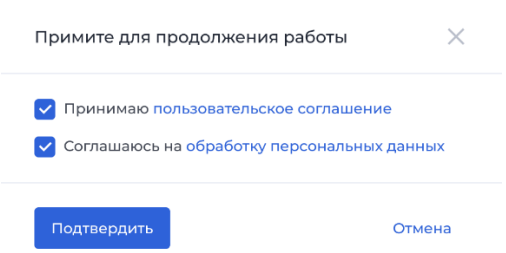
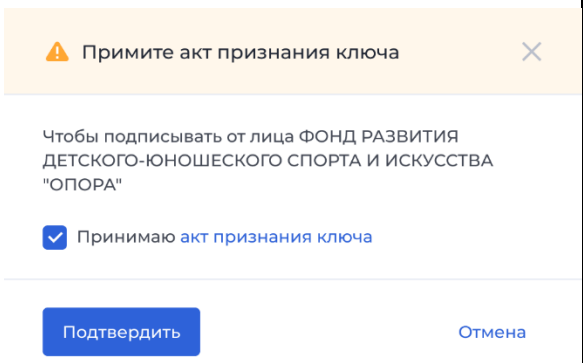
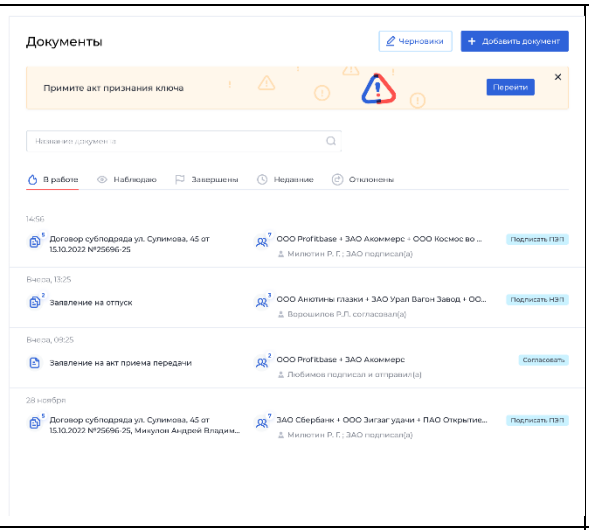
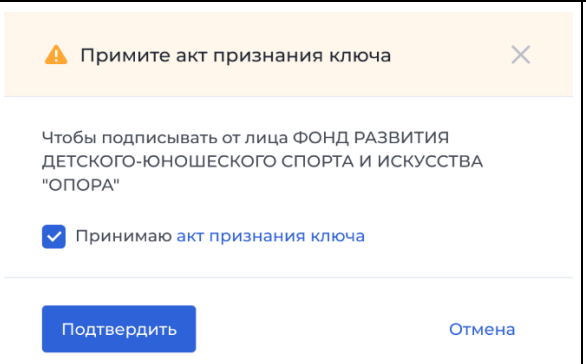
Функциональные характеристики и информация необходимая для установки, эксплуатации компонента «Безбумажный офис - SMS-подпись»

Компонент «Безбумажный офис - SMS-подпись» — веб-приложение, мобильное приложение и программный интерфейс, которые обеспечивают возможность для клиентов-организаций создавать для пользователей –физических лиц и своих сотрудников специальный Ключ ЭП, который хранится на сервере, и возможность для пользователя подписывать документы этим Ключом посредством ввода в приложении одноразового СМС-кода. СМС-код подтверждает волеизъявление пользователя на подписание документа Ключом ЭП на сервере.

