Приложение 3 к приказу № 503/14 от 17.04.2014 г.

УТВЕРЖДАЮ

Генеральный директор
ОАО «ИнфоТеКС Интернет Траст»

А.Е. Прошин

"____" _____ 2014 г.

РЕГЛАМЕНТ
системы защищенного юридически значимого электронного документооборота "ViPNet ЭДО Документ"

Редакция от 17 апреля 2014 г.
(вступает в силу 23 апреля 2014 г.)

г. Москва
2014 г.

Термины и определения.

Термины и определения даны в соответствии с положениями Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Содержащиеся в настоящем Регламенте термины и определения следует также воспринимать как терминологические синонимы терминов и определений, содержащихся в Федеральном законе от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи», до окончания срока его действия.

Система защищенного юридически значимого электронного документооборота "ViPNet ЭДО Документ" (далее – Система- корпоративная информационная система, построенная на базе программных продуктов ViPNet ЭДО, включая программное обеспечение клиентского рабочего места ViPNet ЭДО Документ, (далее - средства Системы) и действующая по правилам, установленным Оператором Системы в соответствии с нормативными правовыми и иными актами, регулирующими электронный документооборот и применение электронной подписи.

Оператор Системы ViPNet ЭДО Документ – ОАО "ИнфоТеКС Интернет Траст".

Участники Системы ViPNet ЭДО Документ – зарегистрированные в Системе юридические и физические лица. Информация об Участниках размещается в Системе.

Доверенный способ передачи информации - способ передачи информации, обеспечивающий требуемую степень ее защищенности.

Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах[1].

Электронная подпись - 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.

Квалифицированная электронная подпись - электронная подпись, которая соответствует следующим дополнительным признакам:

1). ключ проверки электронной подписи указан в квалифицированном сертификате;
2). для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 6.04.2011 № 63-ФЗ "Об электронной подписи".

Сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Квалифицированный сертификат ключа проверки электронной подписи - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром.

---

[1] Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 06.04.2011 г.) "Об информации, информационных технологиях и о защите информации".

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном федеральным законодательством порядке выдан сертификат ключа проверки электронной подписи[2].

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).

Удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные федеральным законодательством.

Аккредитованный удостоверяющий центр - удостоверяющий центр, признанный уполномоченным федеральным органом соответствующим требованиям Федерального закона от 6.04.2011 № 63-ФЗ "Об электронной подписи".

Пользователь Удостоверяющего центра - лицо, пользующееся услугами Удостоверяющего центра.

Список отозванных (аннулированных) сертификатов – электронный документ, подписанный электронной подписью Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, которые на момент времени формирования списка отозванных сертификатов были отозваны или действие которых было приостановлено. Момент времени формирования списка отозванных сертификатов ключей проверки электронной подписи определяет значение поля «время начала действия списка» списка отозванных сертификатов.

Актуальный список отозванных сертификатов – список отозванных сертификатов ключей проверки электронной подписи, являющийся последним изданным на данный момент времени и действующим, т.е. момент времени подписания электронного документа лежит внутри временного интервала, определяемого значениями полей «время начала действия списка» и «время следующего обновления» списка отозванных сертификатов.

1. Предмет Регламента

1.1. Настоящий Регламент разработан в соответствии с действующим законодательством Российской Федерации и определяет принципы взаимодействия Участников системы защищенного юридически значимого электронного документооборота, порядок получения в Удостоверяющем центре сертификатов ключей проверки электронной подписи, а также условия, при соблюдении которых электронная подпись в электронном документе признается равнозначной собственноручной.

1.2. Сторонами Регламента являются Оператор и Участники системы защищенного юридически значимого электронного документооборота **"ViPNet ЭДО Документ"**.

1.3. Стороны понимают термины, применяемые в настоящем Регламенте, строго в контексте общего смысла Регламента.

---

[2] Физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности.

2. Порядок использования электронных документов в Системе

2.1. Участники Системы соглашаются при осуществлении взаимоотношений между ними, а также с Оператором Системы принимать к сведению и исполнению электронные документы, подписанные квалифицированной электронной подписью.

2.2. Участники Системы принимают, что электронная подпись в электронных документах, сформированных владельцем сертификата ключа подписи, является равнозначной собственноручной подписи владельца сертификата ключа проверки электронной подписи и оттиску печати Участника Системы при выполнении условий, определенных настоящим Регламентом.

