**Функциональные и нефункциональные требования для процесса оплаты картой**

Оглавление

[Описание процесса оплаты товара пластиковой картой 2](#_Toc198252493)

[Термины и сокращения 3](#_Toc198252494)

[Предварительные договоренности 3](#_Toc198252495)

[**Функциональные требования** 4](#_Toc198252496)

[**Нефункциональные требования** 7](#_Toc198252497)

# **Описание процесса оплаты товара пластиковой картой**

**(покупка товара с использованием платежного терминала или оплатой через сайт компании)**

#### Инициация платежа

* + Клиент выбирает товар и способ оплаты (или через платежный терминал\кассу самообслуживания в магазине или через сайт компании)
  + Вводит данные банковской карты на сайте или прикладывает пластиковую карту к терминалу оплаты

#### Первичная обработка платежа

* + Первичная проверка корректности данных карты
  + Передача данных о транзакции в **платежный шлюз**
  + Шифрование информации через защищенное SSL-соединение

#### Маршрутизация транзакции

* + Платежный шлюз направляет информацию в **банк эквайер**
  + После проверки банком эквайером данных, сведения направляются в **процессинговый центр (на картинке МПС)**
  + Центр идентифицирует **банк-эмитент** и платежную систему (Visa/MasterCard/Мир). Для нынешних реалий возьмем Национальная система платёжных карт (НСПК)

#### Аутентификация и авторизация

* + **Банк-эмитент** проверяет:
    - Подлинность карты
    - Наличие средств на счете
    - Корректность CVV/3D Secure кода
    - Корректность СМС кода для транзакции
  + Проверка транзакции на риски мошенничества

#### Подтверждение транзакции

* + **Банк-эмитент** принимает решение о проведении платежа
  + Отправка ответа через **процессинговый центр**
  + Блокировка суммы на счете клиента (заморозка суммы до списания ее со счета клиента)

#### Финализация платежа

* + Списание средств со счета клиента
  + Зачисление средств на счет продавца
  + Генерация электронной квитанции

# **Термины и сокращения**

В рамках документа приняты следующие термины и их определения.

|  |  |
| --- | --- |
| **Термин** | **Определение** |
| POS-терминал | Устройство для приема безналичных платежей с банковских карт непосредственно в точках продаж. |
| Банк-эквайер | Финансовое учреждение, занимающееся организацией точек приёма пластиковых банковских карт с помощью банкоматов и терминалов. Поставщик услуги эквайринга. |
| Банк-эмитент | Участник платежной системы, который осуществляет выпуск и обслуживание банковских карт. |
| Клиент | Приобретатель услуги эквайринга. |
| Покупатель | Человек, совершающий покупку через платежный терминал, кассу самообслуживания в магазине или через сайт компании. |
| Продавец | Юридическое лицо, предоставляющий товар или услуги для приобретения. |
| Транзакция | Операция, связанная с движением денежных средств на банковском счете. |

# **Предварительные договоренности**

* + - 1. Мы – ИТ команда банка;
      2. Наш банк – эквайер;
      3. У нас свой собственный уже разработанный платежный шлюз;
      4. Мы можем быть банком эмитентом;
      5. Реализуем систему с нуля;
      6. Процессинговый центр = платежная система;
      7. Платежная система – Мир;
      8. Степень детализации – только прямое взаимодействие, без мелких деталей.

