



МИНИСТЕРСТВО ФИНАНСОВ ЧЕЛЯБИНСКОЙ ОБЛАСТИ

ПРИКАЗ

от 15.10.2015 г.

№ 01/5-196

О Регламенте применения
электронной подписи сторонами
юридически значимого электронного
документооборота

В целях организации и выполнения работ по внедрению юридически значимого электронного документооборота на базе автоматизированной системы Министерства финансов Челябинской области

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемый Регламент применения электронной подписи сторонами юридически значимого электронного документооборота.

2. Признать утратившими силу:

1) приказ Министерства финансов Челябинской области от 09.04.2013г. № 01/5-30 «О регламенте применения электронной подписи сторонами юридически значимого электронного документооборота»;

2) пункт 7 приказа Министерства финансов Челябинской области от 07.10.2013г. № 01/5-107 «О внесении изменений в отдельные приказы Министерства финансов Челябинской области»;

3) приказ Министерства финансов Челябинской области от 16.01.2014г. № 01/5-6 «О внесении изменений в приказ Министерства финансов Челябинской области от 09.04.2013г. № 01/5-30»;

4) приказ Министерства финансов Челябинской области от 26.03.2014г. № 01/5-33 «О внесении изменений в приказ Министерства финансов Челябинской области от 09.04.2013г. № 01/5-30»;

5) приказ Министерства финансов Челябинской области от 31.12.2014г. № 01/5-184 «О внесении изменений в приказ Министерства финансов Челябинской области от 09.04.2013г. № 01/5-30»;

6) приказ Министерства финансов Челябинской области от 14.05.2015г. № 01/5-65 «О внесении изменений в приказ Министерства финансов Челябинской области от 09.04.2013г. № 01/5-30»;

7) приказ Министерства финансов Челябинской области от 20.08.2015г. № 01/5-149 «О внесении изменений в приказ Министерства финансов Челябинской области от 09.04.2013г. № 01/5-30».

3. Контроль за выполнением настоящего приказа возложить на первого заместителя Министра финансов Челябинской области Грязева А.А. и первого заместителя Министра финансов Челябинской области Прыгунова А.Е.

Министр

А.В. Пшеницын

УТВЕРЖДЕН
приказом Министерства финансов
Челябинской области
от 15.10.2015 г. № 01/5-196
(редакции от 31.12.2015г. № 01/5-260)

Регламент
применения электронной подписи сторонами юридически
значимого электронного документооборота

I. Общие положения

1.1. Настоящий Регламент применения электронной подписи сторонами юридически значимого электронного документооборота (далее – Регламент) определяет порядок и технические аспекты использования юридически значимого электронного документооборота (далее – ЮЗЭД) между Министерством финансов Челябинской области (далее – Минфин области) и участниками ЮЗЭД, заключившими с Минфином области соглашение об обмене электронными документами (далее именуемые совместно – стороны), в автоматизированной системе Министерства финансов Челябинской области, статусы электронных документов, на которых происходит наложение электронной подписи в электронном документе, правила разбора конфликтных ситуаций, возникающих между сторонами ЮЗЭД в ходе подписания электронных документов электронной подписью.

1.2. Такие термины и понятия, как «квалифицированный сертификат ключа проверки электронной подписи» (далее – сертификат), «ключ электронной подписи» (далее – ключ), «усиленная квалифицированная электронная подпись» (далее – электронная подпись) и «электронный документ», используемые в настоящем Регламенте, применяются в том же значении, что и в Федеральном законе от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» (далее – Закон № 63-ФЗ).

Иные термины и понятия, используемые в настоящем Регламенте:

автоматизированная система Министерства финансов Челябинской области – программный комплекс, предназначенный для автоматизации бюджетного процесса в Челябинской области (далее – Система)

юридически значимый электронный документооборот (ЮЗЭД) – документооборот на базе Системы, в котором стороны совершают действия по принятию к исполнению документов в электронной форме, удостоверяемых электронной подписью, и несут ответственность за указанные действия;

удостоверяющий центр – Минфин области, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции аккредитованного удостоверяющего центра, предусмотренные Законом № 63-ФЗ в соответствии с регламентом удостоверяющего центра, утвержденным приказом Минфина области;

администратор системы – специалист Минфина области, ответственный за настройку Системы и внесение в реестр Системы сертификатов электронной подписи;

администратор информационной безопасности – специалист, ответственный за обеспечение информационной безопасности в Минфине области.

