QR-код

Соглашение об использовании электронных документов № ____

город Новороссийск «____» _____ 2019 год

ООО “Порт транзит”, именуемое в дальнейшем «Сторона-1», в лице генерального директора Незамутдинова Руслана Яновича, действующего на основании Устава, с одной стороны, и _____ (_____) в лице _____, действующего на основании _____, именуемое в дальнейшем «Сторона-2», с другой стороны, совместно именуемые Стороны, заключили настоящее соглашение об использовании электронных документов (далее по тексту Соглашение).

1. Термины и определения

1.1. Авторизация – подтверждение полномочий (предоставление прав доступа) Стороне-2, успешно прошедшей Аутентификацию входа, на получение услуг Стороны-1, предусмотренных Соглашением.
1.2. Акт признания ключа проверки ЭП – документ на бумажном носителе, подтверждающий принадлежность ключа проверки электронной подписи владельцу акта признания ключа проверки электронной подписи.
1.3. Активация – процедура персонализации Мобильного приложения PayControl, состоящая из следующих шагов:

- успешный ввод/передача в Мобильное приложение PayControl QR-кода/ключа инициализации PayControl;
- формирование в Мобильном приложении PayControl и регистрации на сервере Мобильного приложения PayControl набора уникальных признаков Мобильного устройства Стороны-2;
- создание Ключей ЭП в Мобильном приложении PayControl;
- регистрация ключа проверки ЭП PayControl на сервере Мобильного приложения PayControl с целью дальнейшей проверки ЭП Стороны-2;
- создание Стороной-2 Пароля/TouchID/FaceID для дальнейшего использования в качестве аутентификационных данных.

1.4. Аутентификационные данные – Пароль/TouchID/FaceID, используемый для целей установления личности Стороны-2 при доступе к функциональности Мобильного приложения PayControl.
1.5. Аутентификация входа – процедура проверки соответствия предъявленных Аутентификационных данных Аутентификационым данным, установленным при активации мобильного приложения, выполняемая перед началом работы в Мобильном приложении PayControl. Без успешной Аутентификации входа доступ к функциям подписи в Мобильном приложении PayControl не предоставляется.
1.6. Ключи инициализации PayControl - уникальные ключи, выпускаемые Стороной-1 для каждой учетной записи Стороны-2 – владельца средства ЭП PayControl.
1.7. Ключ ЭП PayControl - уникальная последовательность символов, используемая для формирования ЭП документа Стороной-2. Вырабатывается на Мобильном устройстве Стороны-2 одновременно с Ключом проверки ЭП PayControl с использованием средства ЭП PayControl при выполнении процедуры Активации, а также при плановой смене ключей ЭП PayControl. Однозначно соответствует ключу проверки ЭП PayControl. Хранится на Мобильном устройстве Стороны-2 и защищен средствами Мобильного приложения PayControl, средствами ОС Мобильного устройства и аппаратными средствами устройства.
1.8. Ключ проверки ЭП PayControl - уникальная последовательность символов, служащая для проверки значения ЭП документа. Вырабатывается на Мобильном устройстве Стороны-2 одновременно с Ключом ЭП PayControl с использованием средства ЭП PayControl при выполнении процедуры Активации, а также при проведении плановой смены ключей ЭП PayControl. Однозначно соответствует Ключу ЭП PayControl. Хранится на мобильном устройстве Стороны-2, а также передается на Сервер PayControl, располагающийся в инфраструктуре Стороны-1, для целей обеспечения процедуры Проверки ЭП.
1.9. Компрометация ключей ЭП PayControl - событие, в результате которого ключ PayControl или его часть становятся известны или доступны постороннему лицу, либо при возникновении подозрения, что такое событие могло произойти. К событиям, связанным с компрометацией ключей PayControl относятся, включая, но не ограничиваясь, следующие:
1.9.1. Потеря Мобильного устройства Стороной-2 с загруженными ключами инициализации и/или выпущенными рабочими ключами ЭП;
1.9.2. Потеря Мобильного устройства Стороны-2 с загруженными ключами инициализации и/или выпущенными рабочими ключами ЭП с последующим обнаружением в местах, где к устройству могли получить доступ третьи лица;
1.9.3. Увольнение сотрудников, имевших доступ к Мобильному устройству Стороны-2 с загруженными ключами инициализации и/или выпущенными рабочими ключами;
1.9.4. Нарушение правил хранения Мобильного устройства Стороной-2 с загруженными ключами инициализации и/или выпущенными рабочими ключами;
1.9.5. Возникновение подозрений на утечку ключевой информации или ее искажение;
1.9.6. Случаи, когда нельзя достоверно установить, что произошло с мобильным устройством Стороны-2 с загруженными и/или выпущенными ключами (в том числе случаи, когда Мобильное устройство вышло из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).
1.10. Различаются два вида компрометации ключа ЭП: явная и неявная. Первые четыре события трактуются как явная компрометация ключей. Следующие два требуют специального рассмотрения в каждом конкретном случае.
1.11. Мобильное приложение PayControl – мобильное приложение для операционных систем iOS и Android, разработанное ООО «СэйфТек» (SafeTech LTD), выполняющее функции управления ключевой информацией (считывание, хранение, использование, обновление, удаление), получения информации для подтверждения от серверной части, отображения подтвержденной информации на экране мобильного устройства, выработки кода подтверждения на основе данных операции, ключа пользователя, времени обработки, отправки кода подтверждения в серверную часть.
1.12. Мобильное устройство – смартфоны, мобильные телефоны, планшеты и прочие устройства, на которых есть доступ в Интернет, установлено Мобильное приложение PayControl и которые привязаны к Номеру телефона. Используется как носитель ключевой информации для средства ЭП PayControl.

