Руководство администратора
Модуля СБП

Email: info@payneteasy.ru
Телефон: +7 499 288 22 16

ОГЛАВЛЕНИЕ

Email: info@payneteasy.ru
Телефон: +7 499 288 22 16

1. ПРЕАМБУЛА

Настоящее руководство описывает функциональные возможности управления Личными кабинетами для роли администратора участника СБП.

2. ТЕРМИНОЛОГИЯ

- **Система быстрых платежей (также «СБП»)** - система быстрых платежей платежной системы Центрального Банка России, позволяющая физическим лицам мгновенно (в режиме 24 часа в сутки/7 дней в неделю) переводить денежные средства по номеру мобильного телефона себе или другим физическим лицам вне зависимости от обслуживающего их банка – участника Системы быстрых платежей.
- **SSO (англ. Single Sign-On)** — технология “единого входа”, при использовании которой пользователь переходит из одной системы в другую, не связанную с первой, без повторной аутентификации.
- **Модуль СБП** – программное обеспечение, представляющее собой систему обработки информации о платежах, предназначенное для проведения Транзакций в СБП, автоматизированного взаимодействия с АБС в соответствии со стандартами ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012, исключительные права на которую принадлежат ООО "Гуд Айдиа Технолоджис" (ОГРН: 1077746701053, ИНН: 7734559885) и зарегистрированы Федеральной службой по интеллектуальной собственности за номером 2023683014 от 01.11.2023.
- **Личный кабинет** – персонифицированный раздел (учетная запись) Модуля СБП, доступ в который возможен путем использования специальных идентификационных данных сотрудника участника СБП (уникальной пары логин/пароль), посредством использования которого осуществляется персонифицированное взаимодействие с Модулем СБП;
- **Автоматизированная Банковская Система (далее – «АБС»)** – программное обеспечение банка, осуществляющее регистрацию и учет банковских операций на основе информации, поступающей от Модуля СБП.
- **Торгово-сервисное предприятие (далее – «ТСП»)** – магазин Клиента, который может быть представлен как витриной интернет-магазина, так и розничной точкой продаж, осуществляющий продажу товаров, работ и (или) услуг под определенным брендом. Как правило, одному Клиенту соответствует один ТСП.
- **Клиент** – юридические лица (коммерческие и некоммерческие организации, местом государственной регистрации которых является Российская Федерация), индивидуальные предприниматели, а также зарегистрированные на территории

Email: info@payneteasy.ru
Телефон: +7 499 288 22 16

Российской Федерации в установленном законом порядке представительства иностранных организаций, осуществляющие прием платежей, либо выплаты через СБП

- **Транзакция** — платежная операция расчета за приобретенные (приобретаемые) товары, работы и (или) услуги, выполняемая с использованием номера телефона, либо QR-кода, финансовая операция по перечислению денежных средств в рамках применяемой формы безналичных расчетов, отмена ранее совершенных операций, а также обмен информацией, производной от данных операций.
- **Инфраструктура** — совокупность технических средств, линий связи, объединенных в пределах одного помещения (центра обработки данных).

3. ЦЕЛЕВАЯ АУДИТОРИЯ

Данное руководство предназначено для администратора Модуля СБП, осуществляющего управлением уровнями доступа к функциональным возможностям системы.

4. СВЕДЕНИЯ О ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

Наименование	Модуль СБП
Версия	1.0
Регистрационный номер Роспатента	2023683014 от 01.11.2023
Дата введения в промышленную эксплуатацию	20.09.2023
Официальный сайт, содержащий документацию и спецификации	https://payneteasy.ru/solutions/sbp

Email: info@payneteasy.ru
Телефон: +7 499 288 22 16

5. СВЕДЕНИЯ О ПРАВООБЛАДАТЕЛЕ

Наименование	Общество с ограниченной ответственностью "Гуд Айдиа Технолоджис" (ОГРН: 1077746701053, ИНН: 7734559885)
Адрес правообладателя	123060, г. Москва, ул. Маршала Соколовского, д. 5, эт. 2, ком. 19б
Сайт правообладателя	https://payneteasy.ru
e-mail службы технической поддержки	it@payneteasy.ru
Дата введения в промышленную эксплуатацию	20.09.2023

6. РЕАЛИЗАЦИЯ ПРОЦЕССА АУТЕНТИФИКАЦИИ

Процесс аутентификации, создания Личных кабинетов и управление полномочиями в рамках выделенных ролей (далее – «управление доступом») построен на микросервисной архитектуре и осуществляется посредством SSO. Управление доступом осуществляется на стороне отдельной системы Superfly, распространяемой с открытым исходным кодом по лицензии Apache 2.0[1].