клиент – финансовый орган муниципального образования, главный распорядитель, распорядитель и получатель средств областного бюджета, областное бюджетное учреждение и областное автономное учреждение, юридическое лицо, которому из областного бюджета предоставляется субсидия (за исключением областного бюджетного учреждения и областного автономного учреждения), территориальный фонд обязательного медицинского страхования, Главное управление МВД России по Челябинской области, заключившие соглашение об обмене электронными документами с Минфином области;

в редакции приказа МФ ЧО от 31.12.2015г. № 01/5-260

уполномоченное лицо – должностное лицо, наделенное правом использования электронной подписи в электронных документах, формируемых в Системе;

представитель клиента – должностное лицо клиента, уполномоченное действовать от его имени;

средства криптографической защиты информации (далее – СКЗИ) – аппаратно-программный комплекс, выполняющий функцию по созданию электронной подписи, а также обеспечивающий защиту информации по утвержденным стандартам и сертифицированный в соответствии с законодательством;

правила подписания – настроечный параметр Системы, позволяющий установить права на подписание электронных документов электронной подписью для определенных ролей на определенных статусах согласно приложению 1, 5 к настоящему Регламенту;

роль – совокупность прав уполномоченных лиц при работе в Системе, с использованием которых уполномоченные лица подписывают электронные документы электронной подписью;

статус электронного документа – атрибут электронного документа, идентифицирующий его состояние по определенному признаку;

материальный носитель – материальный объект, используемый для записи и хранения информации, необходимой для подписания электронных документов электронной подписью;

подтверждение подлинности электронной подписи в электронном документе – положительный результат подтверждения сертифицированным средством электронной подписи принадлежности содержащейся в электронном документе электронной подписи ее владельцу и отсутствия искажения и подделки подписанного данной электронной подписью электронного документа.

II. Порядок применения электронной подписи

2.1. В ходе использования ЮЗЭД принимаются и признаются сертификаты, изданные удостоверяющим центром.

2.2. Для определения статуса сертификата используется список отозванных сертификатов, издаваемый и публикуемый удостоверяющим

центром в порядке и с периодичностью, определяемой удостоверяющим центром.

2.3. В качестве средства электронной подписи используются СКЗИ, сертифицированные в соответствии с законодательством Российской Федерации, а также совместимые с Системой и обеспечивающие:

реализацию функций создания электронной подписи в электронном документе с использованием ключа;

подтверждение подлинности электронной подписи в электронном документе с использованием сертификата.

2.4. Функционирование ЮЗЭД происходит на базе Системы.

2.5. Минфин области вправе обновлять версию Системы с дальнейшей эксплуатацией ЮЗЭД на обновленной версии без предварительных уведомлений клиента, если такие изменения не повлекут существенных изменений Системы.

2.6. Перечень документов в электронном виде с применением электронной подписи без их представления на бумажном носителе устанавливается приказом Минфина области.

2.7. Электронные копии подтверждающих документов прикрепляются к электронным документам в Системе, подписываются электронной подписью.

2.8. Требования к составу подписываемых полей юридически значимых электронных документов определяет Минфин области. Клиент имеет право быть ознакомленным с составом подписываемых полей юридически значимых электронных документов.

2.9. При подписании электронных документов применяются электронные подписи лиц, имеющих право подписи в соответствии с правилами подписания электронных документов согласно приложению 1, 5 к настоящему Регламенту.

2.10. Минфин области осуществляет обработку документов в Системе после подписания клиентами документов электронной подписью в соответствии с правилами подписания электронных документов согласно приложению 1, 5 к настоящему Регламенту.

