**Порядок и условия обмена электронными документами**

**1. Термины и определения**

1.1. В настоящих Процедурах применяются следующие термины:

## **Авторство документа** - принадлежность документа одной из Сторон по настоящему Соглашению.

## **Владелец Сертификата** – уполномоченное лицо одной из Сторон, на имя которого Удостоверяющим центром выдан Сертификат ключа проверки электронной подписи и которое владеет соответствующим Ключом ЭП, позволяющим создавать свою Квалифицированную электронную подпись в Электронных документах (подписывать Электронные документы) с помощью Средств ЭП, и однозначно связанным с ним Ключом проверки ЭП.

## **Документ в бумажной форме (документированная информация)** - зафиксированная в бумажной форме информация с реквизитами, позволяющими ее идентифицировать.

**Документ в электронной форме (электронный документ)** - информация, представленная в электронной форме в виде файла или записи базы данных, подписанная электронной подписью и хранящаяся на магнитном, оптическом или ином носителе.

## **Зашифрование данных** - процесс преобразования открытых данных в зашифрованные при помощи шифра. Для зашифрования данных используется сертифицированные ФСБ программное средство криптографической защиты информации «КриптоПро CSP» и ПО «КриптоАРМ».

## **Защита информации** – комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.

**Квалифицированная электронная подпись (квалифицированная ЭП, КЭП)** –электронная подпись, которая соответствует следующим признакам:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

5) ключ проверки электронной подписи указан в квалифицированном сертификате;

6) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с законодательством Российской Федерации.

КЭП создается с помощью подтвержденных ФСБ криптографических средств и имеет сертификат от аккредитованного удостоверяющего центра, выступающего гарантом подлинности подписи. Электронный документ, подписанный КЭП, во всех случаях приравнивается законодательством к бумажному документу с собственноручной подписью. Квалифицированная подпись признается действительной до тех пор, пока решением суда не установлено иное.

## **Компрометация ключа** - утрата доверия к тому, что используемые ключи обеспечивают подлинность, защищенность и безопасность информации, а также доверия к тому, что Ключ ЭП не может быть использован третьими лицами. К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие:

1. утрата ключевого носителя;
2. утрата ключевого носителя с последующим обнаружением;
3. увольнение сотрудников, имевших доступ к ключевой информации;
4. возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
5. нерасшифровывание входящих или исходящих сообщений у абонентов.

**Корректная ЭП** – ЭП, дающая положительный результат при ее проверке с использованием действующего на момент проверки Сертификата, соответствующего Ключу ЭП, с использованием которого сформирована проверяемая ЭП.

**Ключ проверки электронной подписи (Ключ проверки ЭП)** – уникальная последовательность символов, однозначно связанная с Ключом ЭП и предназначенная для проверки подлинности ЭП в Электронном документе.

**Ключ электронной подписи (Ключ ЭП)** – уникальная последовательность символов, предназначенная для создания ЭП в Электронных документах с использованием Средств ЭП.

## **Криптографическая защита** - защита данных при помощи криптографического преобразования данных.

## **Криптографическое преобразование** - преобразование данных при помощи шифрования и (или) выработки имитовставки.

**Некорректный электронный документ** - электронный документ, не прошедший процедуры расшифрования данных, проверки электронной подписи, контроля формата документов, а также документ, имеющий искажения в тексте сообщения (наличие символов, букв или цифр в расшифрованном (открытом) тексте документа, не позволяющих понять его смысл).

**Некорректная ЭП –** ЭП, дающая отрицательный результат при проверке с использованием действующего на момент проверки Сертификата, соответствующего Ключу ЭП, с использованием которого сформирована проверяемая ЭП.

**Несанкционированный доступ к информации** - доступ к информации, нарушающий установленные правила разграничения доступа в результате случайных или преднамеренных действий пользователей или других субъектов, с использованием штатных средств, предоставляемых автоматизированной системой. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения автоматизированной системы.

**Обработка информации** - передача, прием, хранение, преобразование и отображение информации.

**Плановая смена ключей** - смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

**Подтверждение подлинности ЭП в Электронном документе** – процедура, дающая положительный результат проверки соответствующим Средством ЭП с использованием Сертификата принадлежности ЭП в Электронном документе Владельцу Сертификата и отсутствия искажений в подписанном данной ЭП Электронном документе.

