Утвержден
Генеральным директор ООО «ЭКС»
О.И. Лагуткин
Приказ №55 от «11» апреля 2017г.

Приложение №2 к Договору об оказании информационных услуг (договор присоединения)
№ _____ от _____
(далее – Договор)

Регламент электронного взаимодействия

Термины и определения

В настоящем Регламенте используются следующие термины и определения:
База данных – специальным образом структурированная электронная база данных Бюро, хранящая кредитные истории Субъектов кредитной истории;
Система – автоматизированная система с помощью которой осуществляется доступ в Базу данных;
Доступ к Базе данных – формирование запросов на получение кредитного отчета;
Администратор Партнера - сотрудник Партнера, на которого возложена ответственность за взаимодействие с Бюро и контролю над операторами Партнера;
Оператор Партнера –сотрудник Партнера, на которого возложена функция направления запросов в Бюро на получение кредитных отчетов.
Безопасность информации (информационная безопасность)
1) состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.
2) состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз;
СКЗИ – средства криптографической защиты информации;
Ключ (Криптографический ключ) - конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований;
Ключевой носитель – любой электронный носитель информации, на котором хранится секретный ключ;
Компрометация ключа – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но, не ограничиваясь, следующие: утрата ключевых носителей; утрата ключевых носителей с последующим обнаружением; увольнение сотрудников, имевших доступ к ключевой информации; нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа; возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи; нарушение печати на сейфе с ключевыми дискетами; случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда магнитный носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).
Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
Программное обеспечение (ПО) - совокупность данных, команд, предназначенных для функционирования ЭВМ.

1. Общие положения

1.1. Регламент описывает взаимодействия сторон в целях организации безопасной передачи электронных документов, подписанных электронной подписью, между Сторонами в рамках, определенных Договором об оказании информационных услуг, заключенным между Сторонами во исполнение Федерального Закона от 30 декабря 2004 г. №218 ФЗ «О кредитных историях» (далее – Договор), и устанавливает обязательства Сторон по обеспечению информационной безопасности при обмене электронными документами.
1.2. Термины, применяемые в настоящем Регламенте, соответствуют определениям, используемым в Федеральном Законе «Об электронной подписи» № 63-ФЗ от 06.04.2011. Стороны признают, что методы и системы защиты информации, шифрования, используемые между Сторонами в соответствии с настоящим Регламентом достаточны для обеспечения конфиденциальности, подтверждения целостности передаваемых сообщений, подлинности авторства, а также разбора конфликтных ситуаций по ним. Стороны принимают к использованию для осуществления электронной передачи документов в Системе программное средство криптографической защиты, сертифицированное ФСБ России.
1.3. Для электронного взаимодействия стороны используют усиленную неквалифицированную электронную подпись. В случаях, если в договорах и иных документах между Сторонами используется термин «электронно-цифровая подпись» или «электронная подпись», под ним подразумевается усиленная неквалифицированная электронная подпись.
1.4. Стороны признают, что используемые во взаимоотношениях между Бюро и Партнером электронные документы, заверенные действующей на момент передачи Электронной подписью отправителя, подготовленные и переданные с помощью программного обеспечения Системы в соответствии со всеми процедурами защиты информации, предусмотренными Регламентом и эксплуатационной документацией на средства криптографической защиты информации (СКЗИ), юридически эквивалентны документам на бумажном носителе, подписанным уполномоченным лицом организации-отправителя с проставлением печати, имеет равную с ними юридическую силу и порождает для Сторон аналогичные права и обязанности.
1.5. Стороны признают, что применение усиленной неквалифицированной электронной подписи Партнера, а также усиленной неквалифицированной электронной подписи Бюро является безусловным доказательством того, что электронный документ действительно исходит от соответствующей стороны и сформирован (подписан) уполномоченным лицом и не претерпел изменений при информационном взаимодействии Сторон.