2.11. Минфин области осуществляет контроль за соблюдением правил подписания электронных документов, предусмотренных приложением 1,5 к настоящему Регламенту.

2.12. Порядок осуществления операций по межбюджетным трансфертам с применением электронной подписи между Минфином области и участником межбюджетных расчетов определяется подписанным сторонами Регламентом о порядке и условиях обмена информацией между Минфином области и участником межбюджетных расчетов при оформлении операций по межбюджетным трансфертам.

III. Порядок работы в операционном зале Минфина области

3.1. В случае невозможности создания электронных документов на рабочем месте клиента представитель клиента может обратиться в Минфин области для создания электронных документов в Системе в операционном зале Минфина области (далее - оперзал).

3.2. Представитель клиента при обращении представляет в отдел технического и системного программного обеспечения Минфина области обязательство о неразглашении конфиденциальной информации по форме согласно приложению 2 к настоящему Регламенту (далее - Обязательство), а также обращение в Минфин области в письменном виде за подписью руководителя и главного бухгалтера клиента.

3.3. Администратор информационной безопасности проверяет представленные представителем клиента Обязательство на, соответствие формы, реквизитов, подлежащих заполнению, наличия исправлений, а также осуществляет идентификацию представителя клиента по паспорту. В случае отсутствия замечаний разрешает допуск к Системе в оперзале.

В случае нарушения установленного порядка представления документов администратор информационной безопасности отказывает в допуске к работе в Системе в оперзале.

3.4. В случае утраты пароля для входа в Систему клиент обязан уведомить об этом в письменной форме управление информационных систем Минфина области, а также предоставить заявку на создание нового пароля.

3.5. Для работы в Системе в оперзале представитель клиента должен иметь при себе:

материальный носитель, содержащий ключ электронной подписи, на использование которой удостоверяющим центром выдан сертификат ключа проверки электронной подписи;

отсканированные копии документов в электронном виде, которые должны быть прикреплены к созданным документам в Системе (в случае невозможности доставить отсканированные копии документов в электронном виде на USB-флеш-карте снятие копии подтверждающих документов в электронном виде осуществляется в оперзале).

3.6. Для подписания электронной подписью электронных документов представителю клиента необходимо иметь документы на право подписи, в т.ч. соответствующий приказ клиента и карточку с образцами подписей и оттиска печати клиента.

Представитель клиента обеспечивает установку личных сертификатов электронной подписи в Системе в оперзале.

В случае, если в соответствии с правилами подписания электронного документа необходимы две электронные подписи, а прибытие в оперзал уполномоченного лица невозможно, право использования электронной подписи может быть передано приказом клиента представителю клиента, прибывшему в Минфин области.

Минфин области не осуществляет контроль за действиями клиента по передаче прав на использование электронной подписи иным уполномоченным лицам.

3.7. После окончания работы представитель клиента обязан сообщить о завершении работы в Системе ответственному за оперзал сотруднику управления областного казначейства Минфина области.

IV. Порядок работы со СКЗИ в Системе

4.1. Для работы со СКЗИ в Системе допускаются только уполномоченные лица клиента, которые несут персональную ответственность за сохранность СКЗИ (в том числе хранение в тайне ключей электронной подписи).

Клиент обеспечивает контроль за отсутствием на компьютере, на котором осуществляется ЮЗЭД, посторонних программ (вирусов и так далее), способствующих нарушению функционирования ЮЗЭД, и несет ответственность за невыполнение указанных требований.

4.2. При обнаружении на компьютере, на котором осуществляется ЮЗЭД, посторонних программ (вирусов и так далее), эксплуатация ЮЗЭД на этом компьютере должна прекратиться с дальнейшей организацией мероприятий по анализу и ликвидации посторонних программ и возможных последствий.

