СТО СМК 82.19.13 Электронная цифровая подпись. Требования к работе удостоверяющего центра

РАЗРАБОТАН И ВВЕДЕН ВПЕРВЫЕ
ДАТА ВВЕДЕНИЯ В ДЕЙСТВИЕ: "28" сентября 2010 г.
С изменениями № 1 от "25" января 2011 г.

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящий Стандарт системы менеджмента качества (далее – Стандарт) определяет условия, порядок предоставления и правила пользования услугами Удостоверяющего центра (далее – Удостоверяющий центр, УЦ) по предоставлению ЭЦП, правила работы с ЭЦП.

1.2. Стандарт обязателен для применения:

- сотрудниками Удостоверяющего центра;

- участниками информационной системы, присоединившихся в порядке, предусмотренном статьей 428 ГК РФ к Соглашению о применении ЭЦП (по форме Приложения Е), и уполномоченных ими Владельцев сертификатов ключей подписи.

2. НОРМАТИВНЫЕ ССЫЛКИ

2.1. Стандарт разработан в соответствии с требованиями следующих нормативных документов:

- Федеральный закон №001 Об электронной цифровой подписи;

- Федеральный закон №049 Об информации, информационных технологиях и защите информации;

- СТО СМК 82.19.13 Управление документацией. Общие положения

- СТО СМК 70.22.11 "Стандартизация. Порядок создания, управления и применения стандартов"

2.2. При пользовании настоящим СТО целесообразно проверить действие ссылочных стандартов, указанных в нем. Если ссылочный документ заменен (изменен), то при пользовании настоящим СТО следует руководствоваться замененным (измененным) стандартом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

3.1. Термины и определения:

3.1.1. владелец сертификата ключа подписи: Физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою ЭЦП в электронных документах (подписывать электронные документы).

3.1.2. закрытый ключ электронной цифровой подписи (ключ подписи): Уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах ЭЦП с использованием средств электронной цифровой подписи.

3.1.3. информационная система (ИС): совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

3.1.4. область действия сертификата ключа подписи: Включенные в сертификат ключа подписи сведения об отношениях, при которых электронный документ с электронной цифровой подписью, будет иметь юридическое значение.

3.1.5. открытый ключ электронной цифровой подписи: Уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

3.1.6. подтверждение подлинности электронной цифровой подписи в электронном документе: Положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности ЭЦП в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной ЭЦП электронном документе.

3.1.7. пользователь сертификата ключа подписи: физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;

3.1.8. регистрация владельца сертификата ключа подписи: Внесение регистрационной информации о физическом лице, являющемся уполномоченным представителем Участника ИС и намеревающемся получить в Удостоверяющем центре закрытый ключ и сертификат ключа подписи, в соответствующие реестры Удостоверяющего Центра.

3.1.9. реестры Удостоверяющего центра: Набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий следующую информацию:

- реестр заявлений на регистрацию, изготовление и получение ключей подписи и сертификата ключа подписи;

- реестр заявлений на приостановление или возобновление действия сертификата ключа подписи;

- реестр заявлений на аннулирование (отзыв) сертификата ключа подписи;

- реестр сертификатов ключей подписи;

- реестр заявлений на подтверждение подлинности электронной цифровой подписи в электронном документе.

3.1.10. сертификат ключа подписи: документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;

3.1.11. сертификат ключа подписи уполномоченного лица Удостоверяющего центра: Электронный документ, содержащий открытый ключ ЭЦП уполномоченного лица Удостоверяющего центра, предназначенный для подтверждения подлинности ЭЦП уполномоченного лица Удостоверяющего центра и идентификации владельца сертификата ключа подписи. Сертификат ключа подписи уполномоченного лица Удостоверяющего центра считается действительным, если срок его действия начался и не истек и от Удостоверяющего центра не поступала информации о его аннулировании.

3.1.12. сертификат средств электронной цифровой подписи: документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

3.1.13. список отозванных сертификатов ключей подписи: Электронный документ с электронной цифровой подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей подписи, которые на определенный момент времени были отозваны или действие которых было приостановлено.

3.1.14. средства электронной цифровой подписи (СКЗИ): аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей. В данном СТО под СКЗИ подразумевается средство криптографической защиты информации (СКЗИ) «Microsoft Cryptographic Provider».

3.1.15. уполномоченное лицо Удостоверяющего центра (уполномоченное лицо УЦ): Физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное полномочиями по заверению сертификатов ключей подписи и списков отозванных сертификатов ключей подписи.

3.1.16. уполномоченный представитель Участника информационной системы:

Физическое лицо, являющееся сотрудником Участника ИС, которому в соответствии с его должностными обязанностями доверено право получения и использования электронной цифровой подписи.

3.1.17. удостоверяющий центр (УЦ): Юридическое лицо, выдающее сертификаты ключей подписей для использования в информационных системах общего пользования.

3.1.18. участник информационной системы: Юридическое, физическое лицо, присоединившееся в порядке, предусмотренном статьей 428 ГК РФ к Соглашению о применении электронной цифровой подписи в информационной системе.

3.1.19. электронная цифровая подпись (ЭЦП): Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

3.1.20. электронный документ: Документ, в котором информация представлена в электронно-цифровой форме.

3.2. Сокращения:

ИС – информационная система;

СМК – система менеджмента качества;

СТО – стандарт организации;

УЦ – удостоверяющий центр.

СКЗИ – средство криптографической защиты информации.

ЭЦП – электронная цифровая подпись.

4. ОТВЕТСТВЕННОСТЬ

4.1. Ответственность за соблюдение требований данного Стандарта несут лица, указанные в п. 1.2.

4.2. Действия по своевременной актуализации и контроль за соблюдением требований данного Стандарта осуществляет директор Удостоверяющего центра.

5. ОСНОВНЫЕ НОРМАТИВНЫЕ ПОЛОЖЕНИЯ

5.1. Основная цель использования ЭЦП – обеспечение неотрекаемости и применение ЭЦП в условиях равнозначности собственноручной подписи.

5.2. Для единообразного использования электронных документов участниками ИС должно быть заключено Соглашение об использовании ЭЦП.