1.6. Персональные адреса, идентификационные пароли, регистрационные номера, пароли и криптографические ключи обеих сторон, используемые для разграничения доступа, передачи и защиты информации, а также материалы разбора конфликтных ситуаций являются конфиденциальной информацией и не подлежат разглашению Сторонами.

1.7. Удостоверяющим центром при обмене электронными документами между Сторонами является Удостоверяющий Центр e-Notary ЗАО «Сигнал-КОМ». Стороны в своих действиях, осуществляемых в рамках данного Регламента, руководствуются Регламентом Удостоверяющего Центра e-Notary ЗАО «Сигнал-КОМ».

2. Программное обеспечение для взаимодействия с Бюро

2.1. Для обеспечения безопасного соединения Стороны организуют защищенное VPN соединение между программными средствами Партнера и Системы Бюро через сеть Интернет.

2.2. Стороны соглашаются, что средствами безопасного соединения являются программное обеспечение: **«EquifaxVPN Client» «EquifaxVPN VM Universal»**.

2.3. Требования по установке ПО «EquifaxVPN Client»:

2.3.1. Для подключения через версию EquifaxVPN Client, Партнер выделяет рабочую станцию.

2.3.2. Минимальные технические требования для запуска и работы ПО «EquifaxVPN Client»:

- 1 процессор (1 ядро);
- 256 Мбайт оперативной памяти;
- Жесткий диск (не менее 1 GB).

2.4. Требования по установке ПО «EquifaxVPN VM Universal»

2.4.1. Для подключения Партнер выделяет один адрес из своей внутренней сети и адрес шлюза для выхода в сеть Интернет. Эти параметры используются для предварительной настройки загрузочного образа.

2.4.2. Минимальные технические требования для запуска и работы ПО «EquifaxVPN VM Universal»:

- 1 процессор (1 ядро);
- 256 Мбайт оперативной памяти;
- 1 сетевой интерфейс;
- Жесткий диск не требуется, загрузка образа возможна с CD или FLASH-накопителя, или локального хранилища платформы виртуализации.

2.4.3. Далее образ передается Партнеру для запуска на своей платформе виртуализации. Все функции трансляции адресов реализованы средствами ПО «EquifaxVPN VM Universal» и дополнительных настроек со стороны Партнера не требуются.

2.4.4. В зависимости от выбранной Партнером схемы подключения может выделяться несколько адресов из его внутренней сети, в случае если планируется использовать схему из двух и более виртуальных машин для повышения отказоустойчивости, и резервирования каналов связи балансировки нагрузки.

2.4.5. Варианты схем подключения Партнера к Системе Бюро согласовываются отдельно со службой технической поддержки Бюро.

2.5. Сертификат защищенного соединения (VPN) действителен 1 (один) год.

3. Порядок подключения и работы Партнера в Системе Бюро

3.1. Партнер предоставляет Бюро заявку на подключение к Системе Приложение №1. При подключении Партнера к Системе Бюро в заявке необходимо указать номер мобильного телефона Администратора Партнера.

3.2. На основании полученных данных из заявки на подключение Партнера, Бюро формирует образ выбранного ПО и отправляет ссылку для его скачивания на адрес Администратора Партнера с подробной инструкцией.

3.3. Подробные инструкции Администратора Партнера и Оператора Партнера изложены в соответствующих документах и предоставляются по запросу в службу технической поддержки Бюро.

3.4. Для добавления/блокировки Администратора Системы Партнеру необходимо направить в Бюро заявление, форма которого приведена в Приложении №5.

3.5. Для изменения данных Администратора Системы Партнеру необходимо направить в Бюро заявление, форма которого приведена в Приложении №6. Добавление/блокировка и изменение данных Администраторов Партнера при этом осуществляется Администратором Бюро.

3.6. Администратор Партнера, не направляя в Бюро указанные заявления, выполняет действия по добавлению/блокировке или изменению данных Операторов Партнера самостоятельно (см. пп. 4.5 настоящего Регламента).