4.3. Категорически запрещается:

разглашать содержимое материальных носителей, содержащих ключи электронной подписи, или передавать сами материальные носители лицам, к ним не допущенным, выводить данные, содержащиеся на материальном носителе, на дисплей и принтер;

вставлять материальный носитель, содержащий ключи электронной подписи, в дисковод или USB-считыватель компьютера уполномоченного лица клиента или других лиц при осуществлении деятельности, не связанной с ЮЗЭД;

записывать на материальный носитель, содержащий ключи электронной подписи, постороннюю информацию;

вносить какие-либо изменения в программное обеспечение СКЗИ;

использовать бывшие в работе материальные носители (правило не распространяется на носитель типа RuToken, eToken и USB-флеш).

Клиент несет ответственность за проведение в полном объеме организационных и технических мероприятий, обеспечивающих соблюдение указанных в настоящем пункте запретов.

4.4. В случае установления факта компрометации ключа уполномоченное лицо обязано прекратить работу по осуществлению ЮЗЭД и в течение не более чем одного рабочего дня со дня возникновения компрометации, подозрения на компрометацию уведомить об этом администратора информационной безопасности.

Возобновление работы уполномоченного лица по осуществлению ЮЗЭД происходит только после замены скомпрометированного ключа.

К событиям, связанным с компрометацией ключей, относятся следующие:

утрата материальных носителей, содержащих ключи электронной подписи, в том числе с их последующим обнаружением;

разглашение содержимого материальных носителей, содержащих ключи электронной подписи;

несанкционированное копирование содержимого материальных носителей, содержащих ключи электронной подписи;

использование ключа электронной подписи после увольнения уполномоченного лица;

нарушение правил хранения материальных носителей, содержащих ключи электронной подписи, и их уничтожения после окончания срока действия;

нарушение печати на сейфе или замка сейфа, в котором хранятся материальные носители, содержащие ключи электронной подписи;

любые другие виды разглашения содержимого материальных носителей, содержащих ключи электронной подписи, в результате которых ключи могут стать доступными посторонним лицам и (или) процессам.

V. Порядок разбора конфликтных ситуаций при осуществлении ЮЗЭД

5.1. Под конфликтной ситуацией понимается ситуация, которая может быть вызвана следующими разногласиями между сторонами (клиентом и Минфином области):

оспаривание факта отправления и (или) получения электронного документа;

оспаривание времени отправления и (или) получения электронного документа;

оспаривание содержания отправленного (полученного) электронного документа;

оспаривание идентичности экземпляров электронного документа подлиннику и копии документа на бумажном носителе;

оспаривание целостности электронного документа;

оспаривание полномочий лица, подписавшего электронный документ электронной подписью;

оспаривание правомерности использования сертификата, использованного для подписания электронного документа;

иные случаи возникновения конфликтных ситуаций в ходе обмена электронными документами.

5.2. Разрешая конфликтные ситуации, стороны исходят из того, что документ в электронном виде, подписанный электронной подписью в Системе, является документом, имеющим юридическую силу, аналогичным документу на бумажном носителе, подписанному собственноручной подписью уполномоченного лица и заверенному печатью клиента.

Электронный документ порождает обязательства, если документ надлежащим образом оформлен, подписан электронной подписью и доставлен. При этом электронная подпись используется в соответствии с сертификатом, действующим на момент подписания документа.

Математические свойства алгоритма электронной подписи должны соответствовать стандартам, существующим в Российской Федерации. Разбор конфликтной ситуации в отношении авторства, целостности и подлинности электронного документа заключается в доказательстве подписания конкретного электронного документа с использованием конкретного ключа электронной подписи.

Разрешение конфликтных ситуаций между сторонами осуществляется несколькими способами:

в рабочем порядке (без создания экспертной комиссии);

с созданием в Минфине области экспертной комиссии;

в судебном порядке.

5.2.1. Разрешение конфликтных ситуаций в рабочем порядке.

В случае возникновения обстоятельств, свидетельствующих, по мнению одной из Сторон, о возникновении конфликтной ситуации, данная Сторона (далее – Сторона-инициатор) незамедлительно направляет другой Стороне в произвольной форме извещение о конфликтной ситуации, обстоятельствах, свидетельствующих о ее возникновении, а также о ее предполагаемых причинах.