Сценарий использования

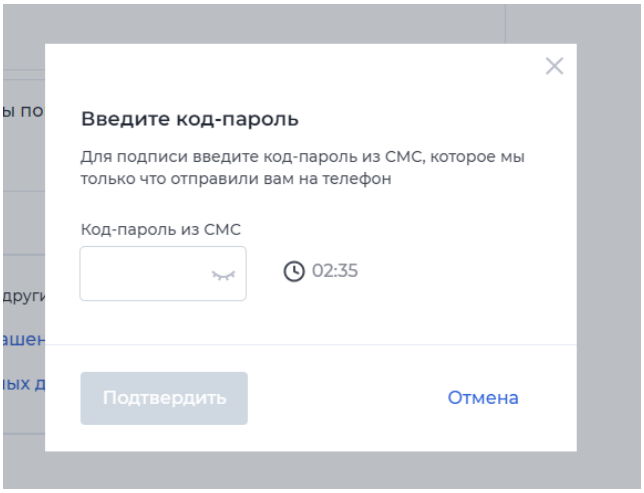
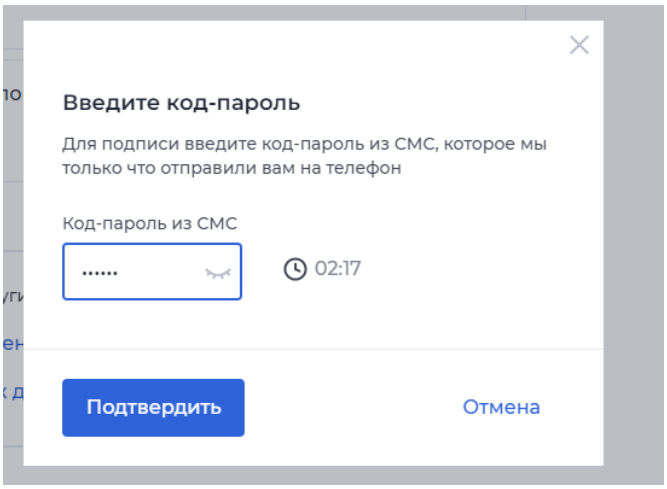
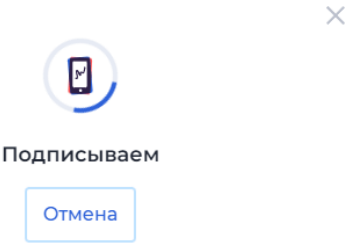
1. Пользователь авторизуется в системе Nopaper

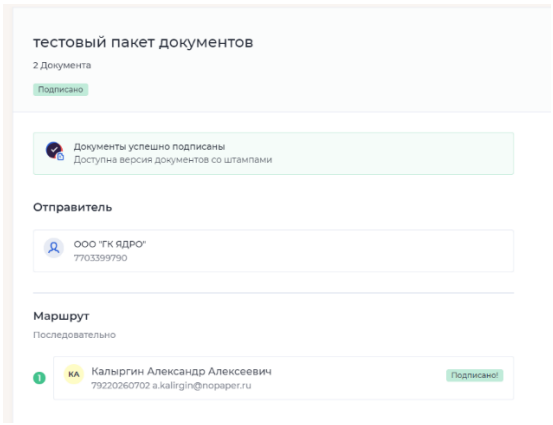
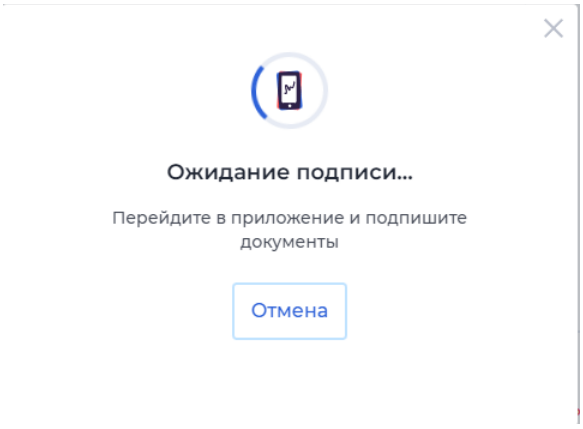
Шаг	Действие	Интерфейс	Требования
Базовый сценарий			
1	**Клиент-организация** регистрирует пользователя в системе через API		• Обязательные поля при регистрации для СМС подписи: • Номер телефона • ФИО
2	**Клиент-организация** выпускает подпись пользователю в системе через API		
3	**Пользователь** выполняет первый вход в систему		
4	**Система** отображает в интерфейсе окно с подтверждением Пользовательского соглашения и Обработки персональных данных		
5	**Пользователь** принимает оба документа и		