Наглядно процесс аутентификации и настройки управления доступом представлен на диаграмме ниже.

[1] https://github.com/payneteasy/superfly/blob/master/LICENSE

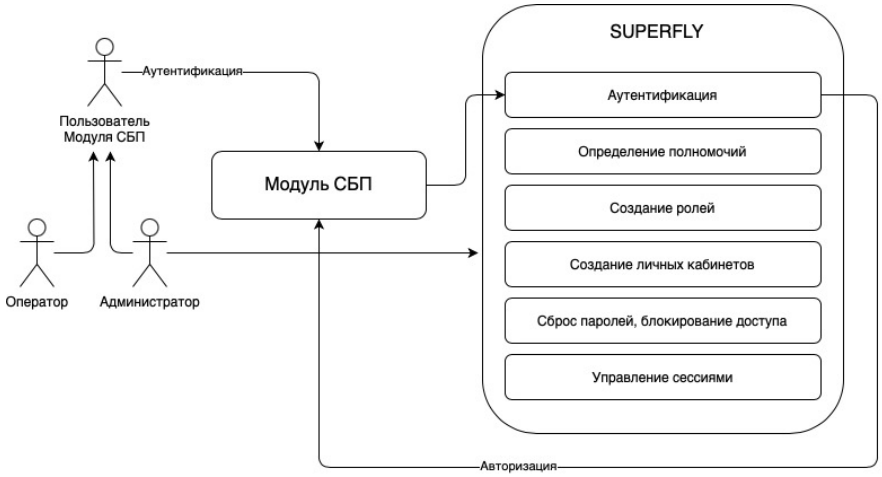

Рисунок 1. Визуализация процесса аутентификации и управления доступом

7. СОЗДАНИЕ ЛИЧНОГО КАБИНЕТА

Ниже будет рассмотрен пошаговый пример создания нового Личного кабинета.

ШАГ ПЕРВЫЙ. ГЕНЕРАЦИЯ КЛЮЧА

Необходимо создать пару открытый/закрытый ключ. Сгенерировать ключ можно штатными средствами операционной системы.

ОПЕРАЦИОННАЯ СИСТЕМА MAC

Стандартный набор OpenSSH включает утилиту ssh-keygen, которая используется для генерации пар ключей. Запустить её можно в терминале при помощи команды:

```
ssh-keygen
```

После этого утилита запросит указать место хранения для ключей. По умолчанию они хранятся в директории ~/.ssh с именами файлов id_rsa для приватных ключей и id_rsa.pub для публичных. Нажмите ENTER, чтобы пропустить этот шаг.

```
Generating public/private rsa key pair.

Enter file in which to save the key (/home/username/.ssh/id_rsa):
```

Внимание! Если пара ключей уже была сгенерирована ранее, может появиться следующее сообщение:

```
/home/username/.ssh/id_rsa already exists.

Overwrite (y/n)?
```

Если вы решите переписать ключ на диске, то уже не сможете использовать старый ключ. Процесс будет необратимым.

Email: info@payneteasy.ru
Телефон: +7 499 288 22 16

После указания места хранения ключа система запросит дополнительный пароль, который зашифрует файл ключа на диске. Оставьте это поле пустым, для этого нажмите ENTER, чтобы пропустить этот шаг.

```
Created directory '/home/username/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

Это был последний шаг. Теперь у вас есть публичный и приватный ключ, которым владеете только вы. Пример итогового сообщения в командной строке вы можете видеть ниже.