Сторона, которой было направлена извещение о конфликтной ситуации (далее – Сторона-ответчик), обязана не позднее чем в течение следующего рабочего дня проверить наличие указанных в извещении обстоятельств и, при необходимости, принять меры по разрешению конфликтной ситуации со своей стороны.

В тот же срок Сторона-ответчик извещает доступным способом Сторону-инициатора о результатах проверки и, при необходимости, о мерах, принятых для разрешения конфликтной ситуации,

Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если Сторона-инициатор удовлетворена информацией, содержащейся в извещениях Стороны-ответчика, не имеет к ней претензий, и информация представлена в установленный срок.

В случае если Сторона-инициатор не удовлетворена информацией, полученной от Стороны-ответчика, для рассмотрения конфликтной ситуации формируется экспертная комиссия.

5.2.2. Разрешение конфликтных ситуаций с созданием экспертной комиссии.

В случае, если конфликтная ситуация не была разрешена в рабочем порядке, Сторона-инициатор не позднее трех рабочих дней после возникновения конфликтной ситуации направляет Стороне-ответчику уведомление о разногласиях (далее – Уведомление) и предложение о создании экспертной комиссии (далее – Предложение). При этом до направления Уведомления Стороне-инициатору необходимо убедиться в целостности установленного на его технических средствах программного обеспечения, в том числе средств электронной подписи, а также в том, что не было произведено несанкционированных действий относительно программного обеспечения и на его технических средствах не установлено вредоносного программного обеспечения.

Уведомление должно содержать следующую информацию:

дату и номер;

наименование организации;

название класса электронного документа и его номер в Системе;

обстоятельства, на которых основаны заявленные требования и сведения о подтверждающих их доказательствах, о наличии конфликтной ситуации, возможных причинах и последствиях ее возникновения;

дату и время подписания (по системному журналу);

нарушенные нормы законодательных и иных нормативных правовых актов Российской Федерации, а также условий соглашения об обмене электронными документами между Сторонами.

Если Стороной-инициатором является клиент, то к Уведомлению должны быть приложены следующие документы:

файл, содержащий электронный документ, а также электронную подпись этого электронного документа (выгружается из Системы);

файл, содержащий вложение электронного документа, а также электронную подпись этого вложения электронного документа (выгружается из Системы);

файлы, содержащие сертификаты ключей электронной подписи, с использованием которых подписан электронный документ.

Предложение должно содержать следующую информацию:

предполагаемую дату (не позднее трех рабочих дней со дня отправления Уведомления), время и место сбора экспертной комиссии;

список предлагаемых для участия в работе экспертной комиссии представителей Стороны-инициатора с указанием фамилий, имен, отчеств, должностей, исполняемых при обмене электронными документами функциональных ролей (администратор, администратор безопасности), контактной информации (телефон, электронная почта, факс).

Уведомление и Предложение составляются в произвольной форме на бумажном носителе, подписываются руководителем Стороны-инициатора (либо его заместителем).

Не позднее следующего рабочего дня после получения Уведомления и Предложения от Стороны-инициатора Сторона-ответчик направляет Стороне-инициатору свои Предложения, подписанные руководителем Стороны-ответчика (либо его заместителем).

Состав экспертной комиссии, время, место и срок ее работы утверждаются приказом Минфина области.

По инициативе любого из участников, участвующих в разрешении конфликтной ситуации, к работе экспертной комиссии могут привлекаться независимые эксперты, представители разработчика программного обеспечения Системы (по согласованию).

Лица, входящие в состав экспертной комиссии, должны обладать необходимыми знаниями и опытом работы с электронными документами, а также в области организации и обеспечения информационной безопасности при обмене электронными документами, иметь соответствующий допуск к необходимым для проведения работы экспертной комиссии документам и программно-техническим средствам.