1.13. Номер телефона – номер мобильного телефона, указанный Стороной-2 в Акте признания электронной подписи или в Заявлении на удаление/ выдачу/ обновление ключей электронной подписи.
1.14. Носитель ключевой информации (НКИ) - носитель информации, предназначенный для записи, хранения, воспроизведения ключа ЭП. Включает Мобильное устройство с загруженными ключами средства ЭП PayControl.
1.15. QR-код – оптическая метка, содержащая компонент Ключа.
1.16. Плановая смена ключей PayControl - процедура смены ключей инициализации и рабочих ключей ЭП PayControl в связи с окончанием срока их действия. Включает загрузку в Мобильное устройство новых ключей инициализации PayControl, автоматизированный выпуск Стороной-2 нового ключа ЭП PayControl, отправку и регистрацию на сервере PayControl.
1.17. Проверка ЭП – процедура проверки соответствия предъявленной ЭП данным Операции, времени формирования ЭП и набору уникальных признаков Мобильного устройства, выполняемая с использованием ключа проверки ЭП PayControl на сервере Мобильного приложения PayControl.
1.18. Система ЭДО – система электронного документооборота.
1.19. Средство ЭП PayControl - программный комплекс, предназначенный для подтверждения уполномоченным лицом Стороны-2 операций в Системах ЭДО.
1.20. Формирование ЭП – процедура выпуска ЭП Стороны-2 в Мобильном приложении PayControl на основе данных операции, времени формирования и набора уникальных признаков Мобильного устройства, выполняемая с использованием ключа ЭП.
1.21. Электронная подпись (ЭП) – информация в электронной форме, созданная с использованием ключа ЭП, которая используется для подтверждения операций в Мобильном приложении. В рамках Услуги используется простая ЭП, предусмотренная Федеральным законом от 06.04.2011 No63-ФЗ «Об электронной подписи».
1.22. Электронное сообщение – информация в электронной форме, переданная или полученная Стороной-2, использующей Мобильное приложение PayControl.
1.23. Электронный документ (ЭД) - документ, в котором информация представлена в электронно-цифровой форме.
1.24. PUSH-сообщение – короткое сообщение, направляемое Стороной-1 Стороне-2, поступает на мобильное устройство Стороны-2 исключительно при наличии доступа к сети Интернет.