4. Формирование ключей шифрования и электронной подписи

4.1. Полномочия лиц, осуществляющих формирование индивидуальной ключевой информации и сертификацию открытых ключей, определяются на основании Доверенностей, форма которой приведена в Приложении №2.

4.2. Формирование ключей шифрования и ЭП Партнера осуществляется на автоматизированном рабочем месте Администратора Партнера при помощи программного обеспечения СКЗИ Admin-PKI или КриптоАРМ (при использовании КриптоПро CSP, версии 3.6 и выше компании «КРИПТО-ПРО»). Инструкции по ПО Admin-PKI или КриптоАРМ приведены в отдельных документах, высылаемых Партнеру по запросу в службу технической поддержки Бюро.

4.3. Регистрационная карточка запроса на сертификат открытого ключа шифрования и ЭП распечатывается в двух экземплярах и заверяется подписью и печатью уполномоченного лица Партнера, один экземпляр хранится у Партнера, второй высылается в Бюро. В карточке запроса необходимо указать *код запроса,* который сгенерировало используемое ПО СКЗИ. Форма регистрационной карточки запроса на сертификат открытого ключа шифрования и ЭП приведена в Приложении №3 Регламента. При использовании Партнером Admin-PKI регистрационная карточка может быть сформирована с помощью данного программного обеспечения (см.пп 4.5 настоящего Регламента).

4.4. Бюро передает Партнеру сертификат, выданный Удостоверяющим Центром e-Notary ЗАО «Сигнал-КОМ».

4.5. Для отзыва сертификата открытого ключа шифрования и ЭП Партнеру необходимо направить в адрес службы технической поддержки Бюро заявление на отзыв сертификата, форма которого приведена в Приложении №4.

4.6. Партнер, при необходимости совместно со службой технической поддержки Бюро, проводит установку и настройку необходимого для подключения к Системе ПО.

5. Правила формирования файлов кредитных историй для передачи в Бюро

5.1. Партнеру предоставляется возможность передавать файлы содержащие кредитные истории в Бюро следующими способами:
- в формате b2b;
- Через web-интерфейс.

5.2. Порядок передачи и описания форматов взаимодействия приведены в отдельных документах, высылаемых Партнеру по запросу в службу технической поддержки Бюро.

6. Порядок формирования запросов для запроса кредитной истории

6.1. Партнеру предоставляется возможность осуществлять запросы в Бюро следующими способами:
- в формате b2b;
- Через web-интерфейс.

6.2. Все инструкции и описания форматов приведены в отдельных документах, высылаемых Партнеру по запросу в службу технической поддержки Бюро.

7. Права и обязанности Сторон

7.1. Права и обязанности Партнера

7.1.1. Партнер обязуется использовать только предоставленные СКЗИ в Системе без права их продажи или передачи каким-либо другим способом иным физическим или юридическим лицам, обеспечивать возможность контроля со стороны федеральных органов за соблюдением требований и условий осуществления лицензионной деятельности.

7.1.2. Партнер назначает своих ответственных должностных лиц, имеющих право работать с Системой, с указанием их полномочий и срока действия таких полномочий.

7.1.3. Партнер обязуется выдавать доверенность лицам, уполномоченным Партнером для обмена электронными документами в рамках электронного взаимодействия с Системой, и предоставить их в Бюро либо предоставить документы, подтверждающие правомочия лица выступать от имени Партнера без доверенности. Партнер обязан самостоятельно следить за изменениями и истечением срока полномочий, указанных в настоящем пункте лиц, своевременно информировать Бюро об этих изменениях в письменном виде предоставлять новые документы по истечении срока действия предыдущих. При этом отслеживание актуальности полномочий является исключительно обязанностью Партнера и не влечет обязанности Бюро требовать соответствующие подтверждающие документы, а также не принимать или не приостанавливать прием электронных документов до поступления таких документов.
Риск неправомерного подписания электронного документа третьими лицами с использованием электронной подписи Партнера несет Партнер, которому принадлежит электронная подпись. Бюро не несет ответственности перед Стороной в случае неправомерного подписания электронного документа третьими лицами и с использованием электронной подписи Партнера.

