Форма: Соглашение об электронном документообороте

Актуально на 04.06.2021

Соглашение N ___
об электронном документообороте

г. _____ "__"_____ ____ г.

_____ в лице _____,
(наименование или Ф.И.О.) (должность, Ф.И.О.)
действующ___ на основании _____,
(устава, доверенности или паспорта)
далее - Сторона 1, с одной стороны и
_____ в лице _____,
(наименование или Ф.И.О.) (должность, Ф.И.О.)
действующ___ на основании _____,
(устава, доверенности или паспорта)
далее - Сторона 2, с другой стороны, совместно именуемые "Стороны",
заключили настоящее Соглашение о нижеследующем:

Принятые сокращения и определения

Электронный документооборот - система работы с электронными документами, при которой все электронные документы создаются, передаются и хранятся с помощью информационно-коммуникационных технологий на компьютерах, объединенных в сетевую структуру.

Электронный документ (далее также - ЭД) - 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.

УЦ - удостоверяющий центр - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 N 63-ФЗ "Об электронной подписи".

ЭП - 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 (электронный документ). Существует простая и усиленная электронная подпись.

Усиленная неквалифицированная электронная подпись (далее также - НЭП) - вид усиленной ЭП, которая: получена в результате криптографического преобразования информации с использованием ключа электронной подписи; позволяет определить лицо, подписавшее ЭД; позволяет обнаружить факт внесения изменений в ЭД после момента его подписания; создается с использованием средств ЭП.

Усиленная квалифицированная электронная подпись - электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном сертификате;

- для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ "Об электронной подписи".

СКЗИ - средства криптографической защиты информации.

Подписанный электронный документ (далее также - ПЭД) - электронный документ с присоединенной электронной подписью, которая была создана на основе ЭД и ключа электронной подписи.

Сертификат ключа проверки электронной подписи (далее также - сертификат) - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. Также называется сертификатом открытого ключа. Сертификат содержит уникальный номер, дату начала и окончания срока действия, сведения о владельце, используемых криптографических алгоритмах, ограничениях на использование, уникальный ключ проверки ЭП, наименование УЦ, выдавшего сертификат, и другую информацию. Сертификат имеет свою ЭП, созданную удостоверяющим центром.

Владелец сертификата ключа проверки электронной подписи (далее также - владелец сертификата) - лицо, которому выдан сертификат ключа проверки электронной подписи. Данные о владельце должны содержаться в сертификате.

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания ЭП. Также называется закрытым ключом.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности ЭП (далее - проверка ЭП). Также называется открытым ключом. Значение ключа проверки электронной подписи содержится в сертификате.

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

Средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

Корневой сертификат УЦ - сертификат, который был выдан удостоверяющим центром самому себе и является самоподписанным. Все остальные сертификаты, выдаваемые данным УЦ, подписываются ключом ЭП этого корневого сертификата. В понятии инфраструктуры открытых ключей: если есть доверие к корневому сертификату УЦ, то автоматически есть доверие ко всем сертификатам, выданным данным УЦ и подписанным ключом ЭП данного корневого сертификата. Обычно в УЦ есть только один корневой сертификат.

Промежуточный сертификат УЦ - сертификат, ключ ЭП которого использовался для подписи другого сертификата, а сам сертификат был подписан ключом ЭП корневого сертификата УЦ или другого промежуточного сертификата этого УЦ. Промежуточные сертификаты позволяют строить широкую иерархическую структуру сертификатов УЦ.

Самоподписанный сертификат - сертификат, который подписан ключом ЭП, соответствующим ключу проверки ЭП из этого сертификата. В полях издателя сертификата содержатся те же данные, что и в полях владельца сертификата.

Создание ЭП - результат работы средства ЭП при создании ЭП, в результате которого получается последовательность бит данных фиксированной длины после криптографического преобразования электронного документа в хеш и шифрования хеша ключом электронной подписи. Длина названия алгоритмов хеширования и шифрования задаются в сертификате.

