Порядок обмена документами в электронном виде

1. Специальные термины, применяемые в тексте Порядка, используются в следующем значении:

1.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.2. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.3. Электронный документ (далее – ЭД) – электронный образ документа, представленный в согласованном между Сторонами формате, определяемом программными средствами создания документа. Электронный документ передается между Сторонами в составе сообщения, подписанного электронной подписью (далее – ЭП).

1.4. Электронная подпись (далее – ЭП) – реквизит ЭД, предназначенный для защиты данного ЭД от подделки, полученный в результате криптографического преобразования информации и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в ЭД.

1.5. Сторона – участник обмена документами в электронном виде.

1.6. Принципал – сторона, осуществляющая обмен документами в электронном виде с АО «ЕИРЦ Петроэлектросбыт».

1.7. Авторство ЭД – принадлежность ЭД Стороне.

1.8. Целостность электронного документа – полное соответствие содержания хранимого или полученного ЭД содержанию исходного ЭД в момент его подписания ЭП.

1.9. Система подготовки электронных документов (далее Система) – система, включающая в себя совокупность программно-аппаратных средств, устанавливаемых у Сторон с целью обеспечения подготовки, защиты, проверки и обработки документов в электронном виде.

1.10. Ключи шифрования - ключи, предназначенные для защиты электронных документов Сторон при их передаче по каналам связи.

1.11. Ключ ЭП (далее – закрытый ключ ЭП) – уникальная последовательность данных (ключ), известная только уполномоченному лицу Стороны и предназначенная для формирования ЭП.

1.12. Компрометация закрытого ключа ЭП – события или действия, в результате которых ключи ЭП могут стать доступными несанкционированным лицам и (или) процессам, в том числе увольнение сотрудников, имевших доступ к ключевой информации, хищение, утрата, разглашение, несанкционированное копирование компонентов ЭП.

1.13. Ключ проверки ЭП (далее – открытый ключ ЭП) – уникальная последовательность данных (ключ), зависящая от (закрытого) ключа, предназначенная для проверки корректности ЭП, сформированной с использованием закрытого ключа ЭП.

1.14. Действующий открытый ключ ЭП Стороны, зарегистрированный в порядке, установленном п.3.7 Порядка, не выведенный из действия по основаниям, предусмотренным настоящим Порядком, и срок действия которого не истек.

1.15. Корректная ЭП – ЭП, дающая положительный результат ее проверки средствами Системы.

1.16. Удостоверяющий центр – организация, выполняющая в Системе функции, предусмотренные Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи». В целях настоящего Порядка АО «ЕИРЦ Петроэлектросбыт» является Удостоверяющим центром.

1.17. Владелец сертификата ключа подписи – уполномоченный сотрудник «Принципала», на имя которого Удостоверяющим центром выдан сертификат ключа подписи и который владеет соответствующим закрытым ключом ЭП, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы)

1.18. Сертификат ключа подписи – документ, который включает в себя открытый ключ электронной подписи и который выдается Удостоверяющим центром участнику Системы для подтверждения подлинности электронной подписи и идентификации владельца сертификата ключа подписи.

1.19. Центр сертификации – программно-аппаратный компонент удостоверяющего центра, предназначенный для формирования сертификатов открытых ключей ЭП.

1.20. Криптопровайдер – программный модуль, содержащий библиотеку криптографических функций со стандартизованным интерфейсом, предназначенный для авторизации, обеспечения конфиденциальности и юридической значимости электронных документов при обмене ими между пользователями, контроля целостности информации.

1.21. Запрос на сертификат открытого ключа ЭП в электронном виде – файл специального формата, содержащий открытый ключ с параметрами алгоритма и сведения о Подписчике сертификата, заверенные его электронной подписью.

2. ЭД, которыми обмениваются Стороны, передаются и принимаются с использованием Системы с возможностью передачи персональных данных на бумажных носителях, в случае неготовности технических средств с одной из сторон, или технического сбоя.

3. Условия передачи ЭД с использованием ЭП:

3.1. Система состоит из программных и аппаратных средств, используемых Сторонами по договоренности, комплектуемых Сторонами за свой счет и эксплуатируемых Сторонами самостоятельно.

3.2.Система использует программные и аппаратные средства связи, обеспечивающие обмен электронными документами между Сторонами.

3.3. При выходе из строя аппаратных или программных средств Системы или их элементов, а также в иных случаях, указанных в разделе 2 Порядка, и, соответственно, приостановлении использования Системы, Сторона обязана в течение суток известить другую Сторону любым доступным способом, а в течение 3 суток дать письменное сообщение о готовности и сроках возобновления обмена документами в электронном виде. На период приостановления использования Системы обмен документами между Сторонами осуществляется на бумажных носителях или с использованием иных систем и средств связи, о которых Стороны договариваются отдельно, вне рамок Порядка.

3.4. Стороны признают, что программные средства, обеспечивающие изготовление закрытых и открытых ключей ЭП, а также формирование и проверку ЭП, предоставляемые Сторонам, выполнены в соответствии с требованиями документа ГОСТ Р 34.10 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой

подписи» и ГОСТ Р 34.11 «Информационная технология. Криптографическая защита информации. Функция хэширования».

3.5.Стороны признают, что получение ими электронных документов, заверенных корректной ЭП другой Стороны, юридически эквивалентно получению документов на бумажном носителе, подписанных уполномоченными лицами и заверенных оттиском печати этой Стороны.

3.6.Стороны признают, что:

– применение усиленной неквалифицированной электронной подписи и шифрования достаточным для обеспечения конфиденциальности, авторства и целостности электронных документов, а также невозможности их фальсификации;

– после заверения электронного документа ЭП любое изменение, добавление или удаление символов документа делает ЭП некорректной, т.е. проверка подписи с открытым ключом ЭП Стороны, подписавшей электронный документ, дает отрицательный результат;

– создание корректной ЭП электронного документа возможно исключительно с использованием закрытого ключа ЭП;

– по содержанию электронных документов, подписанных ЭП, и открытых ключей ЭП невозможно определить закрытые ключи ЭП;

- каждая Сторона несет полную ответственность за обеспечение безопасности и сохранность своих закрытых ключей ЭП, а также за действия своего персонала;

- целостность программных средств Системы, установленных у Сторон, может быть проверена путем вычисления значений хэш-функции в соответствии с документом ГОСТ Р 34.10 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и сравнения их со значениями хэш-функции, вычисленными при установке или обновлении программного обеспечения;

- каждая Сторона является обладателем информационных ресурсов, размещенных на технических средствах Стороны.

3.7.Порядок применения средств Системы предусматривает, что:

– Функции Удостоверяющего центра по данному соглашению выполняет АО «ЕИРЦ Петроэлектросбыт».

– Порядок получения Принципалом сертификата ключа подписи определяется действующим Регламентом Удостоверяющего Центра АО «ЕИРЦ Петроэлектросбыт»;

– Каждая Сторона может иметь несколько закрытых ключей ЭП, каждому закрытому ключу ЭП соответствует собственный открытый ключ ЭП.

– При компрометации или подозрении на компрометацию закрытого ключа ЭП Стороны (т.е. при ознакомлении или подозрении на ознакомление неуполномоченного лица с закрытым ключом ЭП, а также при несанкционированном использовании или подозрении на несанкционированное использование закрытого ключа ЭП) другая Сторона извещается доступным способом о прекращении действия соответствующего ключа ЭП. С момента уведомления Стороны прекращают передачу электронных документов с использованием указанного ключа ЭП, и выводят из действия соответствующий открытый ключ ЭП. Скомпрометированные ключи уничтожаются Сторонами самостоятельно.

– Сторона, получившая сообщение о компрометации и/или замене ключа ЭП, выводит соответствующий открытый ключ из действия в максимально короткие сроки, но не позднее следующего рабочего дня после получения сообщения о компрометации.

– В случае использования нескольких ЭП электронный документ признается имеющим корректную ЭП, если корректны все ЭП, которыми он подписан.

– Стороны самостоятельно выбирают организацию – провайдера, обеспечивающую доступ к сети Интернет, и осуществляют подключение к сети Интернет за счет собственных средств. Все расходы, связанные с подключением к сети Интернет, эксплуатацией и обменом данными по Системе через сеть Интернет осуществляются Сторонами за счет собственных средств.

– Стороны полностью несут все риски, связанные с подключением их вычислительных средств к сети Интернет. Стороны самостоятельно обеспечивают защиту собственных вычислительных средств и криптографических ключей от несанкционированного доступа и вирусных атак из сети Интернет. Стороны также признают, что выход из строя Системы у Стороны в результате вмешательства из сети Интернет рассматривается как выход из строя по вине этой Стороны и восстановление работоспособности Системы осуществляется этой Стороной за счет собственных средств.

3.8. Исходя из изложенного в п.п. 3.4-3.7 настоящего Порядка, Стороны признают аутентификационные свойства ЭП, применяемой ими. Электронный документ, имеющий корректную ЭП одной из Сторон, признается другой Стороной как эквивалентный документу на бумажном носителе, составленному и оформленному в соответствии с законодательством Российской Федерации, и порождает права и обязанности Сторон при выполнении взаимных обязательств по настоящему Порядку.

3.9. Стороны установили, что моментом получения ЭД принимающей Стороной в Системе является текущее время по системным часам принимающей Стороны в момент помещения информации в архив входящих сообщений принимающей Стороны.

3.10. Для выполнения криптографических операций в ходе информационного обмена Стороны используют криптопровайдер КриптоПро CSP.

4. В целях реализации Порядка Стороны обязуются:

4.1.Заранее до начала обмена документами в электронном виде предоставить противоположной Стороне свой открытый ключ ЭП, соответствующих закрытому ключу ЭП, которым будет осуществляются электронная подпись документов.

4.2.Принимать поступившие от противоположной Стороны электронные документы, оформленные и переданные в соответствии с условиями настоящего Порядка и заверенные корректной ЭП Стороны.

4.3.Не принимать поступившие от противоположной Стороны электронные документы, оформленные с нарушением требований действующего законодательства Российской Федерации и условий настоящего Порядка, а также при отсутствии или некорректности ЭП Стороны.

4.4.Не разглашать и не передавать другим лицам (обеспечить конфиденциальность) информацию, связанную с использованием Системы, за исключением случаев, предусмотренных действующим законодательством Российской Федерации и условиями настоящего Порядка.

4.5.Поддерживать до помещения в электронные архивы системные журналы и текущие базы переданных и принятых электронных документов с ЭП на аппаратных средствах Системы в течение не менее тридцати дней после их получения, а в случае возникновения споров – до их разрешения. Обеспечить сохранность архивов переданных и принятых электронных документов, подписанных ЭП, открытых ключей ЭП противоположной Стороны в течение срока, установленного действующим законодательством Российской Федерации.

4.6.Организовать внутренний режим функционирования установленных по месту нахождения Стороны рабочих мест таким образом, чтобы исключить возможность использования Системы и ключей ЭП лицами, не имеющими допуска к работе с Системой.

5. В целях реализации настоящего Порядка Стороны имеют право:

5.1.Требовать от противоположной Стороны замены (формирования) ключей ЭП при проведении периодической плановой замены ключей ЭП, компрометации или подозрении на компрометацию закрытых ключей ЭП.

5.2. При установлении возможности нарушения безопасности Системы, выявлении фактов или признаков таких нарушений, немедленно приостановить использование Системы и оповестить противоположную Сторону в порядке, предусмотренном в п. 3.3 настоящего Порядка.

5.3.В случае неисправности Системы Стороны могут обмениваться документами на бумажном носителе.

6. Ответственность сторон

6.1.За невыполнение или ненадлежащее выполнение обязательств по настоящему Порядку виновная Сторона несет ответственность в соответствии с действующим законодательством Российской Федерации.

6.2.В случае возникновения обстоятельств непреодолимой силы, к которым относятся стихийные бедствия, аварии, пожары, массовые беспорядки, забастовки, революции, военные действия, противоправные действия третьих лиц, вступление в силу законодательных актов, правительственных постановлений и распоряжений государственных органов, прямо или косвенно запрещающих или препятствующих осуществлению Сторонами своих функций по настоящему Порядку и иных обстоятельств, не зависящих от волеизъявления Сторон, Стороны по настоящему Порядку освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых на себя обязательств.

6.3.Стороны несут ответственность за содержание электронных документов, подписанных ЭП их уполномоченных лиц и не отвечают за правильность заполнения и оформления электронных документов другой Стороной.

6.4. Стороны несут ответственность за поддержание в работоспособном состоянии средств криптографической защиты, программных и технических средств, а также каналов связи, необходимых для осуществления и обеспечения электронного документооборота.