```
Your identification has been saved in /home/username/.ssh/id_rsa.
Your public key has been saved in /home/username/.ssh/id_rsa.pub.
The key fingerprint is:
a9:49:EX:AM:PL:E3:3e:a9:de:4e:77:11:58:b6:90:26 username@203.0.113.0
The key's randomart image is:
+--[ RSA 2048]----+
|      ..o        |
|   E o= .        |
|    o. o         |
|        ..       |
|      ..S        |
|     o o.        |
|   =o.+.         |
|. =++..          |
|o=++.            |
+-----------------+
```

Далее вам необходимо открыть сформированный файл с публичным ключом id_rsa.pub и скопировать его содержимое:

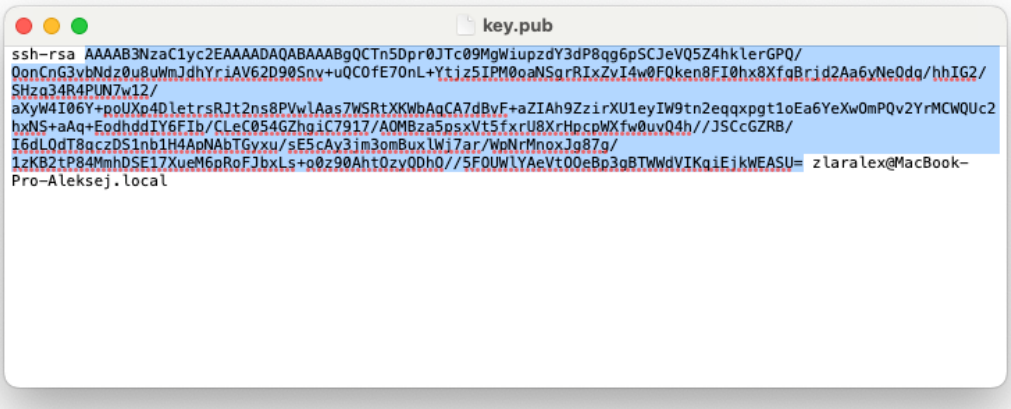

Рисунок 2. Выделенная строка и есть Ваша секретная фраза (Public key)

ШАГ ВТОРОЙ. СОЗДАНИЕ ЛИЧНОГО КАБИНЕТА

Для создания Личного кабинета необходимо воспользоваться пользовательским интерфейсом Superfly.

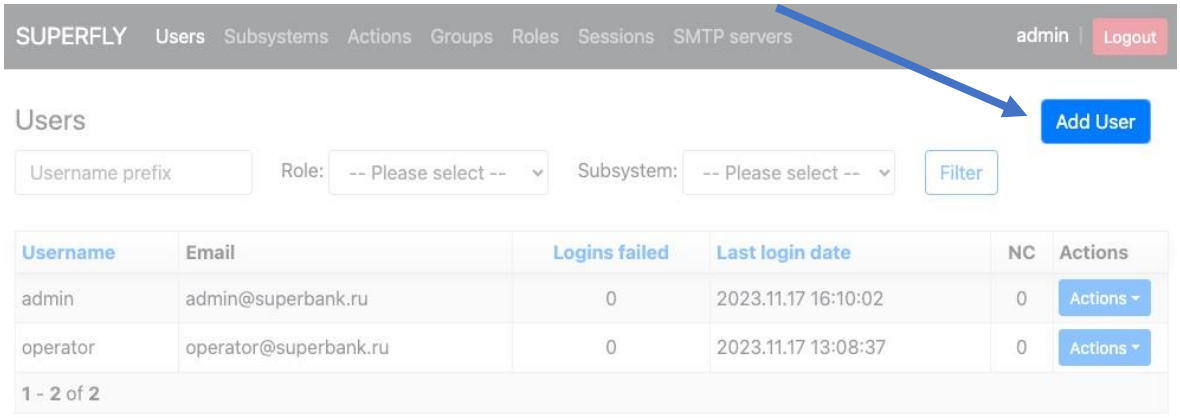

Рисунок 3. Вход в Superfly

Авторизуйтесь в Superfly и нажмите кнопку “Add User”.

После этого откроется форма добавления нового Личного кабинета, которую необходимо будет заполнить данными о новом пользователе. Пример заполнения формы представлен на рисунках на следующей странице.

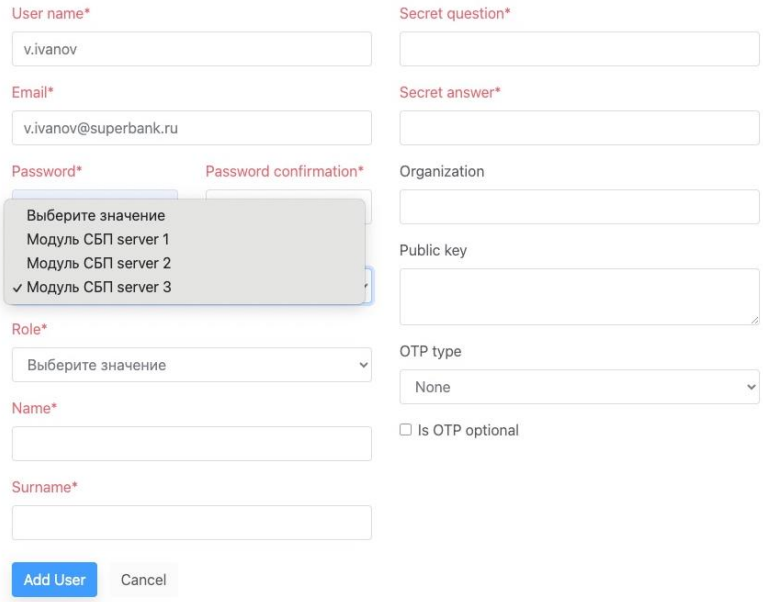