5.3. Удостоверяющий центр предназначен для обеспечения участников ИС средствами для использования сертификатов ключей подписи в целях:

- обеспечения применения электронной цифровой подписи;

- контроля целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников ИС;

- аутентификации (проверки подлинности) участников ИС в процессе обмена электронными документами;

- обеспечения конфиденциальности информации, представленной в электронном виде и передаваемой посредством ИС.

5.4. Действия по регистрации пользователей ЭЦП и предоставление ЭЦП осуществляется Удостоверяющим центром, в порядке, предусмотренном разделом 6. Подключение к услугам Удостоверяющего центра предполагает:

- регистрацию уполномоченного представителя Участника ИС в Удостоверяющем центре;

- изготовление ключа подписи уполномоченному представителя Участника ИС.

5.5. В процессе своей деятельности Удостоверяющий центр предоставляет следующие виды услуг:

- создание ключей электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;

- изготовление и выдача сертификатов ключей подписейс информацией об их действии;

- аннулирование (отзыв), приостановление и возобновление действия сертификатов ключей подписи;

- ведение Реестров Удостоверяющего Центра;

- предоставление в электронной форме копий сертификатов ключей подписи Владельцев сертификата ключа подписи по запросам Владельцев сертификата ключа подписи и Участников ИС;

- предоставление сведений об аннулированных и приостановленных сертификатах ключей подписи;

- подтверждение подлинности электронных цифровых подписей в документах, представленных в электронной форме, по обращениям Участников ИС;

- подтверждение подлинности электронной цифровой подписи уполномоченного лица Удостоверяющего Центра в изготовленных им сертификатах ключей подписи;

- заверение по требованию Участника ИС собственноручной подписью уполномоченного лица Удостоверяющего Центра копии электронного документа, подписанного одной или несколькими электронными цифровыми подписями, в случае необходимости предоставления такого электронного

документа в качестве письменного доказательства в судебные или другие органы.

Порядок оказания услуг описан далее в разделе 6.

5.6. Правила пользования ЭЦП приведены в разделе 7.

5.7. Сроки действия криптографических ключей и сертификатов ключей подписи установлены в разделе 8.

5.8. Порядок разрешения конфликтных ситуаций, возникающих при использовании ЭЦП установлен в разделе 9.

6. ПОРЯДОК ОКАЗАНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

6.1. Порядок регистрации уполномоченного представителя Участника ИС

6.1.1. Регистрация уполномоченного представителя Участника ИС Удостоверяющим Центром осуществляется на основании следующих документов:

- Заявления на регистрацию, изготовление и получение ключей подписи и сертификата ключа подписи (далее – Заявление), оформленного на бумажном носителе согласно Приложения А;

- копии паспорта или иного документа, удостоверяющего личность;

- документов, подтверждающих место регистрации и адрес места жительства уполномоченного представителя Участника ИС и информацию о должности уполномоченного представителя Участника КИС, в случае если они состоят в трудовых отношениях.

6.1.2. Уполномоченное лицо УЦ рассматривает представленные документы в течение 2 (двух) рабочих дней. При положительном результате регистрации уполномоченное лицо УЦ:

а) формирует запрос на регистрацию в электронном виде;

б) вносит соответствующую отметку о регистрации на Заявлении;

в) выполняет регистрационные действия по занесению регистрационной информации в реестр Удостоверяющего центра;

г) производит идентификацию, результатом которой является присвоение уполномоченному представителю Участника ИС идентификатора и занесение идентификатора в Реестр УЦ. Идентификатором являются идентификационные данные из Заявления на регистрацию.

6.1.3. В случае отказа в регистрации в реестре УЦ Заявление возвращается с соответствующей отметкой об отказе в регистрации. Удостоверяющим центром может быть отказано в изготовлении ключей подписи и сертификатов ключа в следующих случаях:

- предоставление заявления на получение ключей и сертификатов ключей подписи, не соответствующего установленным требованиям;

- несоответствие информации, указанной в заявлении на получение ключей и сертификатов ключей подписи, информации, содержащейся в документах, представленных вместе с заявлением на получение ключей и сертификатов ключей подписи;

- отсутствие соответствующих полномочий у лица, представившего заявление на получение ключей и сертификатов ключей подписи.

6.2. Порядок изготовления и получения ключей подписи и сертификата ключа подписи

6.2.1. После успешного прохождения процедуры регистрации по пп. 6.1 Уполномоченное лицо УЦ течение 2 (двух) рабочих дней выполняет следующие действия:

- изготавливает Сертификат ключа подписи в электронной форме и записывает на электронный носитель;

- изготавливает два Бланка сертификата ключа подписи по форме согласно Приложению Б. Все экземпляры Бланка сертификата ключа подписи на бумажном носителе заверяются собственноручной подписью лица, проходящего процедуру изготовления ключей подписи и сертификатов, а также собственноручной подписью Уполномоченного работника Удостоверяющего Центра и печатью Удостоверяющего Центра.

6.2.2. По окончании выполнения действий, указанных в п. 6.2.1, Уполномоченное лицо УЦ выдает под расписку владельцу сертификата ключа подписи (или его представителю, действующему на основании доверенности):

- ключевую пару ключей на электронном носителе ключевой информации;

- сертификат ключа подписи в электронной форме на электронном носителе;

- один экземпляр Бланка сертификата ключа подписи;

- копию сертификата ключа подписи Уполномоченного лица Удостоверяющего Центра в электронном виде на электронном носителе информации.

6.3. Идентификация и аутентификация владельца сертификата ключа подписи

6.3.1. Идентификация владельца сертификата ключа подписи осуществляется по идентификатору, занесенному в реестр Удостоверяющего центра.

6.3.2. Аутентификация владельца сертификата ключа подписи по паролю (маркеру) выполняется путем сопоставления предъявленного зарегистрированным владельцем сертификата ключа подписи пароля с учетной информацией, хранимой в Реестре УЦ. Действие пароля начинается с момента его предоставления владельцу сертификата ключа подписи Срок действия пароля ограничивается датой окончания действия сертификата ключа подписи.

6.3.3. Аутентификация владельца сертификата ключа подписи по сертификату ключа подписи выполняется путем выполнения процедуры подтверждения электронной цифровой подписи с использованием сертификата ключа подписи.