7.1.4. Партнер обязуется использовать ключи электронной подписи исключительно для электронного взаимодействия с Системой в соответствии с Регламентом электронного взаимодействия, и прекратить их использование в случае прекращения действия соответствующих договоров. Ответственность за использование ключей электронной подписи в иных целях лежит на Партнере.

7.1.5. Партнер обеспечивает доработку своей автоматизированной системы для организации безопасного взаимодействия с Бюро.

7.1.6. Партнер обязан:
- Соблюдать положения документов, регламентирующих функционирование Системы со встроенными средствами криптографической защиты информации.
- Эксплуатировать сертифицированные средства криптографической защиты информации в соответствии с условиями сертификатов на данные средства.
- Выполнять условия и требования эксплуатационной документации на средства криптографической защиты информации.
- Допускать к эксплуатации СКЗИ только уполномоченных сотрудников, прошедших необходимую подготовку по применению данных средств и допущенных к работе с ними на основании приказа Партнера, обеспечить персонализацию выдачи и внутреннего учета логинов, используемых ответственными сотрудниками по работе с Бюро.
- следовать рекомендациям Бюро в отношении информационной безопасности.
- Обеспечивать сохранность и целостность программного обеспечения Системы.
- Сохранять конфиденциальность и подлинность своих секретных ключей и паролей.
- Нести риск последствий, вызванных нарушением конфиденциальности и подлинности ключей и паролей.
- Извещать Бюро обо всех случаях компрометации криптографических ключей Партнера.
- Письменно уведомить Бюро о необходимости замены ключа СКЗИ.
- обеспечить эксплуатацию автоматизированных рабочих мест, подключенных к Системе, в соответствии с инструкциями Бюро.
- Размещать автоматизированные рабочие места, подключенные к системе, в охраняемом помещении, оборудованной системой охранной сигнализации, исключающей доступ в помещение посторонних лиц.
- Хранить носители с криптографическими ключами в металлических шкафах (сейфах), исключающих несанкционированный доступ к ним посторонних лиц.
- Оборудовать системные блоки компьютеров автоматизированных рабочих мест средствами защиты от несанкционированного вскрытия.
- Учитывать криптографические ключи и их носители в выделенных для этих целей журналах.

7.2. Права и обязанности Бюро

7.2.1. Бюро назначает ответственных должностных лиц, имеющих право обслуживать аппаратно-программные средства Системы, а также устанавливать и обслуживать ПО СКЗИ у Партнера.

7.2.2. Бюро обязано:
- Обеспечить не позднее согласованных с Партнером сроков установку СКЗИ и подключение вычислительных комплексов Партнера к Системе.
- Сохранять конфиденциальность и подлинность используемых секретных ключей и паролей.

- Протоколировать все случаи и попытки нарушения безопасности Системы. При возникновении таких случаев принимать все возможные меры для предотвращения и/или ликвидации их последствий вплоть до приостановления функционирования Системы.
- В случае компрометации криптографических ключей Партнера заблокировать открытые криптографические ключи Партнера до завершения внеплановой смены криптографических ключей.
- Своевременно информировать Партнера об изменениях порядка осуществления приема/передачи электронных документов и другой информации по Системе. Оказывать консультационные услуги Партнеру по вопросам функционирования Системы и использования СКЗИ.
- Соблюдать положения документов, регламентирующих функционирование Системы.
- За один календарный месяц до истечения срока действия сертификата направить клиенту электронное письмо с напоминанием о скором истечении срока действия сертификата.

7.2.3. Стороны обязуются обеспечить условия сохранения ключевых носителей и условия хранения и использования программного обеспечения СКЗИ, исключающие порчу и утрату ключевых носителей, а также их использование любыми другими лицами.