Подтверждение подлинности ЭП в ПЭД - положительный результат работы средства ЭП при проверке ЭП. Результат работы считается положительным, если после расшифровывания ЭП с помощью ключа проверки ЭП по заданному в сертификате криптографическому алгоритму получается значение, равное хешу электронного документа, полученному по заданному в Сертификате соответствующему криптографическому алгоритму.

Хеш - результат работы хеширующей функции, которая преобразовывает входной массив данных произвольной длины в выходную битовую строку фиксированной длины.

Участники электронного документооборота - лица, осуществляющие обмен информацией в электронной форме в рамках данного Соглашения.

Компрометация ключа ЭП - нарушение конфиденциальности ключа ЭП, при котором значение закрытого ключа стало известно лицу, не являющемуся владельцем сертификата.

Основной договор - Договор об информационно-технологическом взаимодействии при осуществлении переводов физических лиц без открытия счета.

Система - комплекс программно-аппаратных средств, позволяющий осуществлять электронный документооборот между Оператором и Контрагентом в рамках настоящего Соглашения. Система включает в себя средства ЭП и обеспечивает подготовку ЭД, генерацию ЭП, прием, передачу и обработку ПЭД с использованием средств вычислительной техники каждой из Сторон. Передача данных в Системе происходит по интернету.

Список отозванных сертификатов (далее также - СОС) - список, содержащий серийные номера сертификатов, которые были отозваны выдавшим их УЦ и к которым больше нет доверия. Сертификаты добавляются в СОС после извещения о компрометации ключа ЭП.

Экспертная комиссия - комиссия, создаваемая Сторонами для разрешения разногласий, возникающих при обмене ПЭД.

1. Предмет Соглашения

1.1. Настоящим Соглашением Стороны регламентировали порядок организации между Сторонами защищенного электронного документооборота в целях _____ _____ в электронной форме с использованием СКЗИ программного комплекса _____ с функциями шифрования и ЭП.

1.2. Стороны признают электронные документы, заверенные ЭП, при соблюдении требований Федерального закона от 06.04.2011 N 63-ФЗ "Об электронной подписи" юридически эквивалентным документам на бумажных носителях, заверенным соответствующими подписями и оттиском печатей Сторон.

1.3. При реализации настоящего Соглашения Стороны обеспечивают конфиденциальность и безопасность персональных данных в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных" и Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

1.4. Стороны признают, что использование СКЗИ, которые реализуют шифрование и ЭП, достаточно для обеспечения конфиденциальности информационного взаимодействия Сторон, защиты от несанкционированного доступа и безопасности обработки информации, а также для подтверждения того, что:

- электронный документ исходит от Стороны, его передавшей (подтверждение авторства документа);

- электронный документ не претерпел изменений при информационном взаимодействии Сторон (подтверждение целостности и подлинности документа) при положительном результате проверки ЭП;

- фактом доставки электронного документа является формирование принимающей Стороной квитанции о доставке электронного документа.

1.5. Настоящее Соглашение является безвозмездным.

2. Технические условия

2.1. Приобретение, установка и функционирование программного обеспечения, каналов связи, СКЗИ с функциями ЭП осуществляется за счет Сторон, а также с использованием их технических возможностей.

2.2. Изготовление и сертификацию ключей шифрования и ЭП осуществляют УЦ каждой из Сторон (или: - _____ (название конкретного УЦ)).

2.3. Электронные документы, которые передаются по настоящему Соглашению, должны быть подписаны усиленной неквалифицированной электронной подписью. Далее в качестве ЭП подразумевается НЭП.

2.4. Виды электронных документов, передаваемых другой Стороне: _____, _____, _____, _____, _____.

2.5. Обмен иными ЭД в Системе не является основанием возникновения обязательств Сторон по Соглашению.