6.4. Порядок действий Владельца сертификата ключа подписи при компрометации его криптографического ключа

6.4.1. К фактам, которые могут рассматриваться как компрометация (или подозрение на компрометацию) криптографических ключей, относятся следующие события:

а) утрата отчуждаемых носителей ключевой информации, в том числе с последующим их обнаружением;

б) прекращение трудовых отношений Участника ИС и его работника, имевшего доступ к ключу Владельца сертификата ключа подписи, при условии прекращения действия доверенности, на основании которой указанный работник выполнял функции Владельца сертификата ключа подписи;

в) прекращение действия доверенности, на основании которой Владелец сертификата ключа подписи подписывал электронные документы электронной цифровой подписью от лица Участника КИС;

г) нерасшифровывание входящих или исходящих сообщений Владельца сертификата ключа подписи;

д) отрицательный результат при проверке электронной цифровой подписи электронного документа.

6.4.2. Владелец сертификата ключа подписи и Участник ИС самостоятельно принимают решение о факте компрометации закрытого ключа Владельца сертификата ключа подписи.

6.4.3. В случае компрометации закрытого ключа Участник ИС незамедлительно подает в Удостоверяющий Центр заявление на отзыв (аннулирование) сертификата открытого ключа в соответствии с п. 6.6.2.

6.5. Генерация ключей подписи и формирование сертификата ключа подписи при изменении областей применения ЭЦП

6.5.1. Генерация ключей подписи и формирование сертификата ключа подписи с областями действия подписи, отличными от используемых, осуществляется в соответствии с процедурами и технологией изложенными в пункте 6.1 и 6.2.

6.6. Аннулирование (отзыв) сертификата ключа подписи

6.6.1. Удостоверяющий центр аннулирует сертификат ключа подписи в следующих случаях:

- по истечении срока его действия;

- по истечении срока, на который действие сертификата ключа подписи было приостановлено;

- по заявлению владельца сертификата ключа подписи или Участника КИС;

- при компрометации ключа уполномоченного лица Удостоверяющего центра.

6.6.2. Для аннулирования (отзыва) сертификата ключа подписи Владелец сертификата ключа подписи должен направить в Удостоверяющий центр заявление на аннулирование (отзыв) сертификата (по форме Приложения В), заверенное собственноручной подписью Владельца сертификата ключа подписи и (или) подписью единоличного исполнительного органа соответствующего Участника КИС.

6.6.3. Обработка заявления на аннулирование (отзыв) сертификата ключа подписи и уведомление Владельца сертификата ключа подписи об аннулировании (отзыве) его сертификата должно быть осуществлено не позднее 1 (одного) рабочего дня с момента принятия заявления.

6.6.4. Временем аннулирования (отзыва) сертификата ключа подписи признается время официального уведомления Владельца сертификата ключа подписи и (или) Участника ИС об аннулировании (отзыве) указанного сертификата ключа подписи.

6.7. Приостановление действия сертификата ключа подписи

6.7.1. Для приостановления действия сертификата ключа подписи Владелец сертификата ключа подписи должен направить в Удостоверяющий центр заявление на приостановление действия сертификата (по форме Приложения Г) заверенное собственноручной подписью Владельца сертификата ключа подписи и (или) подписью единоличного исполнительного органа соответствующего Участника КИС.

6.7.2. Обработка заявления на приостановление действия сертификата и уведомление Владельца сертификата ключа подписи о приостановлении действия его сертификата должны быть осуществлены не позднее 1 (одного) рабочего дня с момента принятия Удостоверяющим центром заявления.

6.7.3. Временем приостановления действия сертификата ключа подписи признается время официального уведомления Владельца сертификата ключа подписи Удостоверяющим Центром о приостановлении действия данного сертификата.

6.7.4. Если в течение срока приостановления действия сертификата Владелец сертификата ключа подписи не представит в Удостоверяющий Центр заявление о возобновлении действия этого сертификата открытого ключа, то такой сертификат аннулируется (отзывается) Удостоверяющим Центром в течение следующего рабочего дня за днем истечения срока приостановления его действия. В адрес его Владельца Удостоверяющим Центром отправляется соответствующее уведомление.

6.8. Возобновление действия сертификата ключа подписи

6.8.1. Для возобновления действия сертификата ключа подписи Владелец сертификата ключа подписи должен направить в Удостоверяющий центр заявление на возобновление действия сертификата (по форме Приложения Д), заверенное собственноручной подписью Владельца сертификата ключа

подписи и (или) подписью единоличного исполнительного органа соответствующего Участника КИС.

6.8.2. Обработка заявления на возобновление действия сертификата ключа подписи и уведомление его Владельца о возобновлении действия сертификата должны быть осуществлены не позднее 1 (одного) рабочего дня с момента принятия Удостоверяющим центром заявления.

6.8.3. Временем возобновления действия сертификата ключа подписи признается время официального уведомления Владельца сертификата ключа подписи о возобновлении действия данного сертификата.

6.8.4. Возобновление действия сертификата ключа подписи возможно только в течение срока, на который было приостановлено действие сертификата.

6.9. Подтверждение подлинности электронной цифровой подписи в электронном документе

6.9.1. Процедура подтверждения подлинности электронной цифровой подписи в электронном документе выполняется Удостоверяющим Центром при возникновении споров о наличии электронной цифровой подписи в электронном документе и о факте внесения изменений в электронный документ после его подписания электронной цифровой подписью.

6.9.2. Для подтверждения подлинности электронной цифровой подписи электронного документа Участник ИС должен направить в Удостоверяющий центр заявление на подтверждение подлинности электронной цифровой подписи электронного документа, заверенное собственноручной подписью Владельца сертификата ключа подписи и (или) подписью единоличного исполнительного органа соответствующего Участника ИС и содержащее следующую информацию:

- дата и время подачи заявления;

- идентификационные данные Владельца сертификата ключа подписи, электронная цифровая подпись которого требует проверки в электронном документе;

- серийный номер сертификата ключа подписи, на котором требуется осуществить проверку электронной цифровой подписи электронного документа;

- дата и время формирования электронной цифровой подписи в электронном документе.

6.9.3. Обязательным приложением к заявлению на подтверждение подлинности электронной цифровой подписи в электронном документе является файл электронного документа.

6.9.4. Срок рассмотрения заявления на подтверждение подлинности электронной цифровой подписи в электронном документе и предоставление заключения о произведенной проверке составляет 5 (пять) рабочих дней с момента его поступления в Удостоверяющий Центр.