8. Порядок действий при компрометации ключей

8.1. Сторона, допустившая утрату ключевого носителя с ключевой информацией СКЗИ, независимо от наличия или отсутствия сведений о ее несанкционированном использовании, незамедлительно сообщает об этом другой Стороне и прекращает работу с использованием СКЗИ до момента регистрации и ввода в действие новых ключей. Вышедший из-под контроля ключевой носитель может использоваться в дальнейшем только после применения к нему операции форматирования.

8.2. Сторона, допустившая порчу или утрату ключевых носителей незамедлительно сообщает об этом другой Стороне и прекращает работу с использованием СКЗИ до момента приобретения новых ключевых носителей, регистрации и ввода в действие новых ключей.

9. Порядок действий при разрешении спорных ситуаций, связанных с подлинностью электронных документов

9.1. При возникновении спорных ситуаций между Сторонами, связанными с подлинностью электронных документов, несогласная Сторона должна в течение 3 рабочих дней направить другой Стороне письменное заявление, в котором должны быть изложены ее претензии.

9.2. Не позднее 10 рабочих дней со дня получения другой Стороной заявления Бюро созывает согласительную экспертную комиссию (далее – Комиссия).

9.3. Состав Комиссии формируется из двух представителей каждой из Сторон, и, в случае требования Сторон, представителя ЗАО «Сигнал-КОМ».

9.4. Комиссия по договоренности Сторон работает на территории одной из Сторон, либо в помещении Удостоверяющего Центра e-Notary ЗАО «Сигнал-КОМ», и на его компьютерном оборудовании. При этом конфигурация компьютерного оборудования соответствует установленным требованиям ЗАО «Сигнал-КОМ».

9.5. Экспертиза оспариваемого электронного документа осуществляется в присутствии всех членов Комиссии. Экспертиза осуществляется в три этапа:

9.5.1. Подготовка оборудования и программного обеспечения, тестирование их работоспособности.

9.5.2. Контроль целостности оспариваемого электронного документа путем проверки электронной подписи при помощи сертификата ключа проверки электронной подписи, предоставленного Стороной-заявителем.

9.5.3. Аутентификация отправителя оспариваемого электронного документа путем проверки принадлежности, актуальности и целостности сертификата ключа проверки электронной подписи, использованного экспертной комиссией для проверки электронной подписи.

9.6. Подтверждением подлинности оспариваемого электронного документа является единовременное выполнение следующих условий:

9.6.1. Проверка электронной подписи оспариваемого электронного документа на сертификате ключа проверки подписи, файл которого предъявлен Стороной-заявителем, дала положительный результат.

9.6.2. Подтверждена принадлежность, актуальность и целостность сертификата ключа проверки подписи Стороны-заявителя, с помощью которого проводится проверка электронной подписи оспариваемого электронного документа.

9.7. Результаты экспертизы в течение 3 рабочих дней оформляются в виде письменного заключения – Акта экспертной комиссии, подписываемого всеми членами Комиссии. Акт составляется в двух экземплярах, по одному для каждой Стороны. Акт является окончательным и пересмотру не подлежит.
Акт, составленный экспертной комиссией, является доказательством при дальнейшем разбирательстве спора в суде.

10. Порядок внесения изменений и расторжения Договора

10.1. Внесение изменений и дополнений в настоящий Регламент, в том числе во все приложения к нему, производится Бюро в одностороннем порядке.

10.2. При изменении положений Регламента Бюро обязано не менее чем за 30 (календарных) дней до вступления изменений в силу поместить новую редакцию Регламента на Интернет-сервер Бюро www.equifax.ru;

10.3. Изменения вступают в силу по истечении 30 (тридцати) календарных дней с даты размещения новой редакции Регламента на Интернет-сервере www.equifax.ru. Любые изменения и дополнения с момента вступления в силу равно распространяются на всех лиц, заключивших с Бюро Договор, в том числе и ранее даты вступления изменений в силу.

Список приложений

Приложение №1. Заявка на подключение к автоматизированной системе (Easy Connect).
Приложение №2. Доверенность.
Приложение №3. Регистрационная карточка запроса на сертификат открытого ключа шифрования и ЭП.