2.3. Использование в рамках настоящего Регламента электронных документов, подписанных электронной подписью, не изменяет содержания прав и обязанностей Участников системы, содержания документов и правил заполнения их реквизитов, установленных действующим законодательством Российской Федерации и иными нормативными документами.

2.4. Участники Системы принимают, что в случае наличия требований к формату и содержанию электронного документа, в Системе используются электронные документы установленного формата. Перечень электронных документов, в отношении формата и содержания которых нормативными актами или Оператором Системы установлены требования, содержится в Приложении 1.

2.5. Участники Системы самостоятельно определяют круг тех участников Системы, с которыми будет осуществляться обмен электронными документами. Для этого Участник Системы должен отправить другому Участнику Системы запрос на добавление в список контрагентов и получить подтверждение на добавление. Также Участник Системы может в одностороннем порядке исключить другого Участника Системы из списка контрагентов, в этом случае последний получает уведомление об исключении из списка контрагента.

2.6. Участники Системы принимают, что в соответствии с Федеральным законом от 18.06.2003 № 126-ФЗ "О связи" в Системе применяется единое учетно-отчетное время – московское.

2.7. Участники Системы соглашаются со следующими принципами электронного документооборота:

2.7.1. Электронный документ считается отправленным одним Участником Системы (отправителем) другому Участнику Системы (адресату), если отправителем получена квитанция, подтверждающая получение электронного документа Оператором системы.

2.7.2. Электронный документ, отправленный отправителем, считается доставленным адресату, если отправителем получена квитанция, подтверждающая получение электронного документа адресатом.

2.7.3. В случае отправки электронного документа, требующего подписания со стороны адресата:

– документ считается подписанным адресатом, если адресатом отправлены отправителю квитанция о подписании электронного документа и электронный документ с квалифицированной электронной подписью адресата;

– документ считается неподписанным адресатом, если адресатом отправлена отправителю квитанция об отказе в подписании полученного электронного документа.

3. Удостоверяющий центр и сертификаты ключей проверки электронных подписей

3.1. Участники Системы обязуются использовать, принимать и признавать квалифицированные сертификаты ключей проверки электронной подписи, созданные Удостоверяющим центром ОАО "ИнфоТеКС Интернет Траст" или иным аккредитованным удостоверяющим центром, использующим в своей деятельности средства удостоверяющего центра и средства электронной подписи, совместимые со средствами, используемыми Удостоверяющим центром ОАО "ИнфоТеКС Интернет Траст".

3.2. Для получения в Удостоверяющем центре квалифицированного сертификата ключа проверки электронной подписи Участник подает в Удостоверяющий центр пакет документов, предусмотренный Федеральным законом от 06.04.2011 г. № 63-ФЗ "Об электронной подписи" и Регламентом Удостоверяющего центра.

3.3. Квалифицированный сертификат ключа проверки электронной подписи признается созданным Удостоверяющим центром, если подтверждена подлинность электронной подписи издателя квалифицированного сертификата ключа проверки электронной подписи.

3.4. Участники Системы принимают, что данные, содержащиеся в поле Subject квалифицированного сертификата ключа проверки электронной подписи, соответствуют идентификационным данным владельца квалифицированного сертификата ключа проверки электронной подписи, зарегистрированного в реестре Удостоверяющего центра, и однозначно идентифицируют владельца квалифицированного сертификата ключа проверки электронной подписи и соответствующего ключа электронной подписи.

3.5. Участники Системы принимают, что для определения действительности квалифицированного сертификата ключа проверки электронной подписи используются сертификат издателя сертификата ключа проверки электронной подписи и список отозванных сертификатов, издаваемый и публикуемый Удостоверяющим центром в порядке и с периодичностью, определяемыми Регламентом Удостоверяющего центра.

3.6. В качестве места публикации актуального списка отозванных сертификатов принимается адрес информационного ресурса, указанный в поле CRLDistributionPoints сертификата ключа проверки электронной подписи.

4. Средства электронной подписи

4.1. Участники Системы принимают в качестве средства электронной подписи, применяемого для создания и проверки электронной подписи, средство криптографической защиты информации ViPNet CSP или КриптоПро CSP. Применяемые версии указанных средств криптографической защиты информации должны соответствовать требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 г. № 63-ФЗ "Об электронной подписи".

4.2. Участники Системы принимают, что эталонные образцы указанных в п. 4.1 средств электронной подписи находятся у производителя.