**Проверка электронной подписи документа** - проверка соотношения ЭП под этим документом и ключа проверки ЭП Владельца Сертификата. Если рассматриваемое соотношение оказывается выполненным, то подпись признается корректной, а сам документ - подлинным, в противном случае документ считается измененным, а подпись под ним – некорректной.

**Расшифрование данных** - процесс преобразования зашифрованных данных в открытые при помощи шифра.

**Сертификат ключа проверки электронной подписи (Сертификат)** – Электронный документ или документ на бумажном носителе, который выдается Удостоверяющим центром и подтверждает принадлежность Ключа проверки ЭП Владельцу Сертификата. Сертификат применяется для Подтверждения подлинности ЭП в Электронном документе и идентификации Владельца Сертификата.

**Средства ЭП** – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка ЭП, создание Ключа ЭП и Ключа проверки ЭП.

**Стороны** – стороны, заключившие Соглашение об электронном документообороте.

**Удостоверяющий центр** - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче Сертификатов ключей проверки ЭП, а также иные функции, предусмотренные законодательством Российской Федерации.

## **Управление ключами** - создание (генерация) ключей, их хранение, распространение, удаление (уничтожение), учет и применение в соответствии с политикой безопасности.

## **Целостность информации** - свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

## **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. Для выработки и проверки электронной подписи используются сертифицированные ФСБ программное средство криптографической защиты информации «КриптоПро CSP» и ПО «КриптоАРМ».

## **Шифрование** - процесс зашифрования или расшифрования.

## **Шифрование документов (текстов)** - преобразование формы исходных (открытых) текстов сообщений таким образом, что их смысл становится непонятным для любого лица, не владеющего секретом обратного преобразования.

## **ЭДО** – электронный документооборот.

1.2. Остальные термины и определения, используемые в настоящих Процедурах ЭДО, должны пониматься в соответствии с действующим законодательством Российской Федерации.

**2. Общие положения**

2.1. Настоящие Процедуры ЭДО устанавливают условия перехода Сторон к ЭДО, порядок формирования, передачи, приема и обработки электронных документов.

2.2. Для начала работы Стороны:

2.2.1. подписывают Соглашение об электронном документообороте;

2.2.2. подписывают договор на предоставление и техническое сопровождение программных продуктов;

2.2.3. устанавливают СКЗИ и обмениваются ключами проверки ЭП;

2.2.4. подписывают Акт о начале электронного документооборота.

2.3. Обмен Электронными документами между Сторонами в соответствии с настоящими Процедурами осуществляется следующими средствами:

* электронной почтой по протоколу SMTP;
* средствами передачи файлов по протоколу FTP.

2.4. Стороны обязуются использовать для реализации шифрования и ЭП программный продукт «КриптоПро CSP». Использование иных программных продуктов должно оговариваться в отдельном соглашении Сторон.

2.5. Стороны осуществляют проверку аутентичности Электронных документов:

- с использованием средства криптографической защиты информации «КриптоПро CSP» (далее – СКЗИ) и ПО «КриптоАРМ», сертифицированных ФСБ;

- с использованием легальных электронных ключей, выданных лицензированной ФСБ организацией.

2.6. Стороны устанавливают, что во всех случаях обмена Электронными документами между Сторонами, Стороны применяют Квалифицированную ЭП.

2.7. Стороны признают, что:

2.7.1. Использование Средств ЭП, применяемых для формирования и проверки ЭП, обеспечивает подтверждение подлинности, авторства, целостности и неизменности Электронных документов, что позволяет достоверно установить, что Электронный документ исходит от Владельца Сертификата, ЭП которого присоединена к Электронному документу или иным образом связана с ним.

2.7.2. Использование ими Средств ЭП достаточно для защиты информации от несанкционированного доступа, а также разбора конфликтных ситуаций и споров, возникших в связи с осуществлением электронного документооборота.

2.7.3. Получение одной из Сторон Электронного документа, подписанного Квалифицированной ЭП и имеющего Корректную ЭП Владельца Сертификата, юридически эквивалентно получению данной Стороной идентичного по смыслу и содержанию документа на бумажном носителе, оформленного в соответствии с действующим законодательством Российской Федерации и подписанного собственноручной подписью, а в случаях, когда в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью одной из Сторон, электронный документ, подписанный Квалифицированной ЭП и имеющий Корректную ЭП Владельца Сертификата, признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью, и влечет такие же обязательства и правовые последствия для Сторон, как и идентичные по смыслу и содержанию документы на бумажном носителе, подписанные собственноручной подписью.