Приложение №4. Заявление на отзыв сертификата шифрования и ЭП.
Приложение №5. Заявление на добавление/блокировку пользователей.
Приложение №6. Заявление на изменение данных пользователя.

Приложение №1
ОБРАЗЕЦ

Генеральному директору
ООО «ЭКС»

Лагуткину О.И.

Заявка на подключение к автоматизированной системе Общества с ограниченной ответственностью «Эквифакс Кредит Сервисиз»

Настоящим Заявлением _____
(наименование организации для юридического лица
_____
или ИП ФИО индивидуального предпринимателя)
в лице _____,
(должность и ФИО руководителя или ФИО индивидуального предпринимателя)
действующего на основании _____,
(устава или доверенности (номер и дата) для юридического лица
_____
или свидетельства (номер и дата) о регистрации в качестве индивидуального предпринимателя)
выражает намерение установить программное обеспечение с использованием криптографической защиты информации (СКЗИ) и подключиться к Системе Общества с ограниченной ответственностью «Эквифакс Кредит Сервисиз».
Оборудование и помещения, предназначенные для установки программного обеспечения Системы с встроенными средствами криптографической защиты информации (СКЗИ), удовлетворяют техническим требованиям необходимым для поддержания информационной безопасности.

Ответственными лицами назначены:
По техническим вопросам (ФИО, e-mail, телефон): _____
По вопросам выгрузки данных в БКИ (ФИО, e-mail, телефон): _____
По вопросам корректировок кредитных историй (ФИО, e-mail, телефон): _____
Администратор Партнера:
Администратор Партнера выполняет функции управления учетными записями Операторов (создание, блокирование, разблокирование и редактирование) и составления статистики по запросам

Фамилия Имя Отчество	
e-mail	
мобильный телефон	

Выбранное программное обеспечение	**Кол-во экземпляров**
«EquifaxVPN Client»	
«EquifaxVPN VM Universal»	

Данные Партнера – юридического лица (ЮЛ)

Полное наименование юридического лица	
Сокращенное наименование юридического лица	
Фирменное наименование юридического лица (торговая марка, брэнд)	
Адрес веб-сайта	
Наименование юр/лица на одном из языков РФ	
Признак резидентства	
Наименование юр. лица на иностранном языке	
ОКПО	
Адрес	
Номера телефонов	
ОГРН	
ИНН/КПП	
Способ передачи в Бюро кредитных историй	☐ выгрузка кредитных историй на FTP-сервер ☐ с помощью web-интерфейса

Данные Партнера – индивидуального предпринимателя (ИП)

Фамилия Имя *Отчество (при наличии отчества)*	
Признак резидентства	
Адрес фактический	
Номера телефонов	
ОГРНИП	
ИНН	

Данные сетевых настроек Партнеров, приобретающих «EquifaxVPN VM Universal»

Внутренний IP-адрес, выделенный для «EquifaxVPN VM Universal»	
Маска подсети локального IP-адреса	
IP-адрес шлюза для выхода в Интернет	

Данные для доступа

Тестовая среда	10.130.1.2
Продуктивная среда	10.130.10.130

***Все поля обязательны для заполнения,** *кроме полей, выделенных курсивным шрифтом*

Должность _____ Подпись _____ Фамилия и инициалы _____

«___» _____201_ г.

МП (оттиск должен быть получен той же печатью, что и оттиск печати на договоре/соглашении)

Приложение №2
ОБРАЗЕЦ

ДОВЕРЕННОСТЬ

г. Москва «_____» _____20__ г.