5. Условия равнозначности электронной подписи собственноручной

Квалифицированная электронная подпись в электронном документе равнозначна собственноручной подписи владельца квалифицированного сертификата ключа проверки электронной подписи при одновременном соблюдении следующих условий:

5.1. владелец квалифицированного сертификата ключа проверки электронной подписи может быть идентифицирован по содержимому квалифицированного сертификата ключа проверки электронной подписи;

5.2. серийный номер квалифицированного сертификата ключа проверки электронной подписи не содержится в актуальном списке отозванных сертификатов;

5.3. срок действия квалифицированного сертификата ключа проверки электронной подписи наступил и не окончен на момент создания электронной подписи;

5.4. квалифицированная электронная подпись используется в соответствии со сведениями, указанными в квалифицированном сертификате проверки электронной подписи;

5.5. положительный результат проверки с использованием средств электронной подписи отсутствия искажений в подписанном данной квалифицированной электронной подписью электронном документе.

6. Порядок регистрации участника системы

6.1. Для регистрации в Системе Участник должен предоставить Оператору:

- Квалифицированный сертификат ключа проверки электронной подписи, соответствующий положениям настоящего Регламента.
- Заявление об участии в электронном документообороте по телекоммуникационным каналам связи по установленной Оператором форме.

6.2. Заявление об участии в электронном документообороте по телекоммуникационным каналам связи может быть направленов форме электронного документа, сформированного при помощи средств Системы, установленных на стороне Участника Системы, и подписанного квалифицированной электронной подписью уполномоченного лица Участника Системы, являющегося владельцем квалифицированного сертификата или в форме документа на бумажном носителе по форме Приложения 2 к настоящему Регламенту

6.3. В заявлении указываются следующие учетные данные:

- полное наименование организации (фамилия, имя, отчество физического лица);
- место нахождения организации (место жительства физического лица);
- идентификационный номер налогоплательщика организации (физического лица);
- код причины постановки на учет организации;
- сведения о владельцах сертификатов ключа подписи и реквизиты сертификата ключа подписи;
- сведения о налоговом органе, в котором состоит на учете организация (физическое лицо);
- иные установленные Оператором учетные данные.

6.4. В случае использования Участником квалифицированного сертификата ключа проверки электронной подписи, созданного не Удостоверяющим центром ОАО "ИнфоТеКС Интернет Траст" (пункт 4.1. настоящего Регламента), Оператор вправе потребовать представления дополнительных документов, подтверждающих достоверность регистрационных данных Участника.

7. Права и обязанности сторон

7.1. **Участники Системы обязаны:**

7.1.1. Выполнять требования нормативных документов органов исполнительной власти при осуществлении документооборота, в отношении которого такие требования установлены.

7.1.2. В случае изменения учетных данных, содержащихся в Заявлении об участии в электронном документообороте в электронном виде по телекоммуникационным каналам

связи, не позднее трех рабочих дней со дня соответствующего изменения представить Оператору заявление о внесении изменений в ранее сообщенные данные.

7.1.3. Обеспечивать конфиденциальность принадлежащих им ключей электронной подписи.

7.1.4. Немедленно информировать Удостоверяющий центр о факте компрометации принадлежащих им ключей электронной подписи.

7.1.5. Немедленно прекратить использование ключей электронной подписи в случае их компрометации.

7.1.6. Использовать копии средств криптографической защиты информации (средств электронной подписи), полученные легальным путем.

7.1.7. Использовать средства криптографической защиты информации в соответствии с требованиями, определенными эксплуатационной документацией к ним.

7.1.8. Принимать меры для предотвращения несанкционированного доступа к компьютерам с установленными на них средствами криптографической информации, а также в помещения, в которых они установлены.

7.2. **Оператор Системы обязан:**

7.2.1. Выполнять требования нормативных документов органов исполнительной власти при обеспечении обмена информацией по телекоммуникационным каналам связи в рамках электронного документооборота, в отношении которого такие требования установлены.

7.2.2. Обеспечивать круглосуточный и бесперебойный обмен информацией по телекоммуникационным каналам связи в рамках электронного документооборота между Участниками Системы.

7.2.3. Обеспечить функционирование программно-аппаратного комплекса Системы в соответствии с требованиями эксплуатационной документации на него.

7.2.4. В случае получения от Участника заявления о внесении изменений в ранее сообщенные учетные данные, не позднее трех рабочих дней с момента получения заявления осуществить изменение в Системе учетных данных Участника.

7.2.5. Осуществлять техническое сопровождение программных средств Участников в соответствии с обязательствами, изложенными в Приложении 3 к настоящему Регламенту.

7.2.6. Осуществлять хранение в течение 5 лет всех извещений/квитанций, подтверждающих факт отправки или получения документов Участниками Системы.

7.3. **Оператор Системы вправе:**

7.3.1. Проводить регламентные работы по техническому обслуживанию и внесению изменений в Систему. Конкретную дату и время проведения регламентных работ Оператор Системы определяет самостоятельно, при этом, не менее чем за три дня до начала проведения регламентных работ, Оператор Системы обязан разместить на своем сайте информацию о проведении таких работ с указанием точной даты и времени их начала и окончания. При соблюдении указанных условий, в период проведения регламентных работ, Оператор Системы имеет право приостановить оказание услуг Участникам Системы.

7.3.2. Совершать иные действия, не противоречащие действующему законодательству РФ и настоящему Регламенту.

8. Ответственность сторон

8.1. За неисполнение или ненадлежащее исполнение обязанностей, определенных настоящим Регламентом Стороны несут ответственность в соответствии с действующим законодательством РФ.

8.2. Оператор Системы не несет ответственности за содержание и достоверность информации, передаваемой Участниками Системы, а также за какой-либо ущерб, потери и прочие убытки, которые понес Участник Системы по причине несоблюдения им требований настоящего Регламента, а также в следующих случаях:

8.2.1. Нарушения и сбои в работе технических средств Участника Системы, в том числе по причине заражения компьютерными вирусами.

8.2.2. Отсутствие у Участника Системы возможностей по обработке информации в требуемом формате.

8.2.3. Нарушение Участником Системы правил эксплуатации средств электронной подписи, правил хранения и использования ключей электронной подписи.

8.2.4. Невозможность пользоваться услугами Системы по причине их неоплаты.

8.2.5. Неизвещение или сделанное ненадлежащим образом извещение Оператора Системы об изменении реквизитов Участника Системы.

8.2.6. В иных, независящих от Оператора Системы, обстоятельствах, в частности, наступивших в результате действий или бездействия Участников Системы.

9. Конфиденциальность

9.1. Под конфиденциальной информацией подразумевается любая информация и данные, представляющие собой коммерческую, служебную тайну, либо персональные данные, доступ к которым ограничивается в соответствии с законодательством Российской Федерации, а также любая иная информация, помеченная как конфиденциальная или в письменном виде явно определенная в качестве таковой.

9.2. Оператор или Участник Системы, получившие Конфиденциальную информацию при исполнении настоящего Регламента обязаны использовать ее исключительно в целях выполнения настоящего Регламента, охранять ее конфиденциальность и, если иное прямо не установлено законом, не раскрывать эту информацию, как полностью, так и частично, третьим лицам, за исключением работников или контрагентов, которым эта информация необходима для выполнения возложенных на них обязательств.

9.3. К конфиденциальной информации не относится информация, которая:

- была известна стороне, получившей информацию, до ее предоставления;
- самостоятельно созданная этой стороной до такого предоставления;
- стала общеизвестной не по причине действий или бездействия стороны, получившей информацию.

10. Изменение (дополнение) Регламента

10.1. Текст Регламента и последующие изменения публикуются на web-сайте Оператора www.iitrust.rune позднее 30 (Тридцати) календарных дней до даты вступления в силу новой редакции Регламента.

10.2. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Оператором в одностороннем порядке.

10.3. С целью обеспечения гарантированного ознакомления с текстом изменений и дополнений Регламента, Участник Системы обязан не реже 1 (Одного) раза в неделю обращаться на web-сайт Оператора www.iitrust.ru/ за сведениями об изменениях и дополнениях в Регламент.

10.4. Все изменения (дополнения), вносимые в Регламент и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными для Сторон после опубликования на сайте Оператора Системы.

10.5. Все изменения (дополнения), вносимые в Регламент в связи с изменением действующего законодательства Российской Федерации вступают в силу одновременно с вступлением в силу изменений (дополнений).

10.6. Все приложения, изменения и дополнения к настоящему Регламенту являются его составной и неотъемлемой частью.

Приложение 1
к Регламенту системы защищенного юридически
значимого электронного документооборота
"ViPNet ЭДО Документ"

Перечень
электронных документов, в отношении формата и содержания которых органами исполнительной власти установлены требования

№ п/п	Наименование документа	Наименование органа исполнительной власти	Примечание
1.	Счет-фактура	ФНС России	Приказ от 5.03.2012 №ММВ-7-6/138@
2.	Товарная накладная	ФНС России	Приказ от 21.03.2012 №ММВ-7-6/172@
3.	Акт приемки-сдачи работ (услуг)	ФНС России	Приказ от 21.03.2012 №ММВ-7-6/172@

Приложение 2
к Регламенту системы защищенного юридически
значимого электронного документооборота
"ViPNet ЭДО Документ"

ОАО "ИнфоТеКС Интернет Траст"
г. Москва, Старый Петровско-
Разумовский пр., д. 1/23, стр. 1

Заявление

об участии в электронном документообороте по телекоммуникационным каналам связи

_____,
(полное наименование организации или фамилия, имя, отчество индивидуального предпринимателя)

расположенное _____,
(адрес места нахождения организации или места жительства индивидуального предпринимателя)

ИНН _____,
(идентификационный номер налогоплательщика организации или индивидуального предпринимателя)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____,
полностью и безусловно присоединяется к Регламенту системы защищенного юридически значимого электронного документооборота _____ в качестве Участника системы.

С Регламентом системы защищенного юридически значимого электронного документооборота _____ ознакомлен и обязуюсь соблюдать все положения указанного документа.

Сведения о владельце полученного сертификата ключа проверки электронной подписи:

фамилия, имя, отчество: _____,
должность: _____,

Реквизиты полученного сертификата ключа проверки электронной подписи:
наименование удостоверяющего центра, создавшего сертификат: _____
_____,
серийный номер сертификата _____,
дата начала действия сертификата _____.
Контактные данные организации (индивидуального предпринимателя): _____
_____
_____

Сведения о налоговом органе, в котором состоит на учете организация (индивидуальный предприниматель): _____
_____

_____ _____ / _____ /
(дата подачи Заявления) (подпись) (Фамилия, И.О.)

Приложение 3
к Регламенту системы защищенного юридически
значимого электронного документооборота
"ViPNet ЭДО Документ"

ОБЯЗАТЕЛЬСТА
СТОРОН ПО ВОПРОСАМ ТЕХНИЧЕСКОГО СОПРОВОЖДЕНИЯ

1. Обязательства Оператора Системы по техническому сопровождению.

1.1. Оператор консультирует Участника Системы по текущим вопросам, связанным с использованием средств Системы, установленных на стороне Участника, и получением услуг, по телефону или по электронной почте, указанным на сайте Оператора. Режим работы Службы поддержки Оператора - рабочие дни с 2.00 до 18.00 часов по Московскому времени.

1.2. Реакция Оператора на обращение осуществляется максимально оперативно, Оператор информирует Участника о действиях по устранению причин обращения. В случае, если Оператор не в состоянии оперативно определить и/или устранить причину обращения, Участник информируется об этом согласованным способом. Оператор принимает меры для устранения причины обращения и, не позднее 72-х часов с момента получения заявки от Участника, сообщает о принятых мерах. В случае невозможности устранения в указанный срок сбоя или отказа в работе программных средств, вызвавших обращение Участника, Оператор сообщает план мероприятий по устранению причин сбоя или отказа и предполагаемое время, необходимое для его выполнения.

1.3. Техническое сопровождение не включает в себя:

- исправление ошибок, возникших вследствие действий Участника, противоречащих эксплуатационной документации на программные средства;
- исправление ошибок, возникших вследствие неавторизованной модификации программных средств (изменение структуры, корректировка баз данных, и пр.);
- определение причин и сбоев, не связанных с работой средств Системы;
- разработку технических предложений по изменению и/или развитию конфигурации информационной инфраструктуры Участника.

2. Обязательства Участника Системы, связанные с техническим сопровождением.

2.1. Участник обязан своевременно сообщать Оператору обо всех сбоях, отказах и других нештатных ситуациях, связанных с оказанием услуг.

2.2. Участник обязан оперативно предоставлять Оператору возможность выполнять свои обязанности по техническому сопровождению программных средств. В частности, Участник должен обеспечить Оператору возможность удаленного выполнения своих обязанностей по техническому сопровождению. Под возможностью удаленного выполнения Оператором обязанностей по техническому сопровождению программных средств понимается наличие у Участника доступа к сети Интернет, действующего адреса электронной почты (e-mail) и междугородной телефонной связи.

2.3. Участник должен обеспечить соответствие рабочего места требованиям, указанным в эксплуатационной документации на программные средства. При этом на рабочем месте Участника должно быть установлено лицензионное общее программное обеспечение.

При невыполнении Участником вышеизложенных обязательств Оператор не несет ответственности за непредоставление и (или) ненадлежащее предоставление услуг в Системе.