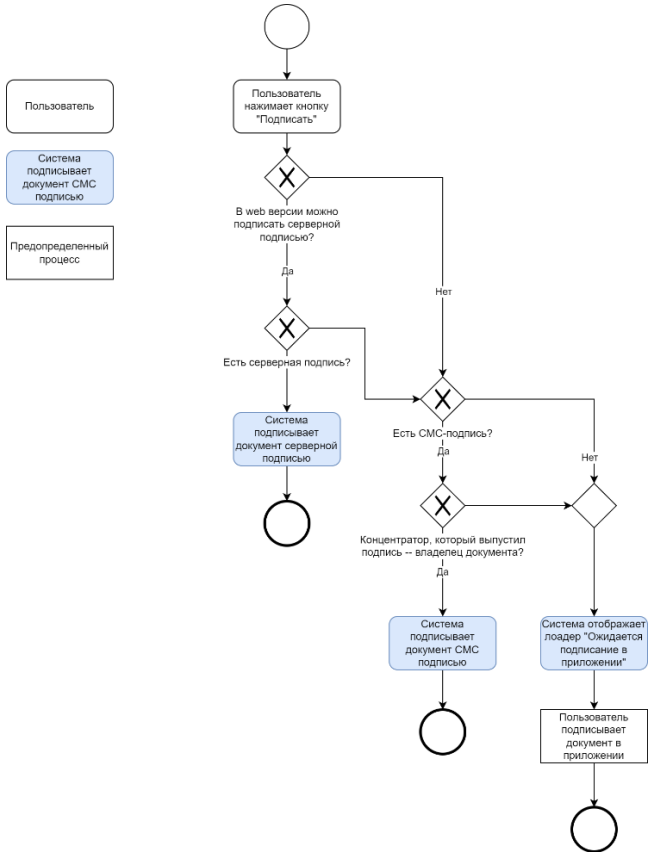
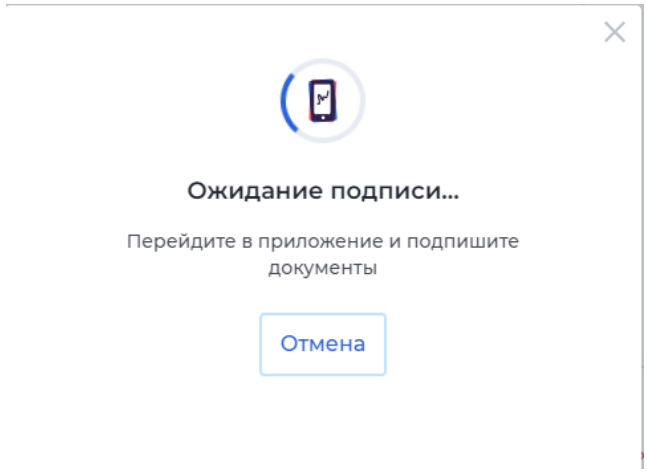
	нажимает кнопку "продолжить"		
6	**Система** отображает в интерфейсе окно с подтверждение акта признания ключа		
7	**Пользователь** принимает акт признания ключа		
Альтернативный сценарий 1 (Пользователь не принимает акт признания ключа)			
7	**Система** отображает в интерфейсе главного экрана информацию "Примите акт признания ключа"		• Весь баннер кликабельный • Баннер можно закрыть • Баннер снова появится при перезаходе в сервис/обновлении страницы
8	**Пользователь** нажимает на информацию "Примите акт признания ключа"		
9	**Система** отображает в интерфейсе окно с подтверждение акта признания ключа		

