УТВЕРЖДАЮ:

Председатель Правления

РНКО «Платежный Центр» (ООО)

Г.М.Мац

Редакция №4 от 19.07.2017

ПРАВИЛА РАБОТЫ СЕРВИСА

«Финансовые операции в торговых сетях»

Настоящие Правила работы сервиса «Финансовые операции в торговых сетях» (далее – «Правила», «Сервис») определяют правила работы Сервиса, порядок и условия его использования Участниками. Текст действующих Правил размещается в сети Интернет по адресу rnko.ru.

Присоединение Участника к условиям Правил осуществляется путём заключения с Организатором сервиса соглашения, согласно условиям которого Участник присоединяется к условиям настоящих Правил, либо путём подачи Организатору сервиса заявления на выдачу сертификата ключа проверки электронной подписи / заявки на регистрацию сертификата ключа проверки электронной подписи / заявки на получение Смарт-ключей. Участник приобретает все права и обязанности, предусмотренные Правилами, с даты вступления такого соглашения в силу, либо с даты принятия Организатором сервиса указанных заявок / заявлений.

Настоящие Правила действуют в рамках правил электронного документооборота корпоративной информационной системы «BeSafe» (далее – Система BeSafe), текст которых представлен в сети Интернет по адресу www.besafe.ru (далее – Правила BeSafe). Присоединение Участника к условиям настоящих Правил означает также присоединение Участника к Правилам BeSafe. Под Участником в настоящих Правилах понимается Клиент в терминах Правил BeSafe.

Присоединение Участника к условиям Правил возможно только в случае, если Участник полностью согласен с настоящими Правилами и Правилами BeSafe, условиями присоединения к Сервису и Системе BeSafe, удовлетворяет содержащимся в Правилах Сервиса и Правилах BeSafe критериям.

1. Предмет регулирования настоящих Правил

Предметом регулирования настоящих Правил является:

1.1. Определение основных принципов организации и проведения электронного документооборота между Участниками и Организатором сервиса (далее – Стороны) в рамках заключенных между ними договоров;

1.2. Установление прав, обязанностей и ответственности Сторон в результате указанной в п.1.1 Правил деятельности.

1.3. В связи с тем, что в рамках данных Правил Стороны действуют во исполнение заключенных между ними договоров, для достижения взаимных интересов, никаких дополнительных финансовых обязательств в результате исполнения прав и обязанностей, установленных данными Правилами, между Сторонами не возникает (если иное не предусмотрено настоящими Правилами).

2. Термины и определения

Владелец сертификата ключа проверки ЭП (Владелец сертификата) – физическое или юридическое лицо, на имя которого Удостоверяющим центром выдан Сертификат ключа проверки электронной подписи и которое владеет соответствующим Ключом ЭП.

Ключ электронной подписи (Ключ ЭП, Закрытый ключ) – последовательность символов, известная Владельцу сертификата и предназначенная для создания в Электронных документах Электронной подписи с использованием Средств ЭП, а также расшифровывания Электронных сообщений.

Ключ проверки электронной подписи (Ключ проверки ЭП, Открытый ключ) – последовательность символов, соответствующая Ключу ЭП, предназначенная для подтверждения (проверки) с использованием

Средств ЭП подлинности Электронной подписи в Электронном документе, а также зашифровывания Электронных сообщений, предназначенных владельцу Ключа электронной подписи.

Средства электронной подписи (Средства ЭП) - аппаратные и/или программные средства, являющиеся частью средств криптографической защиты информации и реализующие хотя бы одну из следующих функций при организации Электронного документооборота: создание Электронной подписи в Электронном документе с использованием Ключа ЭП; подтверждение подлинности Электронной подписи, содержащейся в Электронном документе, с использованием Ключа проверки ЭП; создание Ключей ЭП и Ключей проверки ЭП.

Сертификат ключа проверки электронной подписи (далее – Сертификат) - документ на бумажном носителе или Электронный документ с Электронной подписью уполномоченного лица Удостоверяющего центра, которые включают в себя Ключ проверки ЭП и которые выдаются Удостоверяющим центром участнику Сервиса для подтверждения подлинности ЭП и идентификации Владельца сертификата ключа проверки ЭП.