6.5.Стороны не несут ответственности за ущерб, возникший вследствие разглашения уполномоченными лицами противоположной Стороны собственного закрытого ключа ЭП, его утраты или его передачи, вне зависимости от причин, неуполномоченным лицам.

6.6.Стороны не несут ответственности за последствия совершенных действий в соответствии с полученным электронным документом, защищенным корректной ЭП противоположной Стороны, в т.ч. в случае использования ключей ЭП, ключей шифрования, ключевых носителей и программно-аппаратных средств Системы противоположной Стороны неуполномоченным лицом.

6.7.Стороны не несут ответственности в случае реализации угроз несанкционированного доступа неуполномоченных лиц к части Системы, установленной у противоположной Стороны, и криптографическим ключам противоположной Стороны, включая угрозы со стороны внутренних (локальных) и внешних (глобальных) сетей связи.

7. Порядок разрешения споров

7.1.При возникновении разногласий и споров в связи с обменом электронными документами с помощью Системы с целью установления фактических обстоятельств, послуживших основанием для их возникновения, а также для проверки целостности и подтверждения авторства электронного документа, Стороны обязаны провести техническую экспертизу в соответствии с разделом 8 Порядка. Споры, по которым не достигнуто соглашение Сторон после проведения технической экспертизы, разрешаются в Арбитражном суде Санкт-Петербурга и Ленинградской области в соответствии с действующим законодательством Российской Федерации.

8. Техническая экспертиза спорных ситуаций, связанных с принятием или непринятием сторонами электронного документа

8.1. При возникновении разногласий Сторон в связи с обменом документами в электронном виде с помощью Системы, а также в иных случаях возникновения спорных ситуаций в связи с эксплуатацией Системы, обмен документами в электронном виде с использованием Системы между Сторонами немедленно прекращается.

8.2. Сторона, заявляющая разногласие, (инициатор спора) обязана направить другой Стороне заявление о разногласиях, подписанное уполномоченным лицом Стороны, с предложением создать согласительную комиссию и изложением причин разногласий в объеме, необходимом для исполнения настоящей Процедуры. Заявление должно содержать фамилии, имена, отчества и иные сведения о представителях Стороны – инициатора спора, которые будут участвовать в работе комиссии, место, время и дату сбора комиссии. Дата сбора комиссии должна быть не позднее 10 дней со дня получения другой Стороной заявления.

8.3.В состав комиссии должно входить равное количество представителей (до трех человек) от каждой из Сторон, полномочия которых удостоверяются доверенностями, оформленными в соответствии с действующим законодательством Российской Федерации. При необходимости, с письменного согласия обеих Сторон, в состав комиссии могут быть дополнительно введены эксперты третьей стороны. Состав комиссии должен быть зафиксирован в акте, который является итоговым документом, отражающим результаты работы комиссии.

Полномочия членов комиссии подтверждаются доверенностями, выданными в установленном порядке. Срок работы комиссии - не более пяти рабочих дней. В исключительных ситуациях этот срок может быть увеличен по взаимной договоренности Сторон.

8.4.Стороны способствуют работе комиссии и не допускают отказа от предоставления необходимых документов.

При необходимости Стороны обязаны предоставить комиссии возможность ознакомиться с условиями и порядком работы Системы.

8.5.При возникновении у одной из Сторон претензий к другой Стороне по поводу корректности действий, совершенных в рамках выполнения обязательств по п.п. 4.2-4.3 настоящего Порядка, комиссия должна:

– проверить авторство предъявляемого Стороной электронного документа, полученного ей от другой Стороны, в соответствии с которым совершены действия;

– проверить, что совершенные Стороной действия соответствуют содержанию электронного документа.

8.6.Для проверки авторства электронного документа выполняются следующие действия:

8.6.1. Из электронного архива Стороны, получившей электронный документ, комиссии предъявляется файл с ЭП, содержащий оспариваемый электронный документ.

8.6.2. Проверяется корректность электронной подписи оспариваемого электронного документа на основе открытого ключа ЭП, действующего на момент подписания.

8.6.3. Сторона, получившая оспариваемый документ, предъявляет комиссии действовавший на момент подписания открытый ключ подписи, переданный ей противоположной Стороной и предназначенный для проверки корректности ЭП оспариваемого документа.

8.6.4. Проверяется корректность электронной подписи оспариваемого электронного документа, с помощью программного средства Крипто-АРМ или аналогичного, использующего криптопровайдер КриптоПро CSP.

8.6.5. По требованию Стороны, открытый ключ которой предъявлен второй Стороной, может быть проверена принадлежность предъявленного открытого ключа первой Стороне. Открытый ключ признается принадлежащим первой Стороне, если открытый ключ, представленный комиссии в виде файла, соответствует открытому ключу, содержащемуся в сертификате на бумажном носителе, выданном Удостоверяющим центром в соответствии с условиями настоящего Порядка.

8.6.6. Если предъявленный в виде файла ключ не соответствует открытому ключу, содержащемуся в сертификате на бумажном носителе, либо период действия предъявленного ключа не соответствует времени получения оспариваемого документа, то комиссия признает, что открытый ключ не был представлен Стороной, получившей оспариваемый документ.

8.7. Если в результате проведенной проверки корректности ЭП оспариваемого документа ЭП признана корректной, то авторство оспариваемого электронного документа признается комиссией установленным.

Если авторство оспариваемого электронного документа признано комиссией установленным и действия Стороны, к которой предъявляются претензии, соответствуют содержанию оспариваемого документа, то претензии инициатора спора признаются необоснованными.

Если авторство оспариваемого электронного документа признано комиссией установленным и действия Стороны, к которой предъявляются претензии, не соответствуют содержанию оспариваемого документа, то претензии инициатора спора признаются обоснованными.

8.8. Если в результате проведенной проверки корректности ЭП оспариваемого документа ЭП признана некорректной, то предъявленный для проверки авторства электронный документ признается комиссией ложным.

Если Сторона, представившая ложный электронный документ, является инициатором спора, то претензии данной Стороны к другой Стороне признаются необоснованными.

Если Сторона, к которой предъявляются претензии, представила ложный электронный документ, то претензии к данной Стороне признаются обоснованными.

8.9.Претензии инициатора спора к противоположной Стороне признаются необоснованными, если инициатор спора был обязан в соответствии с п.8.6.1 настоящего Порядка предъявить, но не предъявил комиссии полученный им оспариваемый документ, или не предъявил в соответствии с п. 8.6.2 настоящего Порядка открытый ключ подписи противоположной Стороны.

8.10. С целью выяснения причин и обстоятельств возникновения спорной ситуации комиссией при необходимости проводится исследование внутренних архивов, протоколов и системных журналов рабочих мест Системы Сторон.

8.11. Отсутствие на рабочем месте Системы одной из Сторон признаков отправки электронного документа, принятого другой Стороной с корректной ЭП первой Стороны, не является основанием для отказа первой Стороной от авторства данного документа.

8.12. По итогам работы комиссии составляется акт, в котором в обязательном порядке отражаются:

- состав комиссии;
- действия членов комиссии;
- установленные обстоятельства;
- основания, которые послужили для формирования выводов;
- выводы, влияющие на возможность установления подлинности оспариваемого документа.

В этом случае акт признается Сторонами надлежащим.

8.13. В случае, если предложение о создании комиссии оставлено другой Стороной без ответа, либо Сторона отказывается от участия в комиссии или препятствует работе комиссии, а также отказывается от подписания акта, заинтересованная Сторона самостоятельно составляет акт, в котором указываются сведения о причинах его составления в одностороннем порядке. В данном акте фиксируются обстоятельства, позволяющие сделать вывод о том, что оспариваемый электронный документ является корректным, либо формулируется вывод об обратном. Указанный акт направляется другой Стороне для сведения.

При рассмотрении в суде споров о наличии документа, исполненного с помощью Системы или подписанного электронной подписью, заинтересованная Сторона обязана предоставить суду акт, составленный в соответствии с настоящей Процедурой.

8.14. Составленный комиссией акт является основанием для выработки Сторонами окончательного решения комиссии. Данное решение должно быть подписано Сторонами не позднее 10 дней с момента окончания работы комиссии. В случае, если решение не будет подписано в указанный срок, заинтересованная Сторона вправе обратиться в Арбитражный суд и без выработанного Сторонами решения, а в качестве доказательства представить акт, составленный в соответствии с настоящей Процедурой.