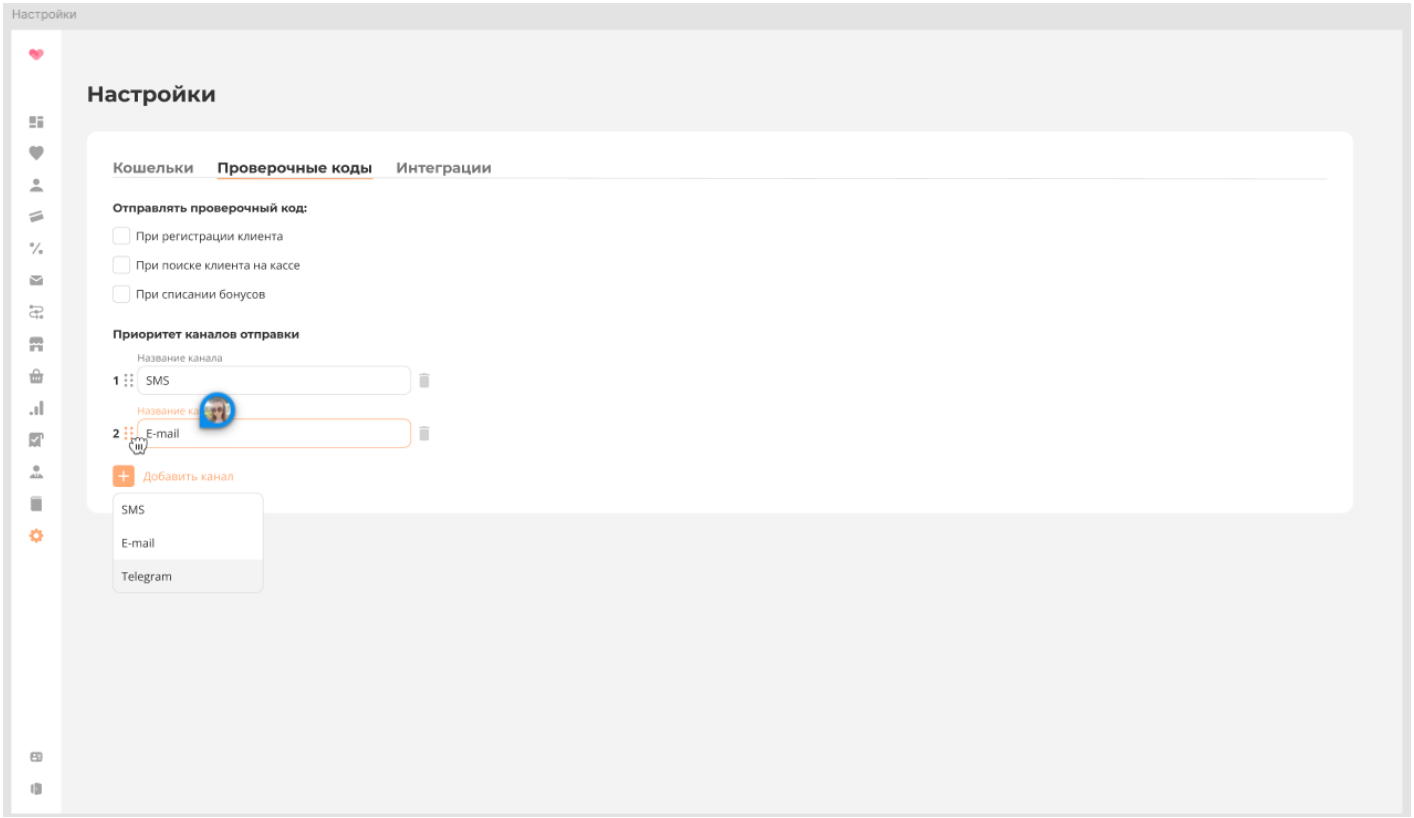
Двухфакторная авторизация операций

Описание механизма

Методы использующие двухфакторное подтверждение операций отмечены в документации красным тэгом `2FA`.

