

## Функциональные характеристики и информация необходимая для установки, эксплуатации модуля «Система дистанционного банковского обслуживания - интеграционные компоненты»

### 1.1. Функциональные характеристики 1. Подключение сертификата PayControl

Форм-фактор – desktop, mobile

Точка входа - раздел «Настройки» в кабинете клиента, страница PayControl.

На странице «PayControl» есть возможность выполнить выпуск нового сертификата, обновить или удалить действующий сертификат PayControl.

### Настройки

Безопасность Подписки RuToken **PayControl**

#### Сертификаты Действия

Используется	Идентификатор пользователя	Дата окончания	Иконки
	ismpl-23ff8ac2-6c4b-4808-947b-cbebb160f643	11.01.2020	

  

Приостановлен	Идентификатор пользователя	Дата окончания	Иконки
	ismpl-28ff8jc2-6c4b-4808-947b-cbebb160f4789	11.01.2020	

ФИО владельца ключа	Бочкарев Александр Вениаминович
Идентификатор устройства	dummy
Начало срока действия	11.02.2019
Идентификатор системы	aa6f98c3-2a83-4e51-af2b-343e79ec6537
Идентификатор пользователя	610524
Текст открытого ключа	-

#### Заявки

№	ДАТА	ЗАЯВКА	СТАТУС
125	24.12.2021	Заявление на подключение PayControl	Исполнен ✓
124	15.12.2021	Заявление на подключение PayControl	Исполнен ✓

Рисунок 1- Страница настроек сертификатов PayControl

На странице отображаются все сертификаты PayControl пользователя, а также информация о сертификатах.

Таблица 1- Состав экранной формы

Название блока ЭФ	Доступные контекстные действия	Информация в детализации
Список сертификатов	Перевыпустить сертификат Удалить сертификат	В краткой форме: - Дата окончания - Идентификатор пользователя - Статус  В детализированной форме (при раскрытии элемента списка при нажатии): - ФИО владельца - Идентификатор устройства - Дата выпуска сертификата - Текст открытого ключа
Список заявок на выпуск сертификатов	Печать	В краткой форме: - Номер заявки - Дата заявки - Тип заявки - Статус
Кнопка «Создать сертификат»	Выпустить сертификат	

Вся работа с ключами пользователя происходит после аутентификации в мобильном приложении в фоновом режиме. После регистрации ключа пользователь может использовать сертификат PayControl для подтверждения операций.

При выходе из мобильного приложения происходит удаление установленных ключей пользователя. Мобильное приложение отправляет запрос на удаление на сервер PayControl.

Удаление ключей необходимо для избегания ситуации, когда другой пользователь может воспользоваться установленными на устройстве ключами для подписи документов.

#### 1.2. Порядок действий при подключении пользователя к PayControl:

1. Пользователь открывает страницу настроек
2. Пользователь нажимает кнопку «Создать сертификат» и создает заявку на выпуск сертификата PayControl через web-интерфейс или мобильное приложение.
3. Фронтэнд создает заявку на выпуск сертификата
4. Банк на стороне бэкэнда привязывает сертификат PayControl к учетной записи пользователя в ДБО.
5. Пользователь авторизуется в мобильном приложении банка.
6. Мобильное приложение проверяет наличие сертификата PayControl, выполняя запрос на получение списка сертификатов пользователя.
7. Мобильное приложение выполняет запрос на получение ключевой информации сертификата пользователя.
8. Мобильное приложение регистрирует открытый ключ пользователя.

#### 2. Подтверждение в web-интерфейсе

Форм-фактор – desktop

Точка входа – кнопка «Подписать» на форме создания документа.