Рисунок 4. Создание Личного кабинета. Выбор системы, в которой создается ЛК

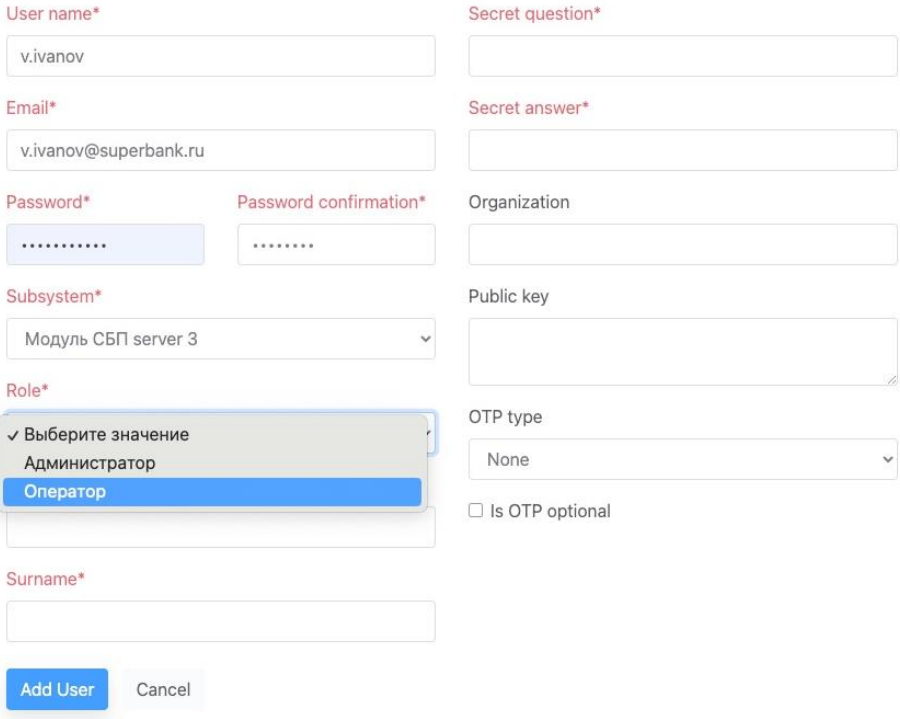

Рисунок 5. Создание Личного кабинета. Выбор системы, к которой предоставляется доступ

В текстовое поле Public key необходимо вставить публичный ключ, который был заранее сгенерирован.

Email: info@payneteasy.ru
Телефон: +7 499 288 22 16

8. РЕГИСТРАЦИЯ КЛЮЧА АУТЕНТИФИКАЦИИ ДЛЯ ОПИСАНИЯ ПРОТОКОЛА ВЗАИМОДЕЙСТВИЯ С ВНЕШНЕЙ ИНФОРМАЦИОННОЙ СИСТЕМОЙ

Для проведения операций по протоколу взаимодействия с внешней информационной средой необходимо задание специального секретного ключа размером 256 бит. Для генерации ключа необходимо создать криптостойкую последовательность размером не менее 256 бит (32 байта). Для этого можно воспользоваться утилитой OpenSSL имеющейся штатно в семействе ОС Linux и MacOS. Чтобы создать ключ длиной 32 байта в кодировке Base64 достаточно воспользоваться следующей командой.

```
openssl rand -base64 32
```

В результате выходная последовательность может выглядеть как

```
BFA4KoR5lRwY29HuoYCs7iF1QQgwIrJR17Yy3B4ntMs=
```

Полученный секретный ключ необходимо передать в службу поддержки, используя безопасный канал, для настройки ПО.