В качестве второго фактора выступает фактор владения покупателем частного ресурса(телефон, почта). Настройка 2FA выполняется в личном кабинете и состоит из двух частей:

- Галка для событий, при которых необходимо выполнить проверку второго фактора
- Список каналов которыми будет доставлен код подтверждения фактора
- В карточке магазина признак отключения проверки фактора, который совсем отключает механизм в конкретных магазинах



Каждое событие проверяется отдельно. Попытка отправки кода выполняется через канал в порядке указания его в списке каналов, в зависимости от наличия канала в конкретном

запросе или в профиле клиента.

> **Пример:** Установлена настройка проверки фактора владения при регистрации клиента. Порядок каналов отправки: Телефон -> Почта. В запросе регистрации телефон не передан, но есть адрес электронной почты. При таких вводных отправка кода будет выполняться на почту, т.к. определить телефон не представляется возможным. При тех же настройках и выполнении запроса идентификации клиента, если в карточке клиента есть телефон, отправка произойдет на телефон, как более приоритетный канал отправки.

Описание протокола

Протокол построен на сессионной модели. Любой защищенный запрос(запрос требующий 2FA) при установленной настройке для соответствующей операции будет начинать сессию работы с пользователем в определенном магазине.

Если для защищенного метода установлена настройка и список каналов отправки не пустой, выполняется проверки:

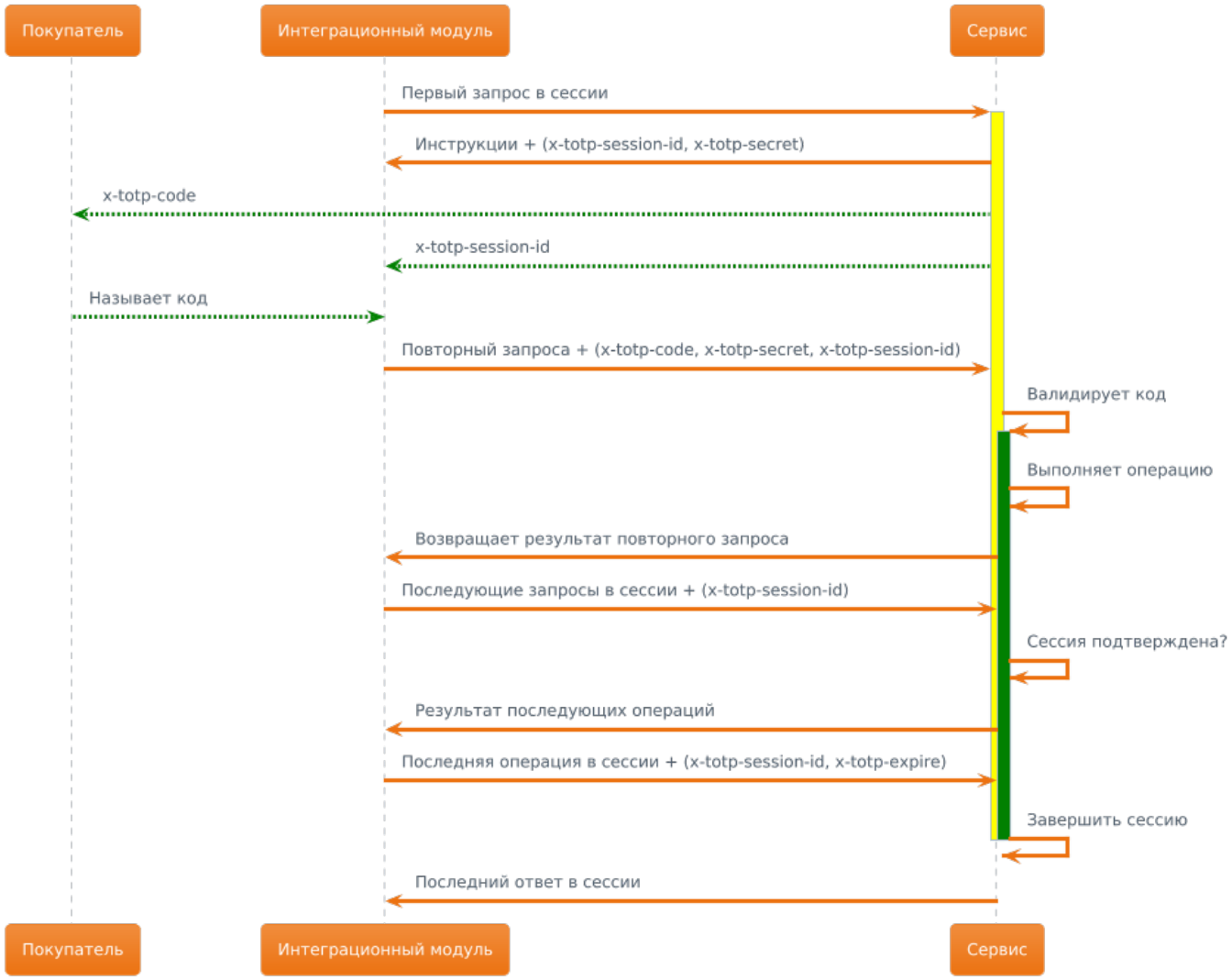
- Этот вызов является началом или продолжением сессии? Проверка выполняется по наличию специального заголовка `x-totp-session-id`.
- Если передан заголовок `x-totp-channel`, попытка отправки кода будет выполняться на этот канал
- Если заголовок `x-totp-session-id` не передан, начинается новая сессия, сервис генерирует и отправляет на первый доступный канал отправки временный код подтверждения фактора владения и отвечает специальными инструкциями для клиентского приложения:

```
{
  "success": true,
  "message": "OK",
  "data": {
    "session": {
      "id": "081ff88e5d1f925d33926fb0f580e49485fd231b", // Идентификатор сессии
      "issuer": "79030000001",
      "issuer_location": "",
      "confirmed": false,
      "created_at": null,
      "updated_at": null
    },
    "instruction": {
```

```
      "channel": "phone", // Канал, на который выполнилась отправка кода подтверждения
      "reciever": "79030000001", // Идентификатор получателя(зависит от канала)
      "secret": "dummy-secret", // Секрет клиентского приложения, используется для проверки
введенного кода подтверждения
      "duration": 120, // Время жизни кода подтверждения в секундах
      "available_channels": [ // Доступные в текущем контексте каналы отправки кодов
подтверждения
        "phone"
      ]
    }
  }
}
```