6.9.5. Процедуру подтверждения подлинности электронной цифровой подписи

в электронном документе выполняет экспертная комиссия, формируемая из числа работников Удостоверяющего Центра по распоряжению руководителя. На заседание экспертной комиссии приглашаются уполномоченные представители заинтересованных Участников КИС.

6.9.6. Результатом выполнения процедуры подтверждению подлинности электронной цифровой подписи в электронном документе является заключение, подписанное собственноручными подписями членов экспертной комиссии, заверенное печатью Удостоверяющего Центра и содержащее результат проверки электронной цифровой подписи электронного документа и отчет по выполненной проверке, в том числе сведения о:

- времени и месте проведения проверки;

- составе экспертной комиссии, осуществлявшей проверку;

- основаниях для проведения проверки;

- данных, представленные экспертной комиссии для проведения проверки;

- содержании проверки с указанием примененных методов;

- обосновании результатов проверки.

7. ПРАВИЛА ПОЛЬЗОВАНИЯ ЭЦП

7.1. ЭЦП используется при обмене электронными документами при помощи КИС.

7.2. При совершении сделок может быть использована как ЭЦП, принадлежащая самой стороне совершаемой сделки, так и ЭЦП лица, действующего от имени стороны сделки. В этом случае лицо, от имени которого совершается сделка, и лицо, совершающее сделку от его имени, должны являться Сторонами Соглашения о применении ЭЦП.

7.3. Электронный документ может быть подписан только ЭЦП, ключ которой зарегистрирован в УЦ.

7.4. Сторона не может ссылаться на отсутствие у нее ключа ЭЦП отправителя электронного документа, если данный ключ зарегистрирован УЦ.

7.5. Электронный документ, подписанный ЭЦП одной из Сторон и полученный другой Стороной, не влечет правовых последствий, если до момента получения данного документа адресатом последний был уведомлен отправителем или УЦ о том, что соответствующий ключ ЭЦП более не используется.

7.6. Поля Subject, Key Usage, Extended Key Usage сертификата ключа подписи содержат сведения об отношениях, при которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

7.7. Владелец сертификата ключа подписи обязан:

- хранить в тайне личный закрытый ключ подписи, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и

несанкционированного использования;

- применять для формирования электронной цифровой подписи только действующий закрытый ключ подписи, сертификат ключа подписи которого изготовлен УЦ;

- не применять закрытый ключ подписи, если стало известно, что этот ключ используется или использовался ранее другими лицами;

- применять закрытый ключ подписи только в области его действия, соответствующей указанной в соответствующем данному закрытому ключу сертификате ключа подписи;

- немедленно обратиться в Удостоверяющий центр с заявлением на приостановление действия сертификата ключа подписи в случае потери, раскрытия, искажения закрытого ключа подписи, а также, в случае если известно, что этот ключ используется или использовался ранее другими лицами;

- не использовать закрытый ключ подписи, связанный с сертификатом ключа подписи, заявление на аннулирование (отзыв) которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) сертификата ключа подписи в Удостоверяющий центр по момент времени официального уведомления об аннулировании (отзыве) данного сертификата;

- не использовать закрытый ключ подписи, связанный с сертификатом ключа подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата ключа подписи в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия данного сертификата;

7.8.1. Владелец сертификата ключа подписи имеет право:

- получить список аннулированных (отозванных) и приостановленных сертификатов ключей подписи владельцев сертификатов ключей подписи;

- получить сертификат ключа подписи уполномоченного лица Удостоверяющего центра;

- применять сертификат ключа подписи уполномоченного лица Удостоверяющего центра для проверки электронной цифровой подписи уполномоченного лица Удостоверяющего центра в сертификатах ключа подписи, изготовленных Удостоверяющим центром;

- применять сертификат ключа подписи для проверки электронной цифровой подписи электронных документов в соответствии со сведениями, указанными в сертификате ключа подписи;

- применять список отозванных сертификатов ключей подписи, изготовленный Удостоверяющим центром, для проверки статуса сертификатов ключей подписи;

- обратиться в Удостоверяющий центр за подтверждением подлинности

электронных цифровых подписей в электронных документах;

- получить копию сертификата ключа подписи в электронной форме, находящегося в реестре сертификатов ключей подписи Удостоверяющего центра;

- обратиться в Удостоверяющий центр за подтверждением подлинности электронных цифровых подписей уполномоченного лица Удостоверяющего центра в изготовленных им сертификатах ключей подписи;

- обратиться в Удостоверяющий центр для аннулирования (отзыва) сертификата ключа подписи в течение срока действия соответствующего закрытого ключа подписи;

- обратиться в Удостоверяющий центр для приостановления действия сертификата ключа подписи в течение срока действия соответствующего закрытого ключа подписи;

- обратиться в Удостоверяющий центр для возобновления действия сертификата ключа подписи в течение срока действия соответствующего закрытого ключа подписи и срока, на который действие сертификата было приостановлено.

8. СРОКИ ДЕЙСТВИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

8.1. Срок действия закрытого ключа Уполномоченного лица Удостоверяющего Центра и сертификата ключа подписи, соответствующего закрытому ключу, составляет 5 (пять) лет.

8.2. Началом периода действия закрытого ключа Уполномоченного лица Удостоверяющего Центра считается дата и время начала действия соответствующего ему сертификата ключа подписи Уполномоченного лица, определяемого по атрибуту сертификата ключа подписи «Действителен с».

8.3. Срок действия закрытого ключа Владельцев сертификатов ключей подписи и сертификата ключа подписи, соответствующего закрытому ключу, составляет 1 (один) год.

8.4. Началом периода действия закрытого ключа Владельца сертификата ключа подписи считается дата и время начала действия соответствующего ему сертификата ключа подписи этого Владельца сертификата ключа.

8.5. Хранение сертификата ключа подписи в Удостоверяющем Центре осуществляется в течение всего периода его действия и еще 5 (пять) лет после его аннулирования (отзыва).

8.6.По истечении указанного срока хранения сертификаты ключа подписи передаются на хранение в архив.

9. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ, ВОЗНИКАЮЩИХ ПРИ ИСПОЛЬЗОВАНИИ ЭЦП

9.1. Возникновение конфликтных ситуаций при использовании ЭЦП

9.1.1. Применение электронной цифровой подписи в информационной системе может приводить к конфликтным ситуациям, заключающимся в оспаривании участниками ИС авторства и/или содержимого документа, подписанного электронной цифровой подписью. Конфликтные ситуации могут возникать в следующих случаях:

- не подтверждение подлинности защищенных электронных документов средствами проверки ЭЦП получателя;

- оспаривание факта идентификации владельца ЭЦП, подписавшего электронный документ;

- заявление отправителя или получателя электронного документа об его искажении;

- иные случаи возникновения конфликтных ситуаций.

9.1.2. Конфликтные ситуации разрешаются (урегулируются) Участниками ИС в рабочем порядке или по итогам работы Экспертной комиссии.

9.1.3. Разбор конфликтной ситуации в отношении авторства электронного документа заключается в доказательстве авторства подписи конкретного электронного документа конкретным лицом (владельцем сертификата ключа подписи).

9.2. Уведомление о конфликтной ситуации

9.2.1. В случае возникновения обстоятельств, свидетельствующих, по мнению одного из участников КИС, о возникновении и/или наличии конфликтной ситуации, данный Участник ИС (далее – Сторона-инициатор) незамедлительно извещает другую заинтересованную Сторону о возможном возникновении и/или наличии конфликтной ситуации, обстоятельствах, свидетельствующих о ее возникновении или наличии, а также ее предполагаемых причинах.

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

9.2.3. В тот же срок Сторона-ответчик извещает доступными способами сторону-инициатора о результатах проверки и, при необходимости, о мерах, принятых для разрешения конфликтной ситуации.

9.3. Разрешение конфликтной ситуации в рабочем порядке

9.3.1. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если Сторона-инициатор удовлетворена информацией, полученной в извещениях Стороны – ответчика, и не имеет к ней претензий в связи с конфликтной ситуацией.

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

9.4. Предложение по формированию экспертной комиссии по разрешению конфликтной ситуации

9.4.1. В случае, если конфликтная ситуация не была разрешена в рабочем порядке, Сторона-инициатор, должна не позднее чем в течение трех рабочих дней после возникновения конфликтной ситуации, направить уведомление о конфликтной ситуации (далее - Уведомление) и предложение о создании Экспертной комиссии по разрешению конфликтной ситуации (далее - Предложение) Стороне-ответчику.

9.4.2. Уведомление должно содержать информацию о предмете и существе конфликтной ситуации, обстоятельствах, по мнению Стороны-инициатора, свидетельствующих о наличии конфликтной ситуации, возможных причинах и последствиях ее возникновения.

9.4.3. Уведомление должно содержать информацию с указанием фамилий, имен, отчеств, должностей и контактной информации должностных лиц Стороны-инициатора, уполномоченных в разрешении конфликтной ситуации.

9.4.4. Предложение должно содержать информацию о предлагаемом месте, дате и времени сбора Экспертной комиссии, список предлагаемых для участия в работе Экспертной комиссии представителей Стороны-инициатора с указанием фамилий, имен, отчеств, должностей, при необходимости исполняемых при обмене электронными документами функциональных ролей (администратор, администратор безопасности и т.п.), их контактной информации (телефон, факс, электронная почта).

9.4.5. Уведомление и Предложение составляются на бумажном носителе, подписываются должностными лицами Стороны-инициатора, уполномоченными в разрешении конфликтной ситуации и передаются Стороне-ответчику в установленном порядке, обеспечивающим подтверждение вручения корреспонденции.

9.4.6. Уведомление и Предложение могут быть составлены и направлены в форме электронного документа. При этом факт их доставки должен быть подтвержден.

9.5. Формирование экспертной комиссии по разрешению конфликтной ситуации, ее состав

9.5.1. Не позднее, чем на третий рабочий день после получения Предложения Сторонами, участвующими в разрешении конфликтной ситуации, должна быть сформирована Экспертная комиссия.

9.5.2. Экспертная комиссия формируется на основании писем Сторон и оформляется приказом. В приказе определяется состав Экспертной комиссии, время и место ее работы.

9.5.3. Устанавливается тридцатидневный срок работы Экспертной комиссии. В исключительных случаях срок работы Экспертной комиссии по согласованию

Сторон может быть дополнительно продлен не более чем на тридцать дней.

9.5.4. Если Стороны не договорятся об ином, в состав Экспертной комиссии входит равное количество уполномоченных лиц каждой из Сторон, участвующих в разрешении конфликтной ситуации.

9.5.5. В состав Экспертной комиссии назначаются представители служб информационно-технического обеспечения и служб обеспечения информационной безопасности, а также представители подразделений – исполнителей электронного документа.

9.5.6. В состав Экспертной комиссии могут быть включены представители юридических служб Сторон, представители органов, осуществляющих государственное регулирование и контроль соответствующих видов деятельности.

9.5.7. В состав Экспертной комиссии должен входить уполномоченный представитель Удостоверяющего центра.

9.5.8. По инициативе любой из сторон к работе Экспертной комиссии для проведения технической экспертизы могут привлекаться независимые эксперты, в том числе представители поставщиков средств защиты информации. При этом Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.

9.5.9. Лица, входящие в состав Экспертной комиссии должны обладать необходимыми знаниями и опытом работы в области подготовки и исполнения электронных документов, построения и функционирования Системы, организации и обеспечения информационной безопасности при обмене электронными документами, должны иметь соответствующий допуск к необходимым для проведения работы Экспертной комиссии документальным материалам и программно-техническим средствам.

9.5.10. При участии в Экспертной комиссии представителей сторонних органов и организаций их право представлять соответствующие органы и организации должно подтверждаться официальным документом (доверенностью, предписанием, копией приказа или распоряжения).

9.6. Права и полномочия экспертной комиссии по разрешению конфликтной ситуации

9.6.1. Экспертная комиссия имеет право:

- получать доступ к необходимым для проведения ее работы документальным материалам Сторон, на бумажных и электронных носителях;

- проводить ознакомление с условиями и порядком подготовки, формирования, обработки, доставки, исполнения, хранения и учета электронных документов;

- проводить ознакомление с условиями и порядком эксплуатации Сторонами программно-технических средств обмена электронными документами;

- проводить ознакомление с условиями и порядком изготовления, использования и хранения Сторонами ключевой информации, а также иной конфиденциальной информации и ее носителей, необходимых для работы

Экспертной комиссии;

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

- получать от Сторон любую иную информацию, относящуюся, по ее мнению, к рассматриваемой конфликтной ситуации.