2.6. ПЭД порождает обязательства Сторон, установленные Соглашением и Основным договором, если передающей стороной он должным образом оформлен, подписан НЭП, а принимающей стороной получен, проверен и принят к обработке в установленном Соглашением порядке.

2.7. Данное соглашение распространяется только на обеспечение защиты информации в ПЭД при передаче по открытым каналам связи. Остальные требования по защите информации выполняются Сторонами самостоятельно на основании требований действующего законодательства и требований внутренних нормативных документов Сторон.

2.8. Передача ПЭД осуществляется через Систему между Сторонами путем передачи

сообщений электронной почты через интернет.

2.9. Подключение Сторон к интернету выполняется самостоятельно и не является предметом Соглашения.

3. Общие принципы электронного документооборота

3.1. Каждая из Сторон при подписании ЭД применяет свой ключ ЭП, а при проверке подписи - ключ проверки ЭП, записанный в сертификате ключа проверки ЭП, другой стороны.

3.2. Стороны обмениваются сертификатами, которые будут использоваться для создания ЭП.

3.3. Для электронного документооборота Стороны могут использовать самоподписанные сертификаты и сертификаты, подписанные другим ключом ЭП.

3.4. Если для документооборота используется несамоподписанный сертификат, выданный УЦ, то Стороны также обмениваются корневыми сертификатами УЦ и, в случае существования, промежуточными сертификатами УЦ.

3.5. Перед началом работы Стороны проверяют свои средства ЭП и с их помощью проверяют подлинность ЭП.

3.6. Стороны признают, что:

- внесение изменений в ПЭД дает отрицательный результат проверки ЭП;

- подделка ЭП невозможна без использования ключа ЭП владельца;

- каждая сторона несет ответственность за сохранность своего ключа ЭП и за действия своего персонала при использовании средств ЭП;

- моментом наступления юридической значимости ПЭД является момент получения этого ПЭД через Систему принимающей стороной и отраженный в журнале.

3.7. Средства ЭП должны быть встроены в Систему. Стороны признают эти средства достаточными для подписания ЭД и проверки подлинности ЭП в ПЭД.

3.8. В состав средств ЭП Системы входит программное обеспечение _____, предоставляющее пользователю интерфейс для выполнения криптографических операций шифрования и расшифровывания данных, подписи данных и проверки корректности подписи, то есть являющееся средством электронной подписи.

4. Обязанности Сторон

4.1. Стороны обязуются:

4.1.1. Самостоятельно укомплектовать Систему необходимыми программно-техническими средствами и общесистемным программным обеспечением.

4.1.2. Назначить лиц, ответственных за работу с Системой в соответствии с настоящим Соглашением.

4.1.3. Назначить Администратора безопасности, отвечающего за генерацию, учет, обмен и сохранность ключей, используемых в Системе, за защиту от несанкционированного доступа и за поддержание средств ЭП Системы в рабочем состоянии.

4.1.4. Произвести обмен сертификатами.

4.1.5. Своевременно производить плановую замену ключей ЭП и соответствующих сертификатов ключей проверки ЭП в соответствии с регламентом УЦ и (или) действующего законодательства. Рекомендуется проводить плановую замену не реже ___ (_____) раз в год и за ____ (_____) рабочих (календарных) дней до окончания срока действия сертификата.

4.1.6. Немедленно информировать другую Сторону обо всех случаях утраты, хищения, несанкционированного использования ключей ЭП по следующим адресам: Оператора - по адресу _____@_____._____.ru, Контрагента - по адресу электронной почты, указанному Контрагентом в Заявлении. При этом работа в Системе приостанавливается до проведения внеплановой смены ключей.

4.1.7. Принимать на себя все риски, связанные с работоспособностью своего оборудования и каналов связи.

4.1.8. За собственный счет поддерживать в рабочем состоянии входящие в Систему программно-технические комплексы обеспечения работоспособности вычислительной техники и техники связи, обеспечивающих электронный документооборот.