_____
(полное наименование юридического лица, ОГРН, ИНН - Партнера)

_____
(с указанием местонахождения)
в лице

_____
(должность, фамилия, имя, отчество)

действующего на основании _____

ДОВЕРЯЕТ

_____
(должность, фамилия, имя, отчество)

_____
(паспортные данные)

формировать и подписывать электронной подписью (ЭП) файлы с кредитными историями, запросы на получение кредитных отчетов, а также формировать ключи электронной подписи и получать ключи шифрования на автоматизированном рабочем месте Администратора Партнера и выполнять все необходимые процедуры по получению сертификатов ключей проверки электронной подписи и шифрованию, в том числе подписывать Акты формирования, передачи и получения сертификатов ключей электронной подписи.

Срок доверенности - _____ (до трех лет).

Подпись доверенного лица_____ удостоверяю.

Должность _____ ФИО _____

Подпись _____

МП (оттиск должен быть получен той же печатью, что и оттиск печати на договоре/соглашении)

Приложение №3

Генеральному директору
ООО «ЭКС»
О.И. Лагуткину

« ___ » _____ 20__ г.

Регистрационная карточка запроса на сертификат открытого ключа шифрования и ЭП

[Вставьте в данное поле криптографическую последовательность запроса: откройте файл запроса *.pem, скопируйте содержимое файла и вставьте в данное поле]

Полное наименование юридического лица: _____ "_____" (далее - Партнер) в лице _____ (далее - Ответственное лицо Партнера), действующего на основании _____.

Должность владельца сертификата:
_____

ФИО владельца сертификата:
_____

Подпись владельца сертификата
_____

Подпись ответственного лица Партнера _____ Расшифровка подписи _____

МП (оттиск должен быть получен той же печатью, что и оттиск печати на договоре/соглашении)

Приложение №4

Генеральному директору
ООО «ЭКС»
О.И. Лагуткину

Заявление на отзыв сертификата шифрования и ЭП

Настоящим Заявлением _____*(наименование организации)*_____в лице_____ _____, действующего на основании _____, выражает намерение отозвать сертификат(ы):

1. Серийный номер сертификата или Ф.И.О., если сертификат выписан на конкретного сотрудника организации
2. Серийный номер сертификата или Ф.И.О., если сертификат выписан на конкретного сотрудника организации
3. Серийный номер сертификата или Ф.И.О., если сертификат выписан на конкретного сотрудника организации

Должность	Подпись	Фамилия и инициалы
_____	_____	_____

«___» _____20 __ г. МП (оттиск должен быть получен той же печатью, что и оттиск печати на договоре/соглашении)

Приложение №5

Генеральному директору
ООО «ЭКС»
О.И. Лагуткину

Заявление на добавление/блокировку пользователей

Настоящим Заявлением _____*(наименование организации)*_____
в лице_____, действующего на основании _____, выражает намерение _____*(добавить/заблокировать)*_____ пользователей в Систему ООО «ЭКС»:

Пользователь 1

Фамилия Имя Отчество	
E-mail	
Мобильный телефон	
Роль (*нужное подчеркнуть*)	*Администратор / Администратор FTP*

Пользователь 2

Фамилия Имя Отчество	
E-mail	
Мобильный телефон	
Роль (*нужное подчеркнуть*)	*Администратор / Администратор FTP*

Пользователь 3

Фамилия Имя Отчество	
E-mail	
Мобильный телефон	
Роль (*нужное подчеркнуть*)	*Администратор / Администратор FTP*

Должность _____ Подпись _____ Фамилия и инициалы _____

«____» _____20_ г. МП (оттиск должен быть получен той же печатью, что и оттиск печати на договоре/соглашении)

Приложение №6

Генеральному директору
ООО «ЭКС»
О.И. Лагуткину

Заявление на изменение данных пользователя

Настоящим Заявлением _____*(наименование организации)*_____
в лице_____, действующего на основании _____, выражает намерение изменить данные пользователя в Системе ООО «ЭКС»:

	Старые данные	**Новые данные**
Логин		
Фамилия Имя Отчество		
E-mail		
Мобильный телефон		

Должность _____ Подпись _____ Фамилия и инициалы _____

«___» _____ 201 __ г. МП (оттиск должен быть получен той же печатью, что и оттиск печати на договоре/соглашении)