9.6.2. Для проведения необходимых проверок и документирования данных, Экспертной комиссией могут применяться специальные программно-технические средства.

9.7. Оформление результатов работы экспертной комиссии по разрешению конфликтной ситуации

9.7.1. Все мероприятия Экспертной комиссии по проверке с применением аппаратно-программных средств должны протоколироваться. Протоколы прилагаются к акту работы комиссии.

9.7.2. По итогам работы Экспертной комиссии составляется акт, при этом акт должен содержать следующую информацию:

- состав Экспертной комиссии;

- дату и место составления акта;

- даты и время начала и окончания работы Комиссией;

- фактические обстоятельства, установленные Комиссией;

- краткий перечень мероприятий, проведенных Комиссией;

- выводы, к которым пришла Экспертная комиссия в результате проведенных мероприятий;

- подписи членов Экспертной комиссии;

9.7.3. К Акту может прилагаться особое мнение члена или членов Экспертной комиссии, не согласных с выводами Экспертной комиссии, указанными в Акте. Особое мнение составляется в произвольной форме, подписывается членом или членами Экспертной комиссии, чье мнение оно отражает

9.7.4. Акт составляется в форме документа на бумажном носителе, по одному экземпляру каждой Стороне. По обращению любого из членов Экспертной комиссии, Стороной, к которой было направлено обращение, ему должна быть выдана заверенная копия Акта.

9.7.5. Акт Экспертной комиссии является основанием для принятия Сторонами решения по урегулированию конфликтной ситуации.

10. ВНЕСЕНИЕ ИЗМЕНЕНИЙ, ХРАНЕНИЕ И РАССЫЛКА

10.1. Решение о внесении изменений в данный СТО принимает Владелец стандарта по представлению Управляющего проектом и Разработчика. Внесение изменений в данный СТО производится в порядке, установленном в

СТО СМК 70.22.11 "Стандартизация. Порядок создания, управления и применения стандартов"

10.2. Контрольный экземпляр СТО хранится в Архиве в условиях, исключающих его порчу, несанкционированный доступ или утерю.

10.3. Данный СТО рассылается в электронном виде посредством ИС в соответствии с требованиями СТО СМК 70.22.11 "Стандартизация. Порядок создания, управления и применения стандартов"

ПРИЛОЖЕНИЯ

Приложение А. Форма Заявления на регистрацию, изготовление и получение ключей подписи и сертификата ключа подписи

(обязательное)

Форма Заявления на регистрацию, изготовление и получение ключей подписи и сертификата ключа подписи

Руководителю Удостоверяющего центра

(ФИО и должность руководителя Удостоверяющего центра)

Заявление на регистрацию, изготовление и получение

ключей подписи и сертификата ключа подписи

для юр. лица:

(наименование, адрес по месту регистрации юридического лица), свидетельство о регистрации № (номер свидетельства) от (дата выдачи свидетельства)г., выдано (кем выдано свидетельство), в лице (должность, ФИО), действующего на основании (документ-основание действия), просит зарегистрировать уполномоченное лицо и изготовить ключи подписи и сертификаты ключей подписи на имя (ФИО, паспортные данные уполномоченного лица, адрес места жительства уполномоченного лица) в реестре Удостоверяющего центра.

для физ. лица:

Я, ((Ф.И.О., паспортные данные) прошу зарегистрировать и изготовить ключи подписи и сертификаты ключей подписи на моё имя в реестре Удостоверяющего центра.

Идентификационные данные:

CN = Общее имя = Фамилия, Имя, Отчество

L = Город = наименование населенного пункта

S = Область = наименование субъекта Федерации

C = Страна/Регион = RU

E = Электронная почта = адрес электронной почты

Подпись (подпись уполномоченного лица, его ФИО)заверяю.

(дата составления заявления)

м. п. (ФИО и подпись руководителя юридического лица - Участника КИС)

Отметка о регистрации:

Подтверждаю, что Заявление на регистрацию (ФИО уполномоченного лица)в реестре Удостоверяющего Центра получено, личность (ФИО уполномоченного лица) идентифицирована, сведения, указанные в Заявлении, проверены.

(дата принятия заявления)

Уполномоченное лицо Удостоверяющего Центра

м. п. (ФИО и подпись Уполномоченного лица Удостоверяющего центра)

Отметка об отказе в регистрации:

Заявление на регистрацию (ФИО уполномоченного лица)в реестре Удостоверяющего Центра получено, личность (ФИО уполномоченного лица) не может быть принято по причине (формулировка причин отказа в регистрации).

(дата отказа в принятии заявления)

Уполномоченное лицо Удостоверяющего Центра

м. п. (ФИО и подпись Уполномоченного лица Удостоверяющего центра)

Приложение Б. Форма Бланка сертификата ключа подписи

(обязательное)

Форма Бланка сертификата ключа подписи

Удостоверяющий Центр ООО "Экспертиза"

Копия сертификата открытого ключа подписи

Сведения о сертификате:

Кем выдан: Удостоверяющий центр "ЭКСПЕРТИЗА"

Версия: 3

Серийный номер:

Издатель сертификата: CN=, DC=, DC=

Срок действия:

Действителен с: 09.09.2010 13:55:32

Действителен по: 09.09.2011 13:55:32

Алгоритм открытого ключа по: RSA

Длина ключа: 1 024

КОД открытого ключа

Расширения сертификата X.509: Количество расширений может меняться

Расширение 1:	Политики применения
Значение:	
Расширение 2:	Сведения о шаблоне сертификата
Значение:	
Расширение 3:	Доступ к информации о центрах сертификации
Значение:	
Расширение 4:	Идентификатор ключа субъекта
Значение:	
Расширение 5:	Использование ключа
Значение:	
Расширение 6:	Дополнительное имя субъекта
Значение:	
Расширение 7:	Точки распространения списков отзыва (CRL)
Значение:	
Расширение 8:	Идентификатор ключа центра сертификатов
Значение:	
Расширение 9:	Улучшенный ключ
Значение:	

Подпись владельца сертификата: _____/_____

____ _____ 20__ г.

Подпись уполномоченного лица : _____/_____

____ _____ 20__ г.

М. П.