Экспертная комиссия имеет право:

получать доступ к необходимым для ее работы документам участников, в том числе к архивам электронных документов;

знакомиться с условиями и порядком подготовки, формирования, обработки, доставки, исполнения, хранения и учета электронных документов участников;

знакомиться с условиями и порядком эксплуатации программных и технических средств обмена электронными документами участников;

знакомиться с условиями и порядком изготовления, использования и хранения участниками ключей, иной конфиденциальной информации, а также

материальных носителей, необходимых для работы средств обмена электронными документами;

получать объяснения от должностных лиц Сторон, обеспечивающих обмен электронными документами;

получать от Сторон любую иную информацию, относящуюся к разрешаемой конфликтной ситуации.

Для проведения необходимых проверок и документирования данных экспертной комиссией могут применяться специальные программные и технические средства.

5.2.2.1. Порядок работы экспертной комиссии.

Сторона-ответчик обязана представить экспертной комиссии документально обоснованные объяснения и (или) доказательства по каждому вопросу, изложенному в Уведомлении.

В ходе работы экспертной комиссии может быть вынесено (в письменной форме) на рассмотрение экспертной комиссии ходатайство об изменении или дополнении требований или возражений любой из Сторон.

Экспертная комиссия может затребовать от Сторон предоставления документов и иных доказательств, необходимых для разрешения конфликтной ситуации между сторонами.

В том случае, если обстоятельства требуют подтверждения факта подлинности электронной подписи в электронном документе, экспертная комиссия назначает экспертизу по подтверждению подлинности электронной подписи. Проведение экспертизы осуществляется уполномоченными сотрудниками удостоверяющего центра, входящими в состав экспертной комиссии.

Все действия, предпринимаемые экспертной комиссией для выяснения фактических обстоятельств конфликтной ситуации, а также соответствующие выводы заносятся в протокол работы экспертной комиссии, который составляется по итогам работы.

Протокол работы экспертной комиссии должен содержать следующую информацию:

дату начала и окончания работы экспертной комиссии и место составления протокола;

состав экспертной комиссии с указанием фамилий, имен, отчеств, мест работы, занимаемых должностей, исполняемых при обмене электронными документами функциональных ролей, контактной информации и квалификации членов экспертной комиссии;

краткое изложение обстоятельств, свидетельствующих о возникновении и (или) наличии конфликтной ситуации;

установленные экспертной комиссией фактические обстоятельства;

мероприятия, проводимые экспертной комиссией для установления наличия, причин возникновения и последствий возникшей конфликтной ситуации, с указанием даты, времени и места их проведения;

выводы, к которым пришла экспертная комиссия в результате проведенных мероприятий;

принятое решение экспертной комиссии;

подписи всех членов экспертной комиссии.

Протокол должен быть составлен в форме документа на бумажном носителе в двух экземплярах, по одному для каждого из Сторон. По обращению любого из членов экспертной комиссии может быть выдана заверенная Минфином области копия протокола.

При наличии особого мнения члена экспертной комиссии к протоколу экспертной комиссии прилагается документ, составленный в произвольной форме и отражающий особое мнение члена экспертной комиссии, не согласного с выводами экспертной комиссии. Этот документ должен быть подписан членом экспертной комиссии, чье мнение он отражает.

5.2.2.2. Разрешение конфликтной ситуации по итогам работы экспертной комиссии.

Протокол экспертной комиссии является основанием для принятия Сторонами, участвующими в разрешении конфликтной ситуации, решения по урегулированию конфликтной ситуации.

В срок не более трех рабочих дней со дня составления протокола экспертной комиссии Стороны, участвующие в разрешении конфликтной ситуации, на основании выводов экспертной комиссии принимают меры по разрешению конфликтной ситуации.

Конфликтная ситуация признается разрешенной по итогам работы экспертной комиссии, если Стороны, участвующие в разрешении конфликтной ситуации, удовлетворены выводами, полученными экспертной комиссией, и не имеют претензий в связи с разрешаемой конфликтной ситуацией.

В случае если конфликтная ситуация признается разрешенной, Стороны, участвующие в разрешении конфликтной ситуации, в срок не позднее пяти рабочих дней со дня составления протокола экспертной комиссии оформляют решение об урегулировании конфликтной ситуации.