4.1.9. Своевременно (не менее чем за три дня) уведомлять друг друга об изменении своего фактического места нахождения, сетевого адреса в интернете, а также об изменении иных реквизитов, имеющих существенное значение для определения юридического статуса и идентификации Сторон и исполнения обязательств по Соглашению.

4.1.10. Не предпринимать действий, способных нанести ущерб другой стороне вследствие использования Системы.

4.1.11. Своевременно информировать (по электронной почте и/или телефону) другую сторону обо всех случаях возникновения технических неисправностей или других обстоятельств, препятствующих электронному документообороту.

4.1.12. В случае обнаружения возможных угроз безопасности Стороны обязуются своевременно извещать друг друга о таких угрозах для принятия согласованных мер по их нейтрализации.

4.1.13. Строго выполнять требования технической и эксплуатационной документации к программному и аппаратному обеспечению Системы.

4.1.14. Разработать и выполнять мероприятия по обеспечению конфиденциальности, целостности и сохранности программных средств Системы, передаваемых ПЭД, протоколов регистрации событий, действующей ключевой информации и парольной информации, используемой для доступа в Систему.

4.1.15. Организовать внутренний режим функционирования рабочего места ответственного лица таким образом, чтобы исключить возможность использования Системы лицами, не имеющими допуска к работе с ней, а также исключить возможность использования средств ЭП не уполномоченными на это лицами.

4.1.16. Обеспечивать сохранение в тайне сведений по вопросам технологии защиты информации, используемых при обмене ЭД между Сторонами, за исключением случаев, предусмотренных действующим законодательством Российской Федерации.

4.1.17. Поддерживать системное время программно-аппаратных средств Системы в соответствии с текущим астрономическим временем с точностью до пяти минут. Стороны признают в качестве единой шкалы времени время GMT с учетом часового пояса г. Москвы.

4.1.18. Обмениваться ЭД, не содержащими компьютерных вирусов и (или) иных вредоносных программ.

4.1.19. Направлять другой стороне и обеспечивать прием от другой стороны ПЭД с контролем целостности и авторства в случаях и в сроки, которые установлены Соглашением и (или) Основным договором.

4.1.20. Принимать к исполнению ЭД в установленные Соглашением и (или) Основным договором сроки, если ЭД получены через Систему, подписаны НЭП и ЭП была успешно проверена.

4.1.21. При осуществлении операций на основании полученных по Системе ЭД руководствоваться требованиями законодательства Российской Федерации, а также условиями Основного договора и Соглашения.

4.1.22. Стороны организуют архивное хранение ПЭД в течение срока действия аналогичных документов, оформленных на бумажных носителях.

5. Права Сторон

5.1. Стороны имеют право:

5.1.1. Ограничивать и приостанавливать использование Системы в случаях ненадлежащего исполнения другой стороной Соглашения с уведомлением не позднее дня приостановления, а по требованию компетентных государственных органов - в случаях и в порядке, предусмотренных законодательством Российской Федерации.

5.1.2. Производить замену программно-аппаратного обеспечения Системы с предварительным уведомлением не менее чем за два рабочих дня другой стороны.

5.1.3. Остановить работу Системы по техническим причинам до восстановления ее работоспособности.

5.1.4. Производить плановую замену ключа ЭП, ключа проверки ЭП и сертификата ключа проверки ЭП по своей инициативе с уведомлением другой стороны не менее чем за два рабочих дня.

6. Ответственность Сторон и риски убытков

6.1. Стороны несут ответственность за содержание любого ПЭД при условии подтверждения подлинности ЭП.

6.2. Стороны несут ответственность за конфиденциальность и порядок использования ключей ЭП.

6.3. Сторона, допустившая компрометацию ключа ЭП, несет ответственность за ЭД, подписанные с использованием скомпрометированного ключа ЭП, до момента официального уведомления об аннулировании (отзыве) соответствующего сертификата и конкретных документов, подписанных указанным ключом.

6.4. Сторона, несвоевременно сообщившая о случаях утраты или компрометации ключа ЭП, несет связанные с этим риски.

6.5. В случае возникновения убытков сторона, не исполнившая (ненадлежащим образом исполнившая) обязательства по Соглашению, несет ответственность перед другой стороной за возникшие убытки. При отсутствии доказательств неисполнения (ненадлежащего исполнения) Сторонами обязательств по Соглашению риск убытков несет сторона, чьей ЭП подписан ЭД, исполнение которого повлекло за собой убытки.

6.6. Если в результате надлежащего исполнения ЭД возникает ущерб для третьих лиц, ответственность несет Сторона, от имени которой ЭД подписан ЭП.

6.7. Если одна из Сторон предъявляет другой Стороне претензии по электронному документу, при наличии подтверждения другой Стороной факта получения такого документа, а другая Сторона не может представить спорный электронный документ, виновной признается Сторона, не представившая спорный документ.

6.8. Стороны освобождаются от ответственности за частичное или полное неисполнение своих обязательств по Соглашению, если таковое явилось следствием обстоятельств непреодолимой силы, возникших после вступления в силу Соглашения, в результате событий чрезвычайного характера, которые не могли быть предвидены и предотвращены разумными мерами. Сторона обязана незамедлительно известить другую сторону о возникновении и прекращении действия обстоятельств непреодолимой силы, препятствующих исполнению ей обязательств по Соглашению, при этом срок выполнения обязательств по Соглашению переносится соразмерно времени, в течение которого действовали такие обстоятельства.

6.9. В случае прекращения действия Соглашения по любому основанию Стороны несут ответственность по обязательствам, возникшим до прекращения действия Соглашения, в соответствии с законодательством Российской Федерации.

7. Порядок создания ключа ЭП, ключа проверки ЭП, сертификатов ключей проверки ЭП, их использования и передачи

7.1. Ключ ЭП, ключ проверки ЭП и соответствующий сертификат ключа проверки ЭП создаются средствами ЭП Сторон или покупаются у сторонних организаций.

7.2. Используемые сертификаты и списки отозванных сертификатов должны соответствовать формату _____, описанному в спецификации _____.

7.3. Параметры сертификата должны быть следующими:

- алгоритм подписи - _____;

- длина ключа - _____;

- алгоритм хеширования - _____;

- срок действия - _____.

7.4. В поле "субъект" сертификата необходимо внести следующие сведения:

- CN = Ф.И.О. ответственного сотрудника, или наименование организации, или псевдоним;

- E = адрес электронной почты, совпадающий с адресом электронной почты, используемым для отправки ЭД;

- OU = наименование подразделения организации;

- O = название организации;

- L = город размещения организации;

- C = код страны (например, для России C = RU).

Остальные поля сертификата могут быть заполнены по желанию.

7.5. Сертификаты, используемые для формирования НЭП, должны иметь атрибуты расширенного использования ключа _____ и _____.

7.6. Сертификаты должны иметь запись с данными о точке распространения списка отозванных сертификатов, доступного по протоколу HTTP в Интернете.

7.7. Удостоверяющий центр должен добавлять в СОС отозванные сертификаты в течение __ часов и публиковать новый СОС в Интернете после каждого добавления.

7.8. Удостоверяющий центр, который используется для выдачи сертификатов, должен соответствовать всем требованиям к неаккредитованным удостоверяющим центрам, установленным Федеральным законом от 06.04.2011 N 63-ФЗ "Об электронной подписи".

7.9. Стороны обмениваются следующими сертификатами:

- корневой сертификат УЦ (если есть);

- промежуточные сертификаты (если есть);

- сертификат, который будет использоваться для подписи ЭД в Системе.

7.10. Файл сертификата должен быть в формате _____.