Таблица 2- Состав экранных форм

Название ЭФ	Доступные действия	Информация в детализации
Модальное окно с таймером	Отмена Показать QR-код	В модальном окне показывается: - заголовок «Подтверждение операции»; - текст подсказки «Подтвердите операцию через мобильное приложение»; - лоадер – показывает факт активного процесса; - таймер обратного отсчета; - кнопка «Отмена» - при нажатии отменяет подтверждение и закрывает модальное окно; - кнопка «Показать QR-код» - переключает на модальное окно подтверждения по QR-коду; - кнопка с иконкой креста в правом верхнем углу - при нажатии отменяет подтверждение и закрывает модальное окно
Модальное окно успешного подписания	Закреть модальное окно	В модальном окне показывается: - заголовок «Подтверждение операции»; - текст подсказки «Операция подтверждена»; - кнопка «Ок» - при нажатии закрывает модальное окно; - кнопка с иконкой креста в правом верхнем углу - закрывает модальное окно.
Модальное окно в случае неуспешного подтверждения	Отмена Повторить подтверждение	В модальном окне показывается: - заголовок «Подтверждение операции»; - текст подсказки «Операция отменена через мобильное приложение» / «Время подтверждения операции истекло» ; - кнопка «Ок» - при нажатии закрывает модальное окно.

Последовательность действий при подписании:

- 1 Пользователь авторизуется в Интернет-Банке
- 2 Пользователь создает документ
- 3 Пользователь нажимает кнопку подтверждения документа - «Подписать»
- 4 Пользователь выбирает PayControl как способ подтверждения операции
- 5 Отображается модальное окно поверх остальных окон. В модальном окне запускается таймер - 3 минуты, в течении которых пользователь должен подтвердить операцию, иначе она будет отменена
- 6 Пользователь подтверждает операцию в мобильном приложении:
  - а. Пользователь открывает мобильное приложение;

- б. Пользователь открывает список неподтвержденных операций, через значок «колокольчик» на Главной странице;
- с. Пользователь выбирает операцию в списке;
- д. В интерфейсе приложения открывается форма с информацией о подписываемом платежном поручении с возможностью подтвердить подпись.

Пример полей для платежного поручения:

- Тип документа
- ИНН контрагента
- Наименование контрагента
- Назначение платежа
- Сумма

- е. Пользователь нажимает кнопку «Подтвердить»;

6.a Пользователь отменяет операцию, нажав кнопку "Отмена" на модальном окне . После происходит возвращение на форму создания документа.

6.b Пользователь выбирает процесс подтверждения операции по QR-коду, нажимает кнопку «Показать QR-код» (описание процесса в пункте 4).

6.c Фронтэнд отменяет операцию, если в течении времени таймера операция не была подтверждена.

7 Фронтэнд отображает страницу результата подтверждения документ

### 3. Подтверждение в мобильном приложении

Форм-фактор – mobile

Точка входа – кнопка «Подписать» на форме создания документа.

Таблица 3- Состав экранных форм

Название ЭФ	Доступные действия	Информация в детализации
Страница подтверждения	Подтвердить Отмена	Информация об операции Кнопка «Подтвердить» Кнопка «Отмена»
Модальное окно успешного подтверждения	Закрыть страницу	Уведомление об успешном подтверждении Кнопка «Ок»

Действия:

- Подписать документ;
- Отменить транзакцию.

Процесс подписания:

- 1 Пользователь авторизуется в мобильном приложении;
- 2 Пользователь создает документ;
- 3 Пользователь нажимает кнопку подтверждения операции;
- 4 Пользователь выбирает PayControl в списке способов подтверждения;

5 В интерфейсе мобильного приложения открывается форма с информацией о подписываемом платежном поручении с возможностью подтвердить подпись. Пример полей для платежного поручения:

- Тип документа
- ИНН контрагента
- Наименование контрагента
- Назначение платежа
- Сумма

6 Пользователь нажимает кнопку «Подтвердить»;

6.a Пользователь нажимает кнопку «Отменить»;

7 Мобильное приложение отображает страницу результата подтверждения операции.

#### 4. Подтверждение с помощью QR-кода

Форм-фактор – desktop

Точка входа – кнопка «Подписать» на форме создания документа, после нажать «Показать QR-код» в модальном окне.