Решение составляется Сторонами, участвующими в разрешении конфликтной ситуации, в произвольной форме в виде документа на бумажном носителе и выдается по одному экземпляру каждой Стороне. Решение подписывается уполномоченными в разрешении конфликтной ситуации лицами Сторон и утверждается руководителями (иными уполномоченными лицами) Сторон.

5.2.3. Разрешение конфликтных ситуаций в судебном порядке.

В случае невозможности разрешения конфликтной ситуации в рабочем порядке и по итогам работы экспертной комиссии споры Сторон подлежат рассмотрению в судебном порядке в соответствии с законодательством Российской Федерации.

5.3. Процедуры проверки для разрешения конфликтных ситуаций.

Список необходимых для разрешения конфликтной ситуации проверок приведен в приложении 4 к настоящему Регламенту.

5.3.1. Проверка наличия электронных документов.

Для проверки наличия электронного документа необходимо:

получить электронный документ и электронную подпись для анализа (документ и электронная подпись могут быть получены из Системы в виде одного или двух файлов);

проверить наличие данного электронного документа в Системе. При этом могут быть сделаны следующие выводы:

при отсутствии данного электронного документа в Системе делается вывод об отсутствии причин конфликтной ситуации;

при наличии электронного документа в Системе необходимо продолжить разрешение конфликтной ситуации в соответствии с настоящим Регламентом.

5.3.2. Подтверждение подлинности электронной подписи.

Подтверждение подлинности электронной подписи в электронном документе выполняется путем проведения экспертизы. Экспертиза подлинности электронной подписи в электронном документе выполняется только удостоверяющим центром.

При неподтверждении удостоверяющим центром подлинности электронной подписи делается вывод об отсутствии причин конфликтной ситуации.

5.3.3. Проверка организационных аспектов.

Соответствие положениям настоящего Регламента:

1) соответствие полномочий на подписание электронного документа электронной подписью требованиям настоящего Регламента, а именно:

соответствие представленного документа описанию класса документов согласно документации к Системе;

возможность подписания электронной подписью электронных документов данного класса;

возможность подписания электронной подписью на заданном статусе;

2) время и дата подписания электронного документа (по времени системного журнала);

3) соответствие личности должностного лица, подписавшего электронный документ, информации, указанной в сертификате.

При установлении факта несоответствия электронной подписи в электронном документе положениям настоящего Регламента, времени и даты подписания электронного документа, указанных в системном журнале, времени и дате подписания электронного документа, указанным в Уведомлении, делается вывод о неправомерности требований соответствующей Стороны.

5.3.4. Корректность использования СКЗИ и Системы в соответствии с документацией на используемые программные и аппаратные средства и аттестатами соответствия.

При установлении факта некорректного использования СКЗИ и Системы делается вывод о неправомерности требований соответствующей Стороны.

5.3.5. Правомерность подписания электронного документа уполномоченным лицом на основании настоящего Регламента и внесения в реестр Системы сертификатов электронной подписи.

При установлении факта неправомерного подписания электронного документа уполномоченным лицом делается вывод о неправомерности требований соответствующей Стороны.

5.3.6. Доказательства корректности условий использования сертификатов в соответствии с областью применения сертификатов.

При установлении факта использования сертификатов не в соответствии с областью применения сертификатов делается вывод о неправомерности требований соответствующей Стороны.

VI. Порядок предоставления электронных документов из Системы по обращениям заинтересованных лиц

6.1. Обратившиеся в Минфин области физические или юридические лица, ответы на запросы которых требуют предоставления электронных документов, содержащихся в Системе, являются заинтересованными лицами.

6.2. В случае предоставления на обращение заинтересованного лица ответа в электронной форме, к ответу в качестве приложения прикрепляются выгруженные из Системы электронные документы с реквизитами электронной подписи и сертификата лица, подписавшего документ электронной подписью, изготовленные администратором системы Минфина области.

6.3. В случае предоставления на обращение заинтересованного лица ответа в печатной форме, к ответу прилагаются бумажные копии выгруженных из Системы электронных документов, изготовленные и заверенные специалистом Минфина области.

Первый заместитель Министра финансов
Челябинской области

А.А. Грязев