2. Пользователь подписывает пакет документов

Шаг	Действие	Интерфейс	Требования
Базовый сценарий			
1	**Пользователь** заходит в личный кабинет Nopaper		
2	**Пользователь** заходит в пакет документов		
3	**Пользователь** изучает информацию о документе и нажимает кнопку подписать		
4	**Система** определяет, что установленный тип подписания - НЭП		
5	**Система** определяет, что Клиент-организация пользователя является владельцем п. документов		
6	**Система** определяет, что у пользователя выпущена СМС-подпись		
7	**Система** начинает процесс подписания п. документов СМС-подписью и отображает лоадер		
8	**Система** отправляет СМС-код по номеру телефона пользователя		

9	**Система** выводит в интерфейсе форму для ввода СМС-кода		
10	**Пользователь** вводит СМС-код в форму интерфейса		
11	**Система** определяет, что введеный СМС-код корректен		
12	**Система** инициализирует подписание пакета документов СМС-подписью		
13	**Система** произвела подписание пакета документов		

14	**Система** отображает в интерфейсе информацию об успешном подписании		
15	**Система** отправляет архив с подписанными документами на почту пользователя		
Альтернативный сценарий 1 (Тип подписания КЭП/согласование)			
	5 **Система** отрабатывает по сценарию подписания КЭП/по сценарию согласования		
Альтернативный сценарий 2 (Клиент-организация не является владельцем п. документов)			
	6 **Система** отражает пользователю баннер с просьбой перейти в приложение для подписания документов	 • Схема определения приоритета подписания:	•

				
Альтернативный сценарий 3 (У пользователя нет СМС-подписи)				
	7	**Система** отражает пользователю баннер с просьбой перейти в приложение для подписания документов		
Альтернативный сценарий 4 (Система НЕ отправила СМС-код по номеру телефона пользователя)				
	9	**Система** выводит в интерфейс информацию "ошибка в процессе подписания"		
Альтернативный сценарий 5 (Введённый СМС-код НЕ корректен)				
	12	**Система** выводит в интерфейсе		

		информацию "неверный код"		
	13	**Система** уменьшает количество попыток на 1		Всего количество попыток 5
	14	**Система** отображает в интерфейсе информацию об отправке нового СМС-кода		Таймер равен 3 минутам (после отправки СМС-кода таймер обнуляется и становится снова 3 мин. после неудачного ввода СМС-кода)
	15	Повторяется процесс с п.10		
Альтернативный сценарий 6 (Система НЕ произвела подписание пакета документов)				
	14	**Система** выводит в интерфейсе информацию "неверный код"		
	15	**Система** выводит в интерфейс информацию "ошибка в процессе подписания"		
Альтернативный сценарий 7 (Система ожидает совершения активного действия от всех участников маршрута)				
	16	**Система** отправляет архив с подписанными документами на почту пользователя		

Общее описание выдачи СМС-подписи через REST-API

1. Получить наличие учетной записи пользователя

- Система партнёра может проверять наличие пользователя в nopaper перед регистрацией нового пользователя. Для этого необходимо выполнить запрос «Проверить наличие пользователя в nopaper» /partner-api/api/v2/external/profile-fl/user-guid/by-phone. В запросе требуется передать номер

телефона будущего пользователя. В ответе noparer вернёт userGuid действующего пользователя или сообщение, что пользователь не найден.

Примечания:

- Запрос принимает российский номер телефона в формате 79*********.

2. Зарегистрировать учётную запись пользователя

- Система партнера может зарегистрировать новых пользователей в Noparer, используя запрос «Зарегистрировать учетную запись физического лица» по адресу /partner-api/api/v2/external/profile-fl. В запросе необходимо указать номер телефона будущего пользователя. В ответе Noparer вернет userGuid созданного пользователя, который должен быть сохранен в системе партнера для дальнейшего использования других методов API.

- При регистрации в Noparer, пользователю будет отправлено СМС-сообщение с логином, временным паролем для авторизации и ссылкой на установку мобильного приложения. После авторизации пользователь сможет использовать стандартный функционал Noparer: выпустить мобильную подпись и начать подписывать документы с другими пользователями. Пароль, генерируемый для пользователя, является временным. После истечения срока действия такого пароля, пользователю будет необходимо самостоятельно установить пароль.

- Время действия пароля задается настройкой в запросе. Долгосрочный временный пароль (30 дней) имеет сложный набор символов, содержащий цифры, латинские буквы и специальные символы (например, 6](tm83). Краткосрочный пароль (12 часов) состоит из 6 цифр (например, 657227).

- Пользователь Noparer — это, в первую очередь, физическое лицо. Далее физическое лицо может добавить свою компанию в Noparer, если является руководителем, или действующая компания может присоединить физическое лицо в Noparer в роли сотрудника.

Примечания:

- Запрос принимает российский номер телефона в формате 79*********.
- Для брендированных приложений имя отправителя СМС-сообщения может быть изменено на имя компании партнера.
- Для SDK-приложений отправка СМС-сообщения при регистрации пользователя может быть отключена.

3. Передать данные о пользователе (физ. лице)

- Системе партнёра необходимо передать ФИО пользователя, чтобы дальше создать подпись Сотруднику п.3.5. Для этого необходимо выполнить запрос «Передать данные пользователя» /partner-api/api/v2/external/profile-fl. В запросе требуется передать userGuid — идентификатор пользователя, который получен при проверке наличия пользователя в noparer п.3.1 или при регистрации п.3.2. В ответе noparer вернёт статус выполнения запроса.

- Noparer проверяет данные при получении запроса.

- Проверяет что профиль Клиента в noparer можно заполнить новыми данными: если Клиент самостоятельно прошёл верификацию личности в сервисе и получил подпись — партнёр не может изменить его данные через API; но партнёр может создать подпись Клиенту п.3.5. для текущих паспортных данных в профиле;

- Передать ФИО можно также сразу при регистрации пользователя, п.3.2.

4. Создать СМС-подпись пользователю

- Система партнёра может создавать СМС подпись Клиентам в noparer. СМС подпись позволяет подписывать документы от имени Клиента без использования мобильного приложения noparer. Для этого необходимо выполнить запрос «Создать СМС подпись клиенту» /partner-api/api/v2/external/certificate/pay-control/pc-sms. В запросе требуется передать userGuid — идентификатор

пользователя, который получен при проверке наличия пользователя в nopaper п.2.1 или при регистрации п.2.2., responsiblePartyForAcceptanceAct – настройку, которая отвечает на чьей стороне будет сгенерирован акт признания ключа (документ подтверждающий принятие подписи) и acceptingAcceptanceActType – настройку, которая отвечает за то как будет принят акт признания ключа (для принятия акта во внешней системе нужно указывать acceptingAcceptanceActType = 1).

- Если выбрана настройка responsiblePartyForAcceptanceAct = 1 – то акт признания ключа будет сгенерирован и подписан в системе Nopaper; если выбрана настройка responsiblePartyForAcceptanceAct = 2 – то акт признания ключа генерируется самостоятельно на стороне Партнёра на основании полученной информации о подписи (п.3.8.). В ответе nopaper вернёт certificateId — идентификатор подписи. certificateId необходимо сохранить в системе партнёра, чтобы использовать при вызове других методов API.
- Nopaper создаёт подпись НЕ активной providerStatus=3 (initialization) при генерации акта признания на стороне Партнёра. Для подписания документов подпись необходимо будет активировать (п.3.6).

Примечания:

- При изменении статуса подписи в статус Initialization система Nopaper отправит уведомление о изменении статуса подписи (см. диаграмму последовательности)
- При изменении статуса сертификата, который создан Партнёром, отправляется CallbackInfo(type(2)) (подробнее в документации “Работа с уведомлениями call-back API Nopaper” - п.4.2.)