- Если заголовок `x-totp-session-id` передан, считается, что это очередной вызов в рамках начатой ранее сессии
  - В таком случае выполняется проверка подтверждения фактора владения(было ли подтверждение) в рамках сессии.
    - Если сессия не была подтверждена ранее, выполняется проверка заголовков `x-totp-code` и `x-totp-secret`, если проверка прошла успешно - код верный, сессия помечается как подтвержденная и защищенный запрос возвращает свое тело ответа(зависит от конкретного запроса)
    - Если сессия уже была подтверждена - запрос просто возвращает свое тело ответа
- Клиентское приложение может завершить сессию любым запросом в сессии с передачей заголовка `x-totp-expire`.

Таким образом начинаться сессия может любым методом, подтверждаться любым методом, любой метод в цепочке вызовов после подтверждения больше не требует подтверждения.



Описание развертывания

Сервис использует переменные окружения связанные с отправкой SMS4B. Также используются две переменные окружения:

TOTP_SESSION_TTL_MIN

Время жизни сессии подтвержденной сессии в минутах. Не менее 10 минут, если указано значение меньше - сессия будет жить 10 минут. Значение по-умолчанию: 10 минут.

TOTP_SESSION_VACUUM_INTERVAL_MIN

Интервал, с которым сервис выполняет очистку просроченных сессий. Не менее 10 минут, если указано значение меньше - сессия будет жить 10 минут. Значение по-умолчанию: 10 минут.

Revision #3
Created 3 March 2025 10:19:35 by Морозов Сергей
Updated 10 March 2025 08:03:05 by Алексей Нам