# **Функциональные требования**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Функция** | **Описание** | **Критерии приемки** |
| *Оплата на сайте* | | | |
| ФТ-1 | Ввод данных пластиковой карты | Система должна позволять заполнять по шаблону данные о платежной карте на сайте | Передача данных с формы на дальнейшую проверку |
| ФТ-2 | Двухфакторная  аутентификация | Система должна предусматривать двухфакторную аутентификацию пользователя с использованием СМС-кода для проведения оплаты | 1. Пользователь получает статус по итогам двухфакторной авторизации;  2. Передача данных в платежный шлюз. |
| *Оплата через платежный терминал* | | | |
| ФТ-3 | Прием данных с платежного терминала | Система должна принимать данные о транзакции с POS-терминалов | Передача данных в платежный шлюз |
| *Требования, не зависящие от способа оплаты* | | | |
| ФТ-4 | Проверка данных в платежном шлюзе | Система в качестве платежного шлюза должна проверять правильность формата номера карты, срока действия, соответствие CVC-кода:   * Номер карты соответствует Luhn-алгоритму; * Срок действия карты не истек; * Формат CVC-кода соответствует стандарту банка-эмитента. | А. Передача данных на шифрование  Б. В случае некорректных данных система логирует ошибку с указанием причины и возвращает ответ в интерфейс покупателя |
| ФТ-5 | Шифрование данных в платежном шлюзе | Система должна шифровать все передаваемые данные о транзакции с использованием протокола TLS версии 1.2 или выше | Передача транзакции в банк-эквайер |
| ФТ-6 | Проверка корректности и передача транзакции в процессинговый центр | Система должна проверять корректность транзакции, шифровать данные и передавать транзакцию в процессинговый центр (НСПК) | Передача зашифрованных данных в процессинговый центр |
| ФТ-7 | Проверка подлинности карты как банк-эмитент | В качестве банка-эмитента система должна принимать информацию о платеже из процессингового центра и проверять наличие карты в реестре и её статус | Передача данных на проверку корректности CVV/ 3D Secure/ СМС-кода |
| ФТ-8 | Проверка корректности CVV/ 3D Secure/ СМС-кода | В качестве банка-эмитента система должна проверять корректность введенного CVV/ 3D Secure/ СМС- кода | Передача данных на проверку легитимности |
| ФТ-9 | Проверка на легитимность транзакции | В качестве банка-эмитента система должна осуществить поиск счета в листах блокировки, проверить на предмет ареста счета | Передача данных на проверку рисков мошенничества |
| ФТ-10 | Проверка транзакции на риски мошенничества | В качестве банка-эмитента система проверяет транзакцию на признаки мошеннических действий | Транзакция передана на проверку наличия средств на счете |
| ФТ-11 | Проверка наличия средств на счете | В качестве банка-эмитента система должна проверять карту на наличие средств на счете, достаточных для оплаты покупки | А. Если баланс счета превышает сумму покупки, данные передаются для авторизации транзакции;  Б. Если средств на счете недостаточно, система отправляет Push-уведомление об этом в мобильный банк;  Б.1. Система возвращает сообщение о нехватке средств на платежный терминал или форму на сайте. |
| ФТ-12 | Авторизация транзакции | В качестве банка-эмитента система проставляет отметку об авторизации платежа | Отправка ответа через процессинговый центр |
| ФТ-13 | Заморозка суммы на счете покупателя | Система должна выполнять временную блокировку денежных средств на счете клиента в размере суммы платежа до завершения транзакции | Общий баланс счета покупателя уменьшен на сумму платежа |
| ФТ-14 | Уведомление покупателя о статусе транзакции | Система должна направлять в POS-терминал или форму на сайте уведомления о результатах выполнения транзакции | А. В случае успешного прохождения проверок и подтверждения транзакции POS-терминал или форма на сайте продавца выводит информацию об одобрении транзакции;  Б. В случае непрохождения проверки на любом из этапов, POS-терминал или форма на сайте продавца выводит информацию об отклонении транзакции с кратким указанием причины. |
| ФТ-15 | Перевод средств со счета клиента на счет продавца | Система должна обеспечить перевод средств в размере платежа со счета покупателя на счет продавца сроком не позднее двух рабочих дней, в случае межбанковских операций, и в течение одного рабочего дня, если операции проводятся внутри одного банка | Средства зачислены на счет продавца |
| Ф-16 | Создание и отправка квитанции | Система должна генерировать электронную квитанцию после завершения платежа. | Клиент получает электронную квитанцию на указанный адрес электронной почты, а также может получить её в приложении мобильного банка |
| Ф-17 | Обработка возвратов и споров | Система должна поддерживать процесс возврата средств и разрешения споров по транзакциям. | Клиент может инициировать возврат, система обрабатывает запрос и уведомляет о результате. |

# **Нефункциональные требования**

|  |  |  |
| --- | --- | --- |
| **№** | **Тип НФТ** | **Описание** |
| НФ-1 | Безопасность | Точность выявления подозрительных операций должна быть не менее 95%. |
| НФ-2 | Безопасность | Система должна осуществлять постоянный мониторинг сетевой активности и выявлять потенциальные угрозы безопасности. |
| НФ-3 | Надежность | Резервные копии должны создаваться каждый час и храниться в защищенном месте. |
| НФ-4 | Производительность | Время отклика от шлюза должно составлять менее 500 мс. |
| НФ-5 | Производительность | Время на обработку одной транзакции (с момента инициации платежа до генерализации квитанций) не должно превышать 1 календарного дня. |
| НФ-6 | Удобство использования | Интерфейс должен быть адаптивным и поддерживать различные устройства (смартфоны, планшеты, компьютеры). |
| НФ-7 | Отчетность | Все действия в системе должны логироваться. |
| НФ-8 | Отчетность | Журнал транзакций должен содержать все необходимые данные (номер карты, сумма, дата, время, статус и т.д.). Данные должны быть доступны для анализа и аудита в течение 5 лет. |
| НФ-9 | Отчетность | Система должна генерировать отчеты по запросу, содержащие информацию о количестве транзакций, суммах, времени обработки транзакции и других ключевых показателях. Время генерации отчета не должно превышать 10 минут. |
| НФ-10 | Отказоустойчивость | Механизм резервирования должен обеспечивать работу даже при временных сбоях связи, при этом время отклика на передачу данных не превышает 500 мс. |
| НФ-11 | Доступность | Система должна работать 24/7 с уровнем доступности не менее 99,9%. |
| НФ-12 | Масштабируемость | Система должна обрабатывать до 1000 транзакций в секунду без снижения производительности. |