Смарт-ключ – компактное программно-аппаратное устройство, предназначенное для хранения Ключа проверки ЭП, Ключа ЭП, Сертификата, а также другой электронно-цифровой информации. Смарт-ключ имеет защищенную память, чтение записанных в память Смарт-ключа данных или копирование памяти Смарт-ключа невозможно.

Идентификация представителя Участника – аутентификация Участника с использованием соответствующего Сертификата ключа проверки электронной подписи при совершении операций, предусмотренных заключенными между Участником и Организатором сервиса договорами. Факт успешного прохождения Идентификации представителя Участника подтверждает, что указанные выше операции осуществляются Участником, а Участник при оспаривании операции лишается права ссылаться на то, что операция совершена лицом, не являющемся представителем Участника.

Организатор сервиса – Расчетная небанковская кредитная организация «Платежный Центр» (общество с ограниченной ответственностью), лицензия Банка России № 3166-К, имеющая в Системе BeSafe статус Организатора сервиса «Финансовые операции в торговых сетях» и осуществляющая в рамках Системы BeSafe и Сервиса функции информационного электронного обслуживания Участников, участвующих в работе Сервиса Организатора сервиса, привлечение Участников к работе в Системе BeSafe и Сервисе. В рамках Правил BeSafe Расчетная небанковская кредитная организация «Платежный Центр» (общество с ограниченной ответственностью) имеет также статус «**Агент Удостоверяющего Центра (далее – Агент УЦ)**, позволяющий организовывать выдачу Участникам Сертификатов, созданных Удостоверяющим Центром».

Удостоверяющий Центр - Удостоверяющий Центр AUTHORITY, созданный Закрытым акционерным обществом «Центр Цифровых Сертификатов», который осуществляет изготовление цифровых сертификатов для юридических и физических лиц для возможности осуществления электронного документооборота в рамках корпоративной информационной системы «BeSafe».

Сервис – сервис «Финансовые операции в торговых сетях», организованный Организатором сервиса в рамках Системы BeSafe, предназначенный для организации и осуществления Электронного документооборота и информационного обмена между Организатором сервиса и Участниками.

Электронный документооборот – обмен Электронными документами в рамках Сервиса в соответствии с настоящими Правилами.

Электронный документ (ЭД) – электронное сообщение, заверенное ЭП, в котором информация представлена в электронно-цифровой форме и соответствует установленному Организатором сервиса формату.

Электронная подпись (ЭП) – реквизит Электронного документа, предназначенный для защиты Электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием Ключа ЭП и позволяющий идентифицировать Владельца сертификата ключа проверки ЭП, а также установить отсутствие утраты, добавления, перестановки или искажения содержащейся в электронном документе информации. Используемые Электронные подписи признаются усиленными неквалифицированными электронными подписями в соответствии с законодательством РФ.

Шифрование – криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного ЭД.

Иные термины и определения, используемые в настоящих Правилах имеют значение, придаваемое им Правилами BeSafe.

3. Общие принципы электронного документооборота в рамках Сервиса

3.1. Все ЭД в рамках Сервиса проходят проверку принадлежности ЭП в ЭД уполномоченным лицам Сторон и отсутствия искажений в данном ЭД.

3.2. Электронный документооборот, а именно отправка, передача и получение ЭД между Сторонами осуществляется посредством электронных каналов связи, с использованием средств информационной системы Организатора сервиса (далее по тексту - Система) и/или адресов электронной почты. Если иные адреса

электронной почты не определены основными договорами между Участниками и Организатором сервиса для конкретных ЭД, Участники и Организатор сервиса принимают к обработке ЭД, подписанные ЭП уполномоченных лиц Сторон, направленные с использованием средств Системы и/или по адресам электронной почты, которые были предварительно указаны Сторонами в заявках, составленных по форме Приложения №3 настоящих Правил.