2. Общие положения

2.1. Условия Соглашения определяют:
2.1.1. порядок электронного обмена документами во исполнение своих обязательств по всем заключенным между Стороной-2 и Стороной-1 договорам, а также по всем договорам, которые будут заключены в будущем;
2.1.2. порядок подключения Стороне-2 средства ЭП PayControl, при котором Сторона-2 принимает условия Соглашения полностью;
2.1.3. порядок подтверждения операций с использованием средства ЭП PayControl;
2.1.4. перечень операций, которые Стороне-2 может подтверждать с помощью средства ЭП PayControl;
2.1.5. порядок прекращения Стороной-1 предоставления Услуги Стороне-2.
2.2. Присоединение к условиям Соглашения осуществляется посредством совершения Стороной-2 следующих действий:
2.2.1. подписание Стороной-2 Соглашения;
2.2.2. получения QR-кода и кода активации, полученного в СМС-сообщении на Номер телефона Стороны-2 для регистрации средства ЭП PayControl;
2.2.3. установки Стороной-2 на Мобильное устройство приложения PayControl.

3. Средства ЭП PAYCONTROL

3.1. Сторона-1 не контролирует, не проверяет, не дает одобрения и не несет какой-либо ответственности за иные приложения, добавляемые Стороной-2 на свое Мобильное устройство.
3.2. Сторона-2 и Сторона-1 признают успешно выполненную Стороной-1 Проверку ЭП в соответствии с Соглашением равнозначной собственноручной подписи Стороны-2 на документах, составленных на бумажном носителе.
3.3. Средство ЭП PayControl является средством простой ЭП. Стороны признают применение средства простой ЭП PayControl в системе ЭДО достаточным для обеспечения целостности, авторства и неотказуемости передаваемой между Сторонами информации и невозможности ее фальсификации после момента её подписания.
3.4. Аутентификационные данные используются Стороной-2 при каждой Авторизации в Мобильном приложении PayControl.

4. Требования технической защиты к Мобильному устройству Стороны-2

4.1. Перед подключением к средству ЭП PayControl Сторона-2 должна обеспечить работу Мобильного устройства в следующем режиме:
4.1.1. на Мобильном устройстве должны быть установлены лицензионные, регулярно обновляемые (устанавливаются обновления безопасности) операционная система, антивирусное программное обеспечение;
4.1.2. мобильное устройство не должно быть подвергнуто операциям повышения привилегий/взлома операционной системы устройства (jail-break, rooting);
4.1.3. Сторона-2 должна использовать процедуру аутентификации доступа к Мобильному устройству.

5. Меры по защите информации

5.1. Сторона-2 никогда и никому не сообщает Ключ и Пароль для Аутентификации входа в Мобильное приложение PayControl.
5.2. Сторона-2 использует со средством ЭП PayControl Мобильное устройство, приобретенное у официального продавца и сертифицированное по требованиям ГОСТ в соответствии с действующим законодательством для использования на территории Российской Федерации.
5.3. Сторона-2 использует на своих рабочих станциях и/или Мобильных устройствах, применяемых для подключения к подсистемам Системы ЭДО только лицензионное ПО.
5.4. Сторона-2 соблюдает требования лицензионного соглашения на СКЗИ и/или средство ЭП PayControl.
5.5. Сторона-2 обязуется устанавливать приложение PayControl из официальных репозиториев AppStore и Google Play.