Таблица 4- Состав экранных форм

Название ЭФ	Доступные действия	Информация в детализации
Модальное окно с таймером	Отмена Показать QR-код	В модальном окне показывается: - заголовок «Подтверждение операции»; - текст подсказки «Подтвердите операцию через мобильное приложение»; - лоадер – показывает факт активного процесса ; - таймер обратного отсчета; - кнопка «Отмена» - при нажатии отменяет подтверждение и закрывает модальное окно; - кнопка «Показать QR-код» - переключает на модальное окно подтверждения по QR-коду; - кнопка «Крест» в правом верхнем углу - при нажатии отменяет подтверждение и закрывает модальное окно.
Модальное окно с QR-кодом	Отмена	В модальном окне показывается: - заголовок «Подтверждение операции»;

		<ul style="list-style-type: none"> <li>- текст подсказки «Подтвердите операцию через QR-код»;</li> <li>- изображение QR-кода;</li> <li>- кнопка «Отмена» - при нажатии отменяет подтверждение и закрывает модальное окно;</li> <li>- поле для ввода пароля.</li> </ul>
Модальное окно успешного подписания	Закреть модальное окно	<p>В модальном окне показывается:</p> <ul style="list-style-type: none"> <li>- заголовок «Подтверждение операции»;</li> <li>- текст подсказки «Операция подтверждена»;</li> <li>- кнопка «Ок» - при нажатии закрывает модальное окно;</li> <li>- кнопка «Крест» в правом верхнем углу - закрывает модальное окно</li> </ul>
Модальное окно в случае неуспешного подтверждения (отмена подтверждения на телефоне, истечение времени подтверждения)	Отмена Повторить подтверждение	<p>В модальном окне показывается:</p> <ul style="list-style-type: none"> <li>- заголовок «Подтверждение операции»;</li> <li>- текст подсказки «Операция отменена через мобильное приложение» / «Время подтверждения операции истекло» ;</li> <li>- кнопка «Ок» - при нажатии закрывает модальное окно.</li> </ul>

Действия:

- Подписать документ;
- Отменить транзакцию.

Процесс подписания:

- 1 Пользователь авторизуется в WEB-интерфейсе Интернет-Банка;
- 2 Пользователь создает документ;
- 3 Пользователь нажимает кнопку подтверждения документа;
- 4 Пользователь выбирает PayControl как способ подтверждения операции;
- 5 Открывается модальное окно подтверждения:

- 6 Отображается модальное окно поверх остальных окон. В модальном окне запускается таймер - 3 минуты, в течении которых пользователь должен подтвердить операцию, иначе она будет отменена;
- 7 Пользователь нажимает кнопку "Показать QR-код";
- 8 Отображается модальное окно с QR-кодом и полем для ввода пароля
- 9 Пользователь открывает мобильное приложение без доступа к интернету
- 10 В мобильном приложении отображается страница отсутствия подключения к интернету с возможностью повторить попытку подключения или считать QR-код;
- 11 Пользователь нажимает на кнопку "Подтверждение по QR";
- 12 Мобильное приложение открывает страницу считывания QR-кода;
- 13 Пользователь сканирует QR-код;
- 14 Мобильное приложение обрабатывает данные кода, после чего отображает пароль и таймер со сроком действия кода;
- 15 Пользователь вводит пароль в WEB-интерфейсе интернет банка;
- 16 Отображается страница результата подтверждения документа.

1.3. Информация, необходимая для установки  
Стек технологий: Angular, TypeScript, cordova.

Требования к инфраструктуре:

Так как сервис запускается как докер контейнер, то он может запускаться на любой ОС, но в целях лучшей производительности рекомендуется запускать их, используя Linux-сервер (предпочтительно Centos 7).

Обязательным требованием для запуска на хостовой машине является наличие следующего предустановленного ПО:

1. Docker (версия не ниже 20.0.0.)
2. docker-compose (версия не ниже 1.21.0)

Также рабочая конфигурация предполагает наличие веб-сервера реверс-прокси, например, nginx, на сервисы docker.

Веб-сервер может располагаться как на одной машине с сервисами, так и отдельно, основным требованием является наличие доступа веб-сервера к порту хостовой машине, на которой запущены сервис nginx маршрутизатора запроса на сервисы, по умолчанию 10000.