7.11. Файлы сертификатов передаются другой стороне по электронной почте или через Систему, если она уже функционирует.

7.12. Корневой сертификат, а при его отсутствии самоподписанный, Стороны печатают на бумажном носителе, подписывают ответственным лицом с оттиском печати организации и отправляют другой стороне курьером или передают друг другу в момент подписания данного Соглашения.

7.13. Стороны обязуются принимать все необходимые меры для сохранения конфиденциальности ключей ЭП.

7.14. Система средствами ЭП для каждого полученного ПЭД должна проверить:

- подлинность ЭП для данного ПЭД;

- факт того, что дата формирования ЭП находится в интервале от даты начала действия сертификата до даты завершения его действия;

- корректность самого сертификата, используемого для формирования ЭП;

- корректность цепочки выдачи сертификатов от используемого для подписи до корневого;

- выполнение требований к ограничению использования сертификата, записанных в самом сертификате;

- отсутствие используемого сертификата в списке отозванных сертификатов стороны, выдавшей этот сертификат.

7.15. При плановой замене сертификата ключа проверки ЭП сторона генерирует новые ключи и соответствующий сертификат и отправляет файл сертификата другой стороне по электронной почте или через Систему.

7.16. При компрометации ключа ЭП (или обоснованных подозрениях в компрометации), используемого для формирования НЭП в ПЭД, сторона должна:

- остановить передачу ПЭД в Системе и немедленно (если невозможно, то в течение __ часов) уведомить другую сторону о факте компрометации сертификата;

- произвести генерацию нового ключа ЭП, ключа проверки ЭП и выпустить в УЦ новый сертификат ключа проверки ЭП;

- передать другой стороне файл с новым сертификатом;

- внести в список отозванных сертификатов своего УЦ серийный номер скомпрометированного сертификата и опубликовать новый СОС;

- восстановить работу Системы по согласованию с другой стороной.

7.17. При компрометации корневого и (или) промежуточного ключа ЭП удостоверяющего центра сторона выполняет действия, указанные в предыдущем пункте, а также другие действия согласно своей нормативной документации.

7.18. Подписание настоящего Соглашения свидетельствует об обмене сертификатами.

8. Порядок разрешения споров, связанных с установлением подлинности ЭД

8.1. Любые споры между Сторонами, предметом которых является установление подлинности, то есть целостности текста и аутентичности отправителя ЭД, передаются для разрешения специально создаваемой Экспертной комиссии.

8.2. Экспертная комиссия созывается на основании письменного заявления (претензии) любой из Сторон. В указанном заявлении сторона указывает реквизиты оспариваемого ПЭД и лиц,

уполномоченных представлять интересы этой стороны в составе Экспертной комиссии.

8.3. Не позднее __ рабочих дней с момента получения другой стороной заявления (претензии) Стороны определяют дату, место и время начала работы Экспертной комиссии, а также определяют, какая сторона предоставляет персональный компьютер и производит конфигурирование средства ЭП.

8.4. Полномочия членов Экспертной комиссии подтверждаются доверенностями.

8.5. Состав Экспертной комиссии формируется в равных пропорциях из числа представителей Сторон.

8.6. Экспертиза оспариваемого ЭД осуществляется в присутствии всех членов Экспертной комиссии.

8.7. Экспертиза осуществляется в четыре этапа:

1-й этап: Стороны совместно устанавливают, конфигурируют и тестируют средство ЭП.

2-й этап: Стороны предоставляют свою копию сертификата ключа проверки ЭП, используемого для создания НЭП оспариваемого ПЭД, а также корневого и промежуточных сертификатов УЦ.

3-й этап: Экспертная комиссия с помощью средства ЭП получает ключи проверки ЭП из сертификатов, предоставленных Сторонами, и сравнивает их с соответствующими ключами из сертификатов, переданными Сторонам на основании пункта 7.11 настоящего Соглашения. Сертификаты, ключи проверки ЭП которых совпали, признаются подлинными. Также сравнивается корневой сертификат, переданный на бумажном носителе до подписания Соглашения, с только что предоставленным сертификатом. Экспертная комиссия с помощью средства ЭП проверяет, выпущен ли сертификат ключа проверки ЭП, использованный для подписи оспариваемого ПЭД, с использованием корневого и промежуточных ключа ЭП УЦ.

4-й этап: проверка правильности ЭП под оспариваемым документом, предоставленным стороной получателем, проверяется по сертификату принимающей стороны, подлинность которого подтверждена как указано выше.

8.8. Подтверждением подлинности оспариваемого ПЭД является одновременное наличие следующих условий:

- проверка подлинности ЭП оспариваемого ЭД дала положительный результат;

- подтверждена принадлежность сертификата ключа проверки ЭП, использованного для проверки подлинности ЭП в оспариваемом ЭД;

- ЭД сформирован в Системе и передан для обработки в соответствии с положениями настоящего Соглашения.

8.9. Результаты экспертизы оформляются в виде письменного заключения - Акта Экспертной комиссии, подписываемого всеми членами Экспертной комиссии. Акт составляется немедленно после завершения третьего этапа экспертизы. В Акте фиксируются результаты всех этапов проведенной экспертизы, а также все существенные реквизиты оспариваемого ПЭД. Акт составляется в двух экземплярах - по одному для каждой из Сторон. Акт комиссии является

окончательным и пересмотру не подлежит.

8.10. Подтверждение подлинности ЭП в оспариваемом ПЭД, зафиксированное в Акте, будет означать, что этот ПЭД имеет юридическую силу и влечет возникновение прав и обязательств Сторон, установленных Основным договором и Соглашением. Неподтверждение подлинности ЭП в оспариваемом ПЭД, зафиксированное в Акте, будет означать, что этот ПЭД не имеет юридической силы и не влечет возникновение каких-либо прав или обязательств Сторон, установленных Основным договором и Соглашением.

8.11. Стороны признают, что Акт, составленный Экспертной комиссией, является обязательным для Сторон и может служить доказательством при дальнейшем разбирательстве спора в Арбитражном суде.

8.12. В случае отсутствия согласия по спорным вопросам и добровольного исполнения решения Экспертной комиссии, все материалы по этим вопросам могут быть переданы на рассмотрение в _____ суд по адресу: _____.

9. Порядок смены ключей шифрования и ЭП

9.1. Порядок выдачи, замены ключей шифрования и ЭП, сертификатов ключей подписи, в том числе в случаях их компрометации, для Сторон определяется в соответствии с действующими регламентами УЦ взаимодействующих Сторон.

10. Уполномоченные лица

10.1. Уполномоченными лицами на использование ЭП от имени Сторон являются:

от Стороны 1 - _____;

от Стороны 2 - _____.

11. Адреса и реквизиты Сторон

Сторона 1:	Сторона 2:
Наименование/Ф.И.О.: _____	Наименование/Ф.И.О.: _____
Адрес: _____	Адрес: _____
_____	_____
ОГРН/ОГРНИП _____	ОГРН/ОГРНИП _____
ИНН _____	ИНН _____
КПП _____	КПП _____
Р/с _____	Р/с _____
в _____	в _____
К/с _____	К/с _____
БИК _____	БИК _____
ОКПО _____	ОКПО _____
(вариант:	(вариант:
_____	_____
(Ф.И.О.)	(Ф.И.О.)
Адрес: _____	Адрес: _____
_____	_____
Паспортные данные: _____	Паспортные данные: _____
_____	_____
Телефон: _____	Телефон: _____
Адрес электронной почты: _____	Адрес электронной почты: _____

Счет _____) Счет _____)

Подписи Сторон

Сторона 1:	Сторона 2:
_____/_____	_____/_____
(подпись) (Ф.И.О.)	(подпись) (Ф.И.О.)