Приложение В. Форма Заявления на аннулирование (отзыв) сертификата

(обязательное)

Форма Заявления на аннулирование (отзыв) сертификата

Руководителю Удостоверяющего центра

(ФИО и должность руководителя Удостоверяющего центра)

Заявление на аннулирование (отзыв) сертификата ключа подписи

Для юр.лица

(наименование, адрес по месту регистрации юридического лица), свидетельство о регистрации № (номер свидетельства) от (дата выдачи свидетельства)г., выдано (кем выдано свидетельство), в лице (должность, ФИО), действующего на основании (документ-основание действия), просит отозвать (аннулировать) сертификат ключа подписи серийный №(серийный номер ключа), выданного на имя (ФИО, паспортные данные уполномоченного лица, адрес места жительства уполномоченного лица).

Владелец сертификата ключа подписи (подпись, ФИО, дата)

Подпись (подпись уполномоченного лица, его ФИО)заверяю.

(дата составления заявления)

м. п.(ФИО и подпись руководителя юридического лица - Участника КИС)

Для физ. лица

(ФИО, паспортные данные уполномоченного лица, адрес места жительства уполномоченного лица) (серийный номер ключа).

(подпись, ФИО, дата)

Отметка о регистрации:

Подтверждаю, что Заявление на аннулирование (отзыв) сертификата ключа подписи (ФИО уполномоченного лица) получено, личность (ФИО уполномоченного лица) идентифицирована, сведения, указанные в Заявлении, проверены.

(дата принятия заявления)

Уполномоченное лицо Удостоверяющего Центра

м. п. (ФИО и подпись Уполномоченного лица Удостоверяющего центра)

Приложение Г. Форма Заявления на приостановление действия сертификата

(обязательное)

Форма Заявления на приостановление действия сертификата

Руководителю Удостоверяющего центра

(ФИО и должность руководителя Удостоверяющего центра)

Заявление на приостановление действия сертификата ключа подписи

(наименование, адрес по месту регистрации юридического лица), свидетельство о регистрации № (номер свидетельства) от (дата выдачи свидетельства)г., выдано (кем выдано свидетельство), в лице (должность, ФИО), действующего на основании (документ-основание действия), просит приостановить действие сертификата ключа подписи серийный №(серийный номер ключа), выданного на имя (ФИО, паспортные данные уполномоченного лица, адрес места жительства уполномоченного лица)на (количество цифрами

и прописью)календарных дней.

Владелец сертификата ключа подписи (подпись, ФИО, дата)

Подпись (подпись уполномоченного лица, его ФИО)заверяю.

(дата составления заявления)

м. п.(ФИО и подпись руководителя юридического лица - Участника КИС)

Отметка о регистрации:

Подтверждаю, что Заявление на приостановление действия сертификата ключа подписи (ФИО уполномоченного лица) получено, личность (ФИО уполномоченного лица) идентифицирована, сведения, указанные в Заявлении, проверены.

(дата принятия заявления)

Уполномоченное лицо Удостоверяющего Центра

м. п. (ФИО и подпись Уполномоченного лица Удостоверяющего центра)

Приложение Д. Форма Заявления на возобновление действия сертификата

(обязательное)

Форма Заявления на возобновление действия сертификата

Руководителю Удостоверяющего центра

(ФИО и должность руководителя Удостоверяющего центра)

Заявление на возобновление действия сертификата ключа подписи

(наименование, адрес по месту регистрации юридического лица), свидетельство о регистрации № (номер свидетельства) от (дата выдачи свидетельства)г. , выдано (кем выдано свидетельство), в лице (должность, ФИО), действующего на основании (документ-основание действия), просит возобновить действие сертификата ключа подписи серийный №(серийный номер ключа), выданного на имя (ФИО, паспортные данные уполномоченного лица, адрес места жительства уполномоченного лица).

Владелец сертификата ключа подписи (подпись, ФИО, дата)

Подпись (подпись уполномоченного лица, его ФИО) заверяю.

(дата составления заявления)

м. п.(ФИО и подпись руководителя юридического лица - Участника КИС)

Отметка о регистрации:

Подтверждаю, что Заявление на возобновление действия сертификата

ключа подписи (ФИО уполномоченного лица) получено, личность (ФИО уполномоченного лица) идентифицирована, сведения, указанные в Заявлении, проверены.

(дата принятия заявления)

Уполномоченное лицо Удостоверяющего Центра

м. п. (ФИО и подпись Уполномоченного лица Удостоверяющего центра)

Приложение Е. Форма Соглашения о применении ЭЦП

(обязательное)

Форма Соглашения о применении ЭЦП

СОГЛАШЕНИЕ о применении электронной цифровой подписи в информационной системе

1. СТОРОНЫ И ПОРЯДОК ЗАКЛЮЧЕНИЯ СОГЛАШЕНИЯ

1.1. Сторонами настоящего Соглашения являются:

- Организатор информационной системы - Общество с ограниченной ответственностью «Информационно-техническая компания»

- Юридические лица, индивидуальные предприниматели, физические лица, присоединившиеся к настоящему Соглашению, в соответствии со ст. 428 Гражданского кодекса Российской Федерации.

1.2. Присоединение к настоящему Соглашению осуществляется в порядке, предусмотренном разделом 10 настоящего Соглашения.

1.3. Стороны договорились понимать используемые в настоящем Соглашении термины в следующем значении:

- **информационная система (ИС):** совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

- **удостоверяющий центр (УЦ):** Юридическое лицо, выдающее сертификаты ключей подписей для использования в информационных системах общего пользования.

2. ПРЕДМЕТ СОГЛАШЕНИЯ

2.1. ЭЦП используется Сторонами настоящего Соглашения и имеет юридическое значение при подписании и обмене ими электронными документами в КИС, в том числе при заключении, изменении и расторжении договоров (соглашений), при исполнении договоров между Сторонами настоящего Соглашения.

2.2. Стороны согласились, что ЭЦП в электронных документах, сформированная владельцем сертификата ключа подписи, является равнозначной собственноручной подписи владельца сертификата ключа

подписи при выполнении условий, определенных настоящим Соглашением.