2.7.4.Действия Сторон, совершенные на основании Электронных документов, подписанных Корректной ЭП, не могут быть оспорены только на том основании, что эти действия не подтверждаются документами, составленными на бумажном носителе.

2.7.5.Каждая Сторона несет ответственность за сохранность (обеспечение конфиденциальности) своих Ключей ЭП и за действия по их использованию со своей Стороны при обмене ЭД.

2.8. Стороны признают, что ЭП обладает следующими свойствами, позволяющими обеспечить подтверждение авторства, целостности и неизменности Электронных документов:

2.8.1. создание Корректной ЭП Электронного документа невозможно без знания соответствующего Ключа ЭП;

2.8.2. при любом изменении Электронного документа его ЭП, сформированная до внесения изменений, становится Некорректной ЭП, то есть проверка ЭП с помощью Ключа проверки ЭП, указанного в действующем Сертификате дает отрицательный результат. Исправление или изменение Электронного документа, заверенного ЭП, возможно только путем создания нового Электронного документа;

2.8.3.знание третьими лицами информации, которая содержится в Сертификате, Электронных документах, созданной ЭП и Ключе проверки ЭП, не приводит к Компрометации Ключа ЭП.

2.9.Средствами ЭП и программными средствами, с которыми непосредственно функционируют Средства ЭП, обеспечивается выполнение всех требований, предусмотренных законодательством к средствам электронной подписи:

● представление Владельцу Сертификата, подписывающему Электронный документ, содержания информации, которую он подписывает;

● создание ЭП только после подтверждения Владельцем Сертификата, подписывающим Электронный документ, операции по созданию электронной подписи;

● представление Владельцу Сертификата, подписавшему Электронный документ информации, что ЭП создана.

Проверка подлинности ЭП, созданной Владельцем Сертификата, производится автоматически Средствами ЭП.

2.10. Подтверждением корректности ЭП является одновременное выполнение следующих условий:

2.10.2. в момент поступления Электронного документа и его проверки между Сторонами было заключено и не было расторгнуто Соглашение об ЭДО;

2.10.3. Сертификат Владельца ЭП, с помощью которого проверялась ЭП, в момент поступления Электронного документа одной из Сторон и его проверки являлся действующим, т.е. был зарегистрирован в установленном порядке, срок его действия не истек, его действие не было приостановлено и/или аннулировано;

2.10.4. подтверждена подлинность и целостность Ключа проверки ЭП, с помощью которого проводилась проверка ЭП;

2.10.5. проверка Электронного документа с помощью Сертификата дала положительный результат, т.е. подтвердила корректность ЭП, созданной к данному документу.

2.11. Выполнение всех условий, перечисленных в п. 2.10, означает, что корректность ЭП подтверждена, т.е. проверяемый Электронный документ подписан Корректной ЭП.

2.12. Невыполнение любого из условий, перечисленных в п. 2.10, означает, что корректность ЭП Электронного документа не подтверждена, т.е. проверяемый Электронный документ подписан Некорректной ЭП.

**3. Формирование электронных документов**

3.1. Для формирования Электронных документов Стороны вправе использовать собственное программное обеспечение или стандартное программное обеспечение.

3.2. Все формы документов, передаваемые в соответствии с настоящими Процедурами ЭДО, должны соответствовать формам документов, определенным соответствующими договорами и соглашениями Сторон об оказании услуг. 3.2. К файлам с Электронными документами предъявляются следующие требования:

* документы могут передаваться в текстовом или графическом форматах, формате XML (extended markup language) и переносимом формате документов PDF;
* файл с документом в текстовом формате должен иметь одно из следующих расширений RTF, DOC, TXT, XLS;
* файл с документом в графическом формате должен иметь расширение TIFF (тип формата – сжатый TIFF) или JPEG;
* файл с документом в формате XML должен иметь такое же расширение (XML).

Допускается передача Электронных документов, соответствующих указанным выше требованиям, в заархивированном виде (файлы с расширением ZIP, RAR).