5. Получить информацию о подписях (опционально)

- Система партнёра может получать информацию подписях Пользователя в nopaper. Для этого необходимо выполнить запрос «Получить список сертификатов Пользователя» /partner-api/api/v2/external/certificate/list. В запросе требуется передать userGuid — идентификатор пользователя, который получен при проверке наличия пользователя п.3.1. или при регистрации п.3.2. В ответе nopaper вернёт список подписей Сотрудника (массив объектов) во всех статусах, с ключевой информацией о каждой подписи.

Список статусов подписи:

- status=1 (Template) — шаблон подписи
- status=2 (Initialization) — инициализация подписи
- status=3 (initializationError) — ошибка при инициализации подписи
- status=4 (Available) — подпись активна
- status=5 (Blocked) — подпись заблокирована
- status=6 (Revoked) — подпись отозвана

Информация о подписи нужна чтобы сформировать и подписать с Сотрудником Акт признания ключа, которым Сотрудник признает использование выпущенной подписи.

Примечания:

- Nopaper не может вернуть информацию о подписи в полном объёме в момент создания п.3.5, полная информация о подписи приходит после того, как подпись завершит инициализацию подписи. Инициализация подписи в системе Nopaper происходит практически мгновенно после создания.

- Можно использовать этот метод API для синхронизации данных между системами в исключительных ситуациях;

- Партнёр может получить только информацию о подписях, которые сам создал/выдал. Если Клиент получил подпись самостоятельно в Nopaper, то подпись не вернётся партнёру в ответе на запрос.

6. Получить акт признания ключа пользователя (опционально)

- Система партнёра может получить акт признания ключа Сотрудника, которому выдала подпись. Для этого необходимо выполнить запрос «Получить акт признания ключа для сертификата» /partner-api/api/v2/external/certificate/pay-control/{certificateId}/act-acceptance-key. В запросе требуется передать certificateId — идентификатор подписи, который получен при создании подписи п.3.5. В ответе nopaper вернёт статус выполнения запроса.

- Примечания:

- Nopaper не может вернуть акт признания ключа в момент создания п.3.4, акт признания ключа можно получить только после того, как подпись завершит инициализацию подписи. Инициализация подписи в системе nopaper происходит практически мгновенно после создания.

7. Активировать подпись пользователя (опционально)

- Система партнёра может активировать подпись Сотрудника своей компании в nopaper. Для этого необходимо выполнить запрос «Активировать сертификат Pay-control» /partner-api/api/v2/external/certificate/pay-control/{certificateId}/activate. В запросе требуется передать certificateId — идентификатор подписи, который получен при создании подписи п.3.5. В ответе nopaper вернёт статус выполнения запроса.

Примечания:

- Активировать акт признания ключа можно только после завершения инициализации подписи.

8. Заблокировать/разблокировать подпись пользователя

Система партнёра может заблокировать/разблокировать подпись Сотрудника своей компании в nopaper, если необходимо заблокировать подпись с возможностью её дальнейшей активации. Для этого необходимо выполнить запрос «Заблокировать/разблокировать сертификат Pay-control» /partner-api/api/v2/external/certificate/pay-control/{certificateId}/blocking-control. В запросе требуется передать certificateId — идентификатор подписи, который получен при создании подписи п.3.5 и параметр isBlock отвечающий за блокировку/разблокировку подписи. В ответе Nopaper вернёт статус выполнения запроса.

9. Отозвать подпись пользователя

Система партнёра может отозвать подпись Сотрудника своей компании в nopaper, если необходимо заблокировать подпись без возможности её дальнейшей активации. Для этого необходимо выполнить запрос «Отозвать сертификат Pay-Control» /partner-api/api/v2/external/certificate/pay-control/{certificateId}/revoke. В запросе требуется передать certificateId — идентификатор подписи, который получен при создании подписи п.3.5. В ответе Nopaper вернёт статус выполнения запроса.