2.3. Стороны согласились, что получение электронного документа, подписанного ЭЦП в соответствии с условиями настоящего Соглашения и подтверждение подлинности ЭЦП в электронном документе, является необходимым и достаточным условием, позволяющим установить, что электронный документ исходит от стороны, его отправившей.

2.4. Риск неправомерного подписания электронного документа ЭЦП несет сторона, уполномоченный представитель которой является владельцем сертификата ключа подписи.

3. СЛУЧАИ И ПОРЯДОК ИСПОЛЬЗОВАНИЯ ЭЦП

3.1. Стороны обязуются использовать, принимать и признавать сертификаты ключей подписи, изданные Удостоверяющим центром, в составе и формате, определяемом договорами, регулирующими отношения Сторон настоящего Соглашения с Удостоверяющим центром.

3.2. Сертификат ключа подписи признается изданным Удостоверяющим Центром, если подтверждена подлинность ЭЦП уполномоченного лица Удостоверяющего центра.

3.3. В рамках настоящего Соглашения электронный документ может быть подписан только ЭЦП, открытый ключ которой зарегистрирован Удостоверяющим центром.

3.4. Стороны согласились, что идентификационные данные, занесенные в поле SubjectName (за исключением адреса электронной почты) сертификата ключа подписи однозначно идентифицируют владельца сертификата ключа подписи и соответствующего ключа подписи и соответствуют идентификационным данным владельца сертификата ключа подписи, зарегистрированным Удостоверяющим центром.

3.5. Для определения действительности сертификата ключа подписи используется актуальный список отозванных сертификатов, издаваемый и публикуемый Удостоверяющим центром в порядке и с периодичностью, определяемыми договорами, регулирующими отношения Сторон настоящего Соглашения с Удостоверяющим центром. В качестве места публикация актуального списка отозванных сертификатов принимается адрес информационного ресурса, определенный в поле CRL Distribuition Point (CDP) сертификата ключа подписи.

3.6. Любой электронный документ, который должен быть подписан ЭЦП при совершении сделок, в случаях и порядке, предусмотренных настоящим Соглашением, и иными договорами, заключаемыми между Сторонами, но не содержащий ЭЦП, не влечет правовых последствий.

4. СРЕДСТВО ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

4.1. Стороны принимают в качестве средства электронной цифровой подписи при выполнении функций создания ЭЦП в электронном документе с использованием закрытого ключа ЭЦП, подтверждения с использованием открытого ключа ЭЦП подлинности ЭЦП в электронном документе, создания открытых и закрытых ключей ЭЦП использовать средство криптографической

защиты информации Microsoft Cryptographic Provider (далее по тексту – СКЗИ).

4.2. Стороны обязуются использовать копии СКЗИ, полученные законным путем

4.3. Стороны обязуются сохранять в тайне закрытые ключи ЭЦП.

5. УСЛОВИЯ РАВНОЗНАЧНОСТИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ СОБСТВЕННОРУЧНОЙ

5.1. ЭЦП в электронном документе равнозначна собственноручной подписи владельца сертификата ключа подписи при одновременном выполнении следующих условий:

- На момент проверки ЭЦП сертификат ключа подписи уполномоченного лица Удостоверяющего центра является действительным;

- сертификат ключа подписи, соответствующий ЭЦП, издан Удостоверяющим центром;

- владелец сертификата ключа подписи идентифицирован по содержимому поля Subject Name сертификата ключа подписи;

- серийный номер сертификата ключа подписи, относящийся к ЭЦП, не содержится в актуальном списке отозванных сертификатов на момент проверки ЭЦП;

- срок действия сертификата ключа подписи, относящегося к ЭЦП, наступил и не окончен на момент проверки ЭЦП;

- период между сроком начала действия сертификата ключа подписи и моментом проверки ЭЦП не превышает срока действия закрытого ключа ЭЦП, определенного в договорах, регулирующих отношения Сторон настоящего Соглашения с Удостоверяющим центром.

6. ОБЯЗАННОСТИ СТОРОН

Стороны настоящего Соглашения обязуются:

6.1. Обеспечивать конфиденциальность закрытого ключа ЭЦП, владельцем которого является уполномоченный представитель Стороны.

6.2. Незамедлительно информировать Удостоверяющий центр о факте компрометации закрытого ключа ЭЦП, владельцем которого является уполномоченный представитель Стороны, и прекратить его использование.

6.3. Соблюдать требования эксплуатационной документации на средство электронной цифровой подписи.

6.4. Содержать в исправном состоянии программно-технические средства, которые подключены к КИС, принимать необходимые и достаточные меры для предотвращения несанкционированного доступа к программному обеспечению и средствам криптографической защиты информации.

6.5. Незамедлительно сообщать Организатору ИС о всех попытках несанкционированного доступа к программному обеспечению и средствам криптографической защиты информации.

7. РАЗРЕШЕНИЕ СПОРОВ

7.1. В случае возникновения споров и разногласий между Сторонами настоящего Соглашения в связи с использованием ЭЦП, Стороны предпримут все меры для их разрешения путем переговоров.

7.2. Любой спор, указанный в п. 7.1. настоящего Соглашения, подлежит разрешению в суде только после соблюдения претензионного порядка, с учетом особенностей, предусмотренных пунктами 9, 10 настоящего Соглашения,

7.3. Все споры и разногласия между Сторонами настоящего Соглашения, возникающие из настоящего Соглашения или в связи с ним, в том числе касающиеся его заключения, действия, исполнения, изменения, прекращения или действительности, а также споры, связанные с использованием ЭЦП, и по которым не было достигнуто соглашение, разрешаются в Арбитражном суде Челябинской области.

7.4. Любой электронный документ, подписанный с применением ЭЦП одной или несколькими сторонами Соглашения в соответствии с договорами, заключаемыми между Сторонами, может быть использован в качестве письменного доказательства в суде.

7.5. В качестве письменного доказательства в суд предоставляется копия подписанного с применением ЭЦП электронного документа на бумажном носителе, заверенная собственноручной подписью уполномоченного лица Удостоверяющего центра в порядке, предусмотренном договорами, регулирующими отношения Сторон настоящего Соглашения с Удостоверяющим центром.

8. ПРОЦЕДУРА ЭКСПЕРТИЗЫ

8.1. При разрешении в претензионном порядке споров, связанных с использованