", "=", ALPHA, DIGIT, HEXDIG, "-", ".", "_", "~", где:

- ALPHA - любая буква верхнего и нижнего регистров кодировки ASCII (в regExp [A-Za-z])
- DIGIT - любая цифра (в regExp [0-9])
- HEXDIG - шестнадцатеричная цифра (в regExp [0-9A-F])

Используется механизм т.н. "Процентного кодирования". Перечисленные выше символы не участвуют в процентном кодировании. Процентно-кодированный символ представляет из себя символьный триплет, состоящий из знака "%" и следующих за ним двух шестнадцатеричных чисел: Т.о., %20, например, означает пробел.

1.4.7. Корневые элементы.

Перечень корневых объектов:

Наименование	ID	Формат	Длина	Признак	Комментарий
Версия стандарта	00	N	«02»	M	
Тип платежной ссылки	01	N	«02»	M	
Информация о поставщике услуг, услуге и т.д.	02 – 51	ans	до «99»	M	
МСС - код производителя услуг	52	N	«04»	M	
Код валюты	53	N	«03»	M	по умолчанию 417
Сумма платежа	54	N	до «13»	C	
Наименование поставщика услуг (латиницей)	59	ans	до «25»	M	
Контрольная сумма данных	63	ans	«04»	M	

ID «00» - Версия стандарта – объект обязательный.

Данное поле должно быть первым и содержать значение «01».

ID «01» - Тип платежной ссылки – объект обязательный.

Если присутствует, то должен содержать значения:

11 – если детали платежа используется для совершения более чем одной транзакции, статические коды, обычно с оплатой, где сумму может вводить сам покупатель, например для использования в такси, уличной торговле и других точках с невысокой скоростью обслуживания покупателей;

12 – если для каждой транзакции необходимы новые детали платежа, динамические детали платежа, которые могут использоваться в интернет-магазинах, объектами общепита.

IDs «02» до «51» - Информация об оплачиваемой услуге, поставщике услуг – объект обязательный.

Структура поля содержит элементы шаблона информации об оплачиваемой услуге.

Элемент с идентификатором «32», обязательный для указания, содержит код услуги в Платежном шлюзе, идентификатор плательщика в пределах услуги в системе поставщика услуг (номер телефона, номер заказа, номер договора и т.д.)

Элементы с идентификаторами от «35» до «39» содержат набор доп. полей платежа.

ID «32» - Объект с информацией об оплачиваемой услуге, для всех поставщиков услуг – объект обязательный.

Наименование	ID	Формат	Длина	Признак	Комментарий
Уникальный идентификатор	00	ans	до «32»	M	Объект по умолчанию содержит elcart.kg

Спецификация платежной сети	01	N	до 10	C	Код услуги в Платежном шлюзе
Уникальный идентификатор плательщика в пределах услуги	10	S	До 32	O	Уникальный идентификатор плательщика в пределах услуги в ИС поставщика услуг
Идентификатор транзакции	11	S	До 32	C	Идентификатор транзакции в ИС Поставщика
Возможность редактирования суммы к оплате	12	N	2	C	11 - разрешить плательщику изменять сумму, переданную в объекте 54. 12 – не разрешить плательщику изменять сумму, переданную в объекте 54. По умолчанию плательщику редактирование суммы разрешено. Приоритетной возможностью редактирования суммы является опция, указанная поставщиком услуг.
Возможность редактирования идентификатора плательщика (ID - 10) к оплате	13	N	2	C	11 - разрешить плательщику изменять значение, переданное в объекте - 10 12 – не разрешить плательщику изменять значение, переданное в объекте 10. По умолчанию плательщику редактирование разрешено.

Если объект «10» пустой и объект «13» равен 12, то необходимо скрыть поле ввода уникального идентификатора плательщика.

Если объект «01» пустой, то должен быть заполнен ID «33» объект «00».

ID “33” - Объект с дополнительной информацией о платеже.

Наименование	ID	Формат	Длина	Признак	Комментарий
Уникальный идентификатор ТСП	00	ans	до “32”	C	
Наименование услуги	01	ans	до “32”	O	

ID “34” - Объект с комментарием к платежу.

Содержит комментарий к платежу.

IDs “35”-“39” - Объект с доп. полями Поставщика услуг. Объект не обязательный

Содержит последовательность, начинается с идентификатора «00» и заканчивается идентификатором «99». Если нужное количество доп. полей не вмещается в первый объект, необходимо использовать следующий, по порядку («35», «36», ..., «39»)

Значение каждого доп. поля содержит строку в следующем формате, с уникальным разделителем «:»:

Наименование	Комментарий
key	Идентификатор поля в ИС Поставщика услуги
label	Название поля
value	Значение поля
title	Значение поля, выводимое пользователю
visible_state	«11» - отображается пользователю; «12» - не отображается пользователю

Признак «visible_state» указывает нужно ли отображать данное поле пользователю в интерфейсе. Как правило, данные доп. поля следует отправлять в используемый Платежный Шлюз, согласно его протоколу взаимодействия.

Если «visible_state» имеет признак «11», заполнено поле «value», то в интерфейсе, пользователю, необходимо вывести значение из поля «title».

ID “52” - MCC - код производителя услуг

Категория торговца (MCC) коды определены в ISO 18245.

ID “53” - Код валюты – объект обязательный.

Код валюты (ISO 4217) и должен содержать 3-х значный код валюты. По умолчанию необходимо использовать 417 – кыргызский сом.

ID “54” - Сумма платежа – объект не обязательный, условный.

Используется Поставщиком услуг при генерации деталей платежа.

Если присутствует, то должен содержать значение отличное от нуля. Поле содержит цифры от “0” до “9” и указывается в тыйнах.

Если поле отсутствует, то покупатель в приложении должен задать сумму, которую он платит Поставщику услуг.

ID “59” - Наименование поставщика услуг (латиницей)

Наименование продавца (производителя услуг).

ID “63” - Контрольная сумма - объект обязательный.

Контрольная сумма данных, используется для проверки целостности данных, указанных в деталях платежа.

Алгоритм формирования:

- > Все значения деталей платежа до объекта 63 (ID “00” – “90”, за исключением ID 63) преобразуются в одну строку.
- > Строка данных переводится в массив байт с кодировкой UTF-8.
- > Вычисляется хеш массива, используя алгоритм SHA256.
- > Массив байт преобразуется в строку.
- > Удаляются все символы “-”, если они есть.
- > Из строки берутся последние 4 символа.

1.5. Использование данных из платежной ссылки для осуществления информационного взаимодействия.

При генерации динамической платежной ссылки, Поставщиком услуги, необходимо использовать код услуги в Платежном шлюзе, для корректной обработки деталей платежа.

1.6. Дополнительное использование платежной ссылки

Платежная ссылка, которая используется для формирования QR-кода, может передаваться плательщикам дополнительными следующими способами:

- генерация на сайте (мобильным приложением) поставщика услуг (в том числе в виде URI-кнопки);
- push-уведомление в приложении;

- sms-уведомление;
 - мессенджеры (в том числе в виде URI-кнопки).
 - e-mail;
 - NFC/метка - передача приложением на смартфоне поставщика услуг на смартфон плательщика, или считывание смартфоном плательщика URI, записанный на пассивной NFC-метке поставщика услуг).
- другое.