3.3. Участники и Организатор сервиса признают, что:

- внесение изменений в ЭД после его подписания ЭП дает отрицательный результат проверки ЭП;
- каждый Участник несет ответственность за сохранность Ключей ЭП/Закрытых ключей своих уполномоченных лиц и за действия своего персонала при работе в Системе и/или посредством электронных адресов электронной почты;
- моментом формирования ЭП принимается момент получения ЭД, подписанного ЭП, принимающей Стороной, отраженный в Электронном журнале Системы Организатора сервиса.
- Электронные документы юридически эквивалентны документам на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц с проставлением оттиска печати.

3.4. Для создания Ключей ЭП и Ключей проверки ЭП, подписания ЭД, проверки ЭП, зашифровывания и расшифровывания Электронных сообщений в Системе, а также в случаях передачи ЭД с использованием адресов электронной почты Участники используют только совместимые Средства криптографической защиты информации (далее – СКЗИ), и признают их достаточными для Подтверждения подлинности Электронной подписи в Электронном документе, для защиты от несанкционированного доступа, а также для обеспечения конфиденциальности, авторства и подлинности информации, содержащейся в пересылаемых ЭД. Список совместимых (разрешенных к использованию) СКЗИ представлен в Приложении №2 к Правилам «BeSafe».

3.5. Стороны принимают на себя все риски, связанные с работоспособностью своего оборудования, каналов связи, программного обеспечения, установленного на своих программно-аппаратных комплексах.

3.6. Стороны обязуются своевременно информировать друг друга обо всех случаях возникновения технических неисправностей или других обстоятельств, препятствующих обмену ЭД. В случае обнаружения возможных угроз безопасности ЭД Стороны обязуются своевременно извещать друг друга о них для принятия согласованных мер по защите.

3.7. Участники строго выполняют требования технической и эксплуатационной документации по системам защиты информации, обеспечивающие конфиденциальность, целостность и сохранность программных средств, ЭД, протоколов регистрации событий, действующей парольной и ключевой информации, используемой для доступа в Систему, кодирования данных и определения их авторства.

3.8. Участники организовывают внутренний режим функционирования рабочего места таким образом, чтобы исключить возможность использования Системы и/или адресов электронной почты лицами, не имеющими допуска к работе с ней, а также исключить возможность использования паролей доступа и Ключей ЭП не уполномоченными на то лицами.

3.9. Участники принимают необходимые меры для исключения обмена ЭД, содержащими компьютерные вирусы и/или иные вредоносные программы.

3.10. Участники признают в качестве единой шкалы времени время часового пояса г. Новосибирска. Участники обязуются поддерживать системное время аппаратных средств, обеспечивающих работоспособность Системы в соответствии с текущим астрономическим временем с точностью до пяти минут. При возникновении разногласий эталонным считается время, установленное на аппаратных средствах Организатора сервиса.

3.11. Участники организуют архивное хранение ЭД, подписанных ЭП, в течение срока действия аналогичных документов, оформленных на бумажных носителях.

4. Особенности Электронного документооборота в рамках Сервиса.

4.1. Порядок выдачи и регистрации Сертификата ключа проверки электронной подписи.

4.1.1. Уполномоченное лицо Участника самостоятельно изготавливает ключ электронной подписи, ключ проверки электронной подписи, сохраняя их в памяти своего персонального компьютера или на Смарт-ключах, и направляет Агенту УЦ заявление о создании Сертификата ключа проверки электронной подписи. Для этого уполномоченное лицо Участника, при необходимости, устанавливает требуемое программное обеспечение, заходит по ссылке https://secure.authority.ru/auth/1st_class.jsp?class=3&type=2&f=fin&agentId=1084, заполняет отображаемую форму Заявления на выдачу Сертификата ключа проверки электронной подписи и отправляет заявление. Заявление формируется в виде Электронного документа и направляется Агенту УЦ с использованием программно-аппаратных средств Участника, подключенных через каналы связи к программно-техническим средствам Агента УЦ. После отправки заявления в электронном виде, Участник направляет его Агенту УЦ в бумажном виде с собственноручной подписью уполномоченного лица Участника, действующего на основании учредительных документов (с заверением печатью Участника, если имеется) или доверенности (далее по тексту – уполномоченное лицо Участника), с приложением документов, подтверждающих личность и

полномочия уполномоченного лица Участника (в доверенности должны быть обязательно указаны ФИО и должность/паспортные данные уполномоченного лица; при указании должности одновременно с доверенностью должна быть представлена заверенная копия документа о назначении на должность с указанием паспортных данных).

4.1.2. В течение 3 (Трёх) дней с момента получения заявления в бумажном виде Агент УЦ направляет Участнику изготовленный Удостоверяющим Центром Сертификат в электронном виде, либо мотивированный отказ от его выдачи. Участник направляет Агенту УЦ Акт приёма-передачи Сертификата ключа проверки электронной подписи в бумажном виде за подписью уполномоченного лица Участника.

4.1.3. Создание Сертификата осуществляется Удостоверяющим центром в соответствии с Правилами работы Удостоверяющего Центра «AUTHORITY», размещенными на сайте www.authority.ru (далее – Правила Удостоверяющего Центра). Срок действия Сертификата – 1 (один) год.

4.1.4. После получения Сертификата Участник передает Организатору сервиса полученный Сертификат, который содержит в себе Ключ проверки электронной подписи.

4.1.5. Участник направляет Организатору сервиса в бумажном виде заявку о регистрации в Сервисе Сертификата ключа проверки электронной подписи в соответствующей роли (перечень ролей представлен в п.4.1.7. Правил). Заявка должна быть заполнена в строгом соответствии с утвержденными формами (Приложение №1 Правил) и подписана уполномоченным лицом Участника.

4.1.6. Сертификат может быть зарегистрирован в Сервисе только при условии получения Организатором сервиса всего пакета оригиналов документов на бумажном носителе и в надлежащей форме, а именно: Заявления на выдачу Сертификата, Акта приема-передачи Сертификата, Заявки на регистрацию Сертификата, доверенности, подтверждающей полномочия уполномоченных лиц Участника (при необходимости).

В исключительных случаях, а также при регистрации Сертификата в ролях, предусмотренных пп. 2) – 6) п.4.1.7. настоящих Правил, Организатор сервиса вправе зарегистрировать Сертификат в Сервисе на основании поступивших сканированных копий указанного пакета документов на условии поступления оригиналов документов течение 1 (одного) месяца с даты регистрации Сертификата. В случае непоступления оригиналов пакета документов, Организатор сервиса вправе заблокировать возможность использования Сертификата в Сервисе до поступления оригиналов. При этом Участник несет ответственность за все операции, совершенные с использованием Сертификата, зарегистрированного на основании поступивших сканированных копий, в любом случае.

4.1.7. Участник и соответствующий Сертификат ключа проверки электронной подписи регистрируется в одной или нескольких из представленных ролей:

1) уполномоченный работник Участника (сертификат Агента);
2) оператор точки обслуживания;
3) бухгалтер;администратор ключей точки обслуживания;
4) оператор информационного центра;
5) аудитор безопасности;
6) уполномоченное лицо по получению сертификатов

4.1.8. До истечения срока действия Сертификата уполномоченное лицо Участника должно изготовить и получить новые: Ключ электронной подписи, Ключ проверки электронной подписи и Сертификат ключа проверки электронной подписи в порядке, установленном п. 4.1.1 настоящих Правил, за исключением следующего: уполномоченное лицо Участника заходит по ссылке https://secure.authority.ru/auth/renew.jsp?agentId=1084 и не направляет Агенту УЦ Заявление на выдачу Сертификата ключа проверки электронной подписи, Акта приёма-передачи Сертификата ключа проверки электронной подписи и Заявки на регистрацию Сертификата ключа проверки электронной подписи в бумажном виде, вместо этого, Участник подтверждает свое заявление, акт приёма-передачи и заявку в электронном виде действующим Сертификатом ключа проверки электронной подписи.

4.1.9. Участник несет полную ответственность по всем операциям, подтвержденным любым Сертификатом Участника, вне зависимости от зарегистрированной для соответствующего Сертификата роли.

4.1.10. Организатор сервиса получает и регистрирует Сертификаты на свое имя в том же порядке, что предусмотрен настоящими Правилами для Участника.

4.1.11. В случае, если Участник является Владельцем Сертификата ключа проверки электронной подписи, зарегистрированного в рамках настоящих Правил в роли «уполномоченное лицо на получение

сертификатов», указанные в пункте 4.1 Правил документы Участник вправе направлять в виде Электронных документов, подписанных соответствующей Электронной подписью Участника. Такие Электронные документы юридически эквивалентны документам на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц с проставлением оттиска печати Участника. Организатор сервиса / Агент УЦ / УЦ вправе отказать любому Участнику в выдаче и регистрации Сертификата ключа проверки электронной подписи в роли «уполномоченное лицо по получению сертификатов» по своему усмотрению.

4.2. Допускается регистрировать также Сертификат, ранее полученный в рамках Системы BeSafe.

4.3. Участник обязуется обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование кем-либо принадлежащих Участнику ключей электронных подписей без его согласия. При компрометации/аннулировании (отзыве) Ключа электронной подписи Участник обязан незамедлительно сформировать и направить Организатору сервиса уведомление о компрометации/аннулировании Ключа электронной подписи в соответствии с утвержденной в Приложении №3 Правил формой в электронном виде на адрес https://jira.korona.net с последующей отправкой в бумажном виде. В течение 24 (Двадцати четырёх) часов с даты получения уведомления в электронном виде Организатор сервиса блокирует Сертификат, однозначно связанный со скомпрометированным Ключом электронной подписи в Сервисе. До момента блокировки Сертификата в Сервисе Электронные документы, направленные с использованием скомпрометированного Ключа электронной подписи, считаются направленными Участником и Участник несет всю полноту ответственности за совершенные с использованием такого Сертификата действия.

4.4. Стороны подтверждают, что настоящие Правила также являются надлежащим письменным уполномочием (имеющим силу доверенности в силу ч.4 ст.185 ГК РФ), выданным Участником уполномоченному лицу Участника, получившему и зарегистрировавшему от имени Участника Сертификат ключа проверки электронной подписи в соответствии с п.4.1. Правил, на совершение с использованием такого Сертификата любых действий, предусмотренных договорами между Участником и Организатором сервиса, от имени Участника, в течение всего срока действия Сертификата. Стороны договорились распространить действие настоящего пункта Правил на отношения Сторон, возникшие с момента присоединения Участника к Правилам.

4.5. При изменении данных Участника, данных уполномоченного лица Участника, отзыва доверенности на имя уполномоченного лица Участника, Участник обязуется направить Организатору сервиса уведомление об аннулировании Ключа электронной подписи в порядке, предусмотренном п.4.3 Правил.

4.6. Удостоверяющий Центр, Организатор сервиса (Агент УЦ) не несут ответственности за несанкционированное использование Сертификатов, а также за ущерб, причиненный Участнику или уполномоченному лицу Участника таким использованием.

4.7. В рамках настоящих Правил Электронные документы признаются полученными с момента получения Электронного документа получателем Электронного документа.

4.8. В рамках настоящих Правил действуют Сертификаты ключей электронной подписи Класса 2 и Класса 3.

4.9. В рамках настоящих Правил Участник не вправе осуществлять отзыв отправленных Электронных документов.

5. Дополнительные положения, действующие самостоятельно, вне Правил Системы Besafe.

5.1. Для доступа Участника к Системе Организатора сервиса в рамках заключенного между Участником и Организатором сервиса основного договора и работы в ней, а также для создания и подтверждения запросов и сообщений, не требующих подписания Электронной подписью, Участник получает Технологический сертификат либо Пароль в следующем порядке:

Для получения Технологического сертификата (сертификата точки обслуживания Участника) Участник оформляет заявление по ссылке https://www.authority.ru/auth/1st_class.jsp?class=5&type=2&f=fin&agentId=3802. Сертификат точки обслуживания Участника является технологическим сертификатом, создаваемым в соответствии с Правилами Удостоверяющего Центра. Заявление формируется в виде Электронного документа и направляется Агенту УЦ. После отправки заявления в электронном виде Участник направляет его Агенту УЦ в бумажном виде с собственноручной подписью уполномоченного лица Участника, с приложением документов, подтверждающих личность и полномочия уполномоченного лица Участника.

5.1.1. В течение 3 (Трёх) дней с момента получения заявления в бумажном виде Агент УЦ направляет Участнику изготовленный Удостоверяющим Центром Сертификат в электронном виде, либо мотивированный отказ от его выдачи. Участник направляет Агенту УЦ акт приёма-передачи Сертификата в бумажном виде за

подписью уполномоченного лица Участника. Участник регистрирует указанный сертификат в Сервисе, направив заявку в бумажном виде (форма представлена в Приложении №3 к настоящим Правилам) Организатору сервиса.

5.1.2. Для получения Пароля Участник направляет посредством средств Системы Организатора сервиса запрос на получение Пароля. Пароль – набор символов, состоящий из двух частей, сгенерированный в Системе Организатора и единый для всех точек обслуживания Участника. Срок действия Пароля составляет 2 (два) года.

5.2. Выдача и регистрация сертификатов точки обслуживания Участника может также происходить путем формирования сотрудником Участника, зарегистрированным в роли «Администратор ключей точки обслуживания» соответствующих заявлений. «Администратор ключей точки обслуживания», используя АРМ «Администратор», создает и подписывает заявление на получение сертификата точки обслуживания Участника своей электронной подписью. После получения Сертификата точки обслуживания Участника «Администратор ключей точки обслуживания» формирует заявление на регистрацию сертификата точки обслуживания Участника.

5.3. Участник регистрирует у Организатора Сервиса свои точки обслуживания, в которых осуществляется Электронный документооборот, путем направления заявки на регистрацию точек обслуживания Участника по форме Приложения №5 к настоящим Правилам. Регистрация точек обслуживания Участника может также происходить путем формирования сотрудником Участника, зарегистрированным в роли «Администратор ключей точки обслуживания» соответствующего заявления, используя АРМ «Администратор» и подписывая заявление на регистрацию точки обслуживания Участника своей электронной подписью.

5.4. В согласованных с Организатором сервиса случаях Участнику необходимо получить Смарт-ключи в целях работы по настоящим Правилам.

Получить Смарт-ключи Участник может в Удостоверяющем центре на основании заключенного между ними договора, текст которого размещен в сети Интернет по адресу rnko.ru в виде документа «Условия поставки USB-ключей «MS_Key K» для Участников РНКО «Платежный Центр» (ООО)».

Организатор сервиса вправе принимать от Участника заявки на поставку Смарт-ключей, выдаваемых Удостоверяющим центром, по почтовому адресу РНКО «Платежный Центр» (ООО), в целях передачи указанных заявок Удостоверяющему Центру.

Организатор сервиса вправе отказать Участнику в принятии заявки на передачу Смарт-ключей без объяснения причин.

Учитывая, что получение Участником Смарт-ключей осуществляется им в целях исполнения своих обязательств по агентскому договору с Организатором сервиса, Организатор сервиса обязуется возмещать расходы, понесенные Участником на получение Смарт-ключей. Для возмещения расходов Участник предоставляет Организатору сервиса счет на оплату с приложением следующих документов:

1. Заверенной копии заявки на передачу Смарт-ключей,
2. Заверенной копии акта приема-передачи Смарт-ключей,
3. Заверенной копии платежного поручения на оплату Смарт-ключей

6. Порядок внесения изменений и дополнений в настоящие Правила.

6.1. Настоящие Правила утверждаются Организатором сервиса. Изменения в Правила вносятся Организатором сервиса в одностороннем порядке путём размещения новой редакции Правил на сайте www.besafe.ru и www.rnko.ru не позднее, чем за 15 (Пятнадцать) календарных дней до даты вступления в силу новой редакции Правил.

7. Переходные положения.

7.1. Заявки, оформленные Участником по формам, представленным в приложениях к настоящим Правилам до даты вступления в силу действующей редакции Правил, считаются надлежащими, создающими соответствующие права и обязанности в рамках действующих Правил.