6. Выпуск Ключей для Средства ЭП PayControl

6.1. Перед выпуском рабочих ключей средства ЭП PayControl Стороне-2 необходимо выполнить требования технической защиты к Мобильному устройству, включая установку Мобильного приложения PayControl из одного из официальных репозиториев Google Play или App Store.
6.2. Ключи инициализации Средства ЭП PayControl выпускается Стороной-1 для каждой учетной записи Стороны-2 – владельца Средства ЭП PayControl.
6.3. Первая часть ключей инициализации в виде QR-кода передается Стороной-1 каждой учетной записи Стороны-2 на бумажном носителе (на первой странице Соглашения).
6.4. Вторая часть ключей инициализации направляется учетной записи в виде SMS сообщения.
6.5. После сканирования приложением PayControl Мобильного устройства Стороны-2 первой части ключей инициализации и ввода в приложение PayControl значения второй части из SMS сообщения, система PayControl выполняет автоматическую процедуру выпуска рабочего ключа ЭП с сохранением его в зашифрованном виде в Мобильном устройстве, отправки к Стороне-1 значения ключа проверки ЭП и инициализации ключа проверки ЭП у Сторон-1.
6.6. Сторона-1 средствами системы формирует Акт признания ключа проверки ЭП, подписывает и передает Стороне-2 на физическом бумажном носителе.
6.7. Сторона-2 просматривает полученный Акт признания ключа проверки ЭП PayControl, сравнивает реквизиты Акта, включая Идентификатор пользователя и значение Ключа проверки ЭП PayControl из приложения PayControl Мобильного устройства со значениями в Акте, подписывает и передает один экземпляра Акта признания ключа проверки ЭП PayControl Стороне-1.

7. Порядок подписания ЭД Средством ЭП PAYCONTROL

7.1. ЭД, подписанный Средством ЭП PayControl, считается подписанным, если он подписан с помощью ключа ЭП, для которого Стороной-1 зарегистрирован ключ проверки ЭП.
7.2. Порядок подписания ЭД в Мобильном приложении PayControl:
7.2.1. Сторона-1 на основании указания Стороны-2 формирует и направляет Стороне-2 Электронное сообщение с шаблоном ЭД из информационной системы PayControl;
7.2.2. после поступления Стороне-2 от Стороны-1 через Мобильное приложение PayControl Электронного сообщения с шаблоном ЭД на Мобильное устройство Стороны-2 поступает PUSH-сообщение о необходимости подписания ЭД;
7.2.3. Сторона-2 проходит Аутентификацию входа в Мобильном приложении PayControl;
7.2.3. в Мобильном приложении PayControl Сторона-2 видит Электронное сообщение Стороны-1 с шаблоном ЭД;
7.2.4. Стороне-2 предоставляется возможность подписать ЭД Средством ЭП PayControl или отклонить подписание;
7.2.5. в случае решения Стороны-2 не подписывать ЭД, Сторона-2 нажимает кнопку «Отказаться». В этом случае ЭД не будет подписан ЭП и не будет направлен на исполнение к Стороне-1;
7.2.6. в случае решения Стороны-2 подписывать ЭД, Сторона-2 нажимает кнопку «Подтвердить». В этом случае с помощью Мобильного приложения PayControl ЭД подписывается ЭП и направляется на исполнение к Стороне-1;
7.2.7. Сторона-1 выполняет проверку ЭП;
7.2.8. если Сторона-2 приняла решение не подписывать ЭД в течение установленного времени с момента получения соответствующего Электронного сообщения от Стороны-1, такое Электронное сообщение исчезает из списка операций в Мобильном приложении PayControl и будет аннулировано в Средстве ЭП PayControl.

8. Права и обязанности Сторон

8.1. Сторона-1 вправе:
8.1.1. требовать от Стороны-2 неукоснительного соблюдения Соглашения;
8.1.2. отказать Стороне-2 в оказании Услуги, если Стороной-2 не соблюдены требования законодательства РФ, условий Соглашения, а также в случае, если установлено предоставление Стороной-2 недостоверной информации, необходимой для оказания Услуги;
8.1.3. без предварительного уведомления Стороны-2 временно приостановить или ограничить доступ Стороны-2 к Средству ЭП PayControl, при наличии у Стороны-1 достаточных оснований считать, что по используемому Стороной-2 каналу доступа возможна попытка несанкционированного доступа от имени Стороны-2 или в иных случаях по усмотрению Стороны-1. О временном приостановлении или ограничении доступа Сторона-1 оповещает Сторону-2 через приложение ЭП PayControl;
8.1.4. Осуществлять сбор информации о Мобильном устройстве для целей противодействия угрозам возникающим при использовании Средства ЭП PayControl, таких как:
- геолокация;
- информация об устройстве;
- информация о подключении к сети;
- события, происходящие в Мобильном приложение PayControl;
- обнаруженное потенциально вредоносное ПО;