**4. Прием-передача и обработка электронных документов**

4.1. Прием-передача и обработка Электронных документов Сторонами осуществляется в сроки не позднее времени, определенного соответствующими договорами и соглашениями Сторон об оказании услуг.

4.2. Прием Электронных документов производится путем расшифрования и проверки ЭП на полученных документах. По результатам приема Электронных документов Сторона-получатель направляет Стороне-отправителю электронное письмо, подтверждающее получение Электронных документов (далее – Отчет).

4.3. Если Сторона-отправитель Электронного документа не получила Отчет в течение дня, следующего за датой отправки соответствующего Отчета, то Сторона-отправитель по телефону информирует об этом Сторону-получателя. Последняя обязана незамедлительно отправить соответствующий Отчет.

4.4. Сторона-отправитель, допустившая некорректность при формировании Электронного документа, после получения уведомления об этом от стороны-получателя обязана незамедлительно направить другой Стороне исправленный Электронный документ.

**5. Порядок разрешения конфликтных ситуаций и споров,**

**возникших в связи с осуществлением электронного документооборота**

5.1. При возникновении конфликтных ситуаций, споров между Сторонами, связанных с установлением авторства и целостности Электронного документа, подготовленного и переданного по электронной почте в соответствии с Соглашением об электронном документообороте, Сторона-инициатор в срок три рабочих дня с момента, когда ей стало известно о нарушении ее права, обязана направить другой Стороне уведомление о конфликтной ситуации, с подробным изложением обстоятельств происшедшего.

5.2. Сторона, которой направлено уведомление, обязана незамедлительно, но не позднее, чем в течение следующего рабочего дня, проверить наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и направить уведомителю информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации.

5.3. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от Стороны, которой направлялось уведомление.

5.4. В случае, если уведомитель не удовлетворен информацией, полученной от другой Стороны, для рассмотрения конфликтной ситуации формируется Согласительная комиссия.

5.5. Не позднее чем на следующий рабочий день после того, как принято решение о необходимости сформировать Согласительную комиссию, или не позднее, чем на шестой рабочий день после получения уведомления о конфликтной ситуации, в случае, если конфликтная ситуация не была урегулирована в рабочем порядке, Согласительная комиссия должна быть сформирована.

5.6. В состав Согласительной комиссии входит равное количество, но не менее чем по одному уполномоченному представителю каждой из конфликтующих сторон. В состав Согласительной комиссии, как правило, назначаются специалисты из числа сотрудников технических служб, служб информационной безопасности сторон. Лица, входящие в состав Согласительной комиссии, должны обладать необходимыми знаниями в области построения системы криптозащиты, работы компьютерных информационных систем.

5.7. Сформированная Согласительная комиссия при рассмотрении конфликтной ситуации устанавливает на технологическом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о факте и времени составления и/или отправки Электронного документа, его подлинности, а также о подписании Электронного документа конкретной электронной подписью, аутентичности отправленного документа полученному.

5.8. По результатам работы Согласительной комиссией принимается решение простым большинством голосов членов комиссии. Решение комиссии фиксируется в Акте, который составляется и подписывается всеми членами Согласительной комиссии.

5.9.  В Акте в обязательном порядке отражаются:

* установленные обстоятельства;
* действия членов Комиссии;
* выводы, влияющие на возможность установления подлинности оспариваемых документов.

5.10. Акт, составленный Согласительной комиссией, является доказательством при дальнейшем разбирательстве спора в суде.

5.11. В случае, если конфликтная ситуация полностью или частично не урегулирована в результате работы Согласительной комиссии, то такие споры и/или разногласия разрешаются в порядке, установленном действующим законодательством Российской Федерации.

**6. Разрешение споров**

* 1. В случае возникновения споров о наличии ЭП на Электронном документе бремя доказывания лежит на Стороне, не соглашающейся с наличием ЭП.
	2. В случае возникновении споров о факте внесения изменений в Электронный документ после его подписания ЭП бремя доказывания лежит на Стороне, утверждающей, что в данный документ были внесены изменения после подписания данного документа сотрудником этой Стороны.
	3. В случае возникновения споров о факте получения одной из Сторон какого-либо документа, подписанного ЭП, от другой Стороны бремя доказывания лежит на Стороне, не соглашающейся с фактом получения кем-либо Электронного документа, подписанного ЭП.