8.1.5. Отказать в доступе к Средству ЭП PayControl Стороне-2 в случае:
- обнаружения или возникновения подозрений о неправомерности проводимых Стороной-2 операций;
- выявления в ЭД признаков сомнительных операций, связанных с легализацией доходов, полученных преступным путем, либо операций, несущих репутационные риски для Стороны-1.

8.2. Сторона-1 обязуется:
8.2.1. осуществить подключение Стороны-2 к Услуге;
8.2.2. обеспечить Защиту информации в рамках осуществления подписанных Стороной-2 ЭД, проводимых в соответствии с Соглашением;
8.2.3. принять меры для предотвращения несанкционированного доступа третьих лиц к конфиденциальной информации, связанной с использованием Стороной-2 Средства ЭП PayControl. Любая информация такого рода может быть предоставлена третьим лицам не иначе как в порядке, установленном законодательством Российской Федерации;
8.2.4. в случаях, когда использование Ключа, Пароля предполагает передачу Стороне-2 либо хранение Стороной-1 какой-либо конфиденциальной информации, Сторона-1 обязуется принять все необходимые меры организационного и

технического характера для предотвращения доступа третьих лиц к такой информации до передачи ее Стороне-2, а также во время ее хранения Стороной-1;
8.2.5. не использовать для подписи документов скомпрометированные Ключи ЭП Стороны-2;
8.2.6. на основании полученной от Стороны-2 информации о фактах компрометации прекратить доступ к Средству ЭП PayControl.
8.3. Сторона-2 вправе:
8.3.1. использовать Мобильное приложение PayControl для электронного обмена документами в соответствии с Соглашением;
8.3.2. отказаться от использования Мобильного приложения PayControl;
8.3.3. оформить письменную претензию в случае несогласия с операцией, проведенной с использованием подтверждения в Мобильном приложении PayControl. Процедура разрешения конфликтных ситуаций описана в Приложении № 1 к Соглашению.
8.4. Сторона-2 обязуется:
8.4.1. своевременно и в полном объеме до момента подписания Соглашения ознакомиться с условиями Соглашения;
8.4.2. соблюдать Соглашение;
8.4.3. обеспечить использование Ключей ЭП в Системе ЭДО только их владельцами (с установленными правами подписи).
8.4.4. обеспечить конфиденциальность, а также хранение Мобильного устройства, Ключа, Пароля способом, исключающим доступ к ним третьих лиц, а также немедленно уведомлять Сторону-1 о подозрении, что Мобильное устройство, Ключ, Пароль может быть использовано посторонними лицами;
8.4.5. немедленно известить Сторону-1 о фактах компрометации по телефону и в письменной форме.
8.4.6. при смене Мобильного устройства и/или Номера телефона обратиться к Стороне-1 для получения нового QR-кода для Активации в Средстве ЭП PayControl.

9. Ответственность Сторон

9.1. Сторона-1 не несет ответственность за ущерб, возникший:
9.1.1. вследствие несанкционированного доступа к мобильному устройству Стороны-2, Ключа, Паролю и их использования третьими лицами;
9.1.2. вследствие нарушения Стороной-2 требований технической защиты мобильного устройства;
9.1.3. в случае нарушения Стороной-2 настоящих Условий;
9.1.4. вследствие принятия высшими органами законодательной и исполнительной власти Российской Федерации решений, которые делают невозможным для Стороны-1 выполнение своих обязательств по предоставлению Услуги;
9.1.5. вследствие сбоев в работе линий связи, обрыва линий связи, выхода из строя оборудования у телефонного оператора и/или оператора доступа к сети Интернет;
9.1.6. Сторона-1 не несет ответственность за качество линий связи.
9.2. Сторона-1 не несет ответственности за любые убытки, понесенные Стороной-2 в результате действия или бездействия оператора сотовой связи либо иного третьего лица. Иск может быть предъявлен фактическому виновнику убытков, исключая Сторону-1.
9.3. Сторона-2 несет ответственность:
9.3.1. за все ЭД, подписанные Стороной-2;
9.3.2. за нарушение требований технической защиты мобильного устройства.

10. Реквизиты и подписи Сторон

Сторона-1:	Сторона-2:
ИНН: 2315190510	ИНН:
353960, г.Новороссийск, ул.Ленина 1 «А»	Адрес:
р/с: 40702810530000018368	Р/счет:
Банк: Краснодарское отделение №8619 ПАО Сбербанк	
БИК: 040349602	
к/с: 30101810100000000602	
_____ Незамутдинов Р.Я.	_____ ФИО

Приложение № 1

к Соглашению об использовании электронных документов № ____ от «____» _____ 2019 года

Процедура разрешения конфликтных ситуаций

1. Определения:
1.1. АРМ РКС – автоматизированное рабочее место разбора конфликтных ситуаций.
1.2. Ключ ЭП PayControl - уникальный ключ, самостоятельно выпускаемый Стороной-2 одновременно с ключом проверки ЭП PayControl с использованием средства ЭП PayControl при выполнении процедуры первичного выпуска ключа ЭП PayControl, а так-же при плановой смене ключей ЭП PayControl. Однозначно соответствует ключу проверки ЭП PayControl.
1.3. Средство ЭП PayControl - программный комплекс, предназначенный для подтверждения уполномоченным лицом Стороны-2 операций в Системах ЭДО.
1.4. Электронный документ (ЭД) - документ, в котором информация представлена в электронно-цифровой форме.
1.5. Электронная подпись (ЭП) – информация в электронной форме, созданная с использованием Закрытого ключа ЭП, которая используется для подтверждения операций в Мобильном приложении. В рамках Услуги используется простая ЭП, предусмотренная Федеральным законом от 06.04.2011 No63-ФЗ «Об электронной подписи».
2. В данном документе описан порядок разрешения конфликтов между пользователями Системы ЭДО (Сторона-2) и Стороной-1, связанных с подлинностью ЭД, и разрешение которых осуществляется на основании результатов проверки ЭП Стороны-2 под ЭД, подписанным при помощи Средства ЭП PayControl. ЭД считается подлинным, если получен положительный результат подтверждения подлинности ЭП.
3. Для рассмотрения конфликтных ситуаций по письменному заявлению Стороны-2 в течение 7 дней с момента его подачи создается Экспертная комиссия. Результатом деятельности комиссии является определение Стороны, несущей ответственность по документам, вызвавшим конфликтную ситуацию. Заявление подается Стороной-2 в офис Стороны-1.
4. Экспертная комиссия состоит из 4 человек, ее членами являются представители: Стороны-1, Стороны-2, разработчика Средства ЭП PayControl и разработчика Системы ЭДО.
5. Экспертная комиссия осуществляет свою работу на территории Стороны-1, с использованием эталонного программного обеспечения и ключами системы защиты информации, участвующих в конфликте Сторон.
6. Экспертная комиссия приступает к работе в течение 7 рабочих дней со дня поступления письменного заявления от Стороны-2. Все действия, предпринимаемые Экспертной комиссией для выяснения фактических обстоятельств, а также выводы, сделанные Экспертной комиссией, заносятся в Протокол работы Экспертной комиссии. Протокол работы Экспертной комиссии должен содержать следующие данные:
- дата и места проведения;
- состав Экспертной комиссией с указанием сведений о квалификации каждого из членов комиссии;
- краткое изложение обстоятельств возникшей конфликтной ситуации;
- указанные в пунктах с 7 по 11 мероприятия, проводимые Экспертной комиссией для установления причин и последствий возникшей конфликтной ситуации;
- выводы, к которым пришла Экспертная комиссия в результате проведенных мероприятий;
- подписи всех членов Экспертной комиссии.

7. С целью соблюдения Стороной-2 требований по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации Системы ЭДО проводится техническая экспертиза.
8. Для проведения технической экспертизы спорного ЭД Экспертная комиссия получает:
8.1. у Администратора Системы ЭДО Стороны-1 и разработчика Средства ЭП PayControl:
8.1.1. специализированное ПО разработчика Средства ЭП PayControl – АРМ РКС;
8.1.2. идентификатор пользователя;
8.1.3. файл спорного ЭД и/или данные транзакции;
8.1.4. код подтверждения, выработанный на симметричных ключах;
8.1.5. ЭП, выработанная на асимметричных ключах (при оффлайн-подтверждении отсутствует);
8.1.6. время выработки ЭП.
8.2. Акт признания ключа проверки ЭП Стороны-2 (достоверность и работоспособность которого установлена на время совершения спорной операции).
9. Проведение технической экспертизы спорного ЭД включает в себя выполнение следующих действий:
9.1. загрузку в АРМ РКС:
- идентификатора пользователя;
- спорная операция;
- код подтверждения, выработанный на симметричных ключах;
- ЭП, выработанная на асимметричных ключах (при оффлайн-подтверждении отсутствует);
- время выработки ЭП.

9.2. проверку результатов разбора в АРМ РКС;
9.3. печать протокола работы АРМ РКС.
10. Спор решается в пользу Стороны-1, если:
10.1. ЭП для данной спорной операции верна;
10.2. ключ проверки ЭП PayControl, отобранный для разбора конфликтной ситуации, соответствует значению ключа в Акте признания ключа проверки ЭП;

10.3. проверяемая спорная операция была подписана ключом ЭП, соответствующим зарегистрированному Стороной-1 ключу проверки ЭП, использованному при проведении технической экспертизы;
10.4. владельцем ключа ЭП и ключа проверки ЭП PayControl является Представитель Стороны-2, зарегистрированный Стороной-1.
11. Спор решается в пользу Стороны-2, если:
11.1. ЭП для данной спорной операции не верна;
11.2. ключ проверки ЭП PayControl, отобранный для разбора конфликтной ситуации, не соответствует значению ключа в Акте признания открытого ключа (достоверность и работоспособность которого однозначно установлена на время совершения спорной операции);
11.3. проверяемая спорная операция не была подписана ключом ЭП, соответствующим зарегистрированному Стороной-1 ключу проверки ЭП, использованному при проведении технической экспертизы;
11.4. владельцем ключа ЭП и ключа проверки ЭП PayControl не является Представитель Стороны-2, зарегистрированный Стороной-1.
12. В случае если мнение члена (или членов) Экспертной комиссии относительно порядка, методики, целей проводимых мероприятий не совпадает с мнением большинства членов Экспертной комиссии, об этом в Протоколе составляется соответствующая запись, которая подписывается членом (или членами) Экспертной комиссии, чье особое мнение отражает соответствующая запись.
13. Протокол составляется на бумажном носителе в двух экземплярах, имеющих одинаковую силу. Экземпляры Протокола хранятся у Стороны-1 и Стороны-2.
14. Сторона-2 и Сторона-1 признают решения Экспертной комиссии обязательными и обязуются добровольно их исполнять.
15. Протокол Экспертной комиссии является окончательным и пересмотру не подлежит. Действия, вытекающие из него, являются обязательными для участников конфликтной ситуации.
16. Протокол Экспертной комиссии является основанием для предъявления претензий к лицам, виновным в возникновении конфликта.
17. Протокол Экспертной комиссии может являться доказательством при дальнейшем разбирательстве конфликта в судебно-арбитражных органах.

Сторона-1:	Сторона-2:
ИНН: 2315190510	ИНН:
_____ Незамутдинов Р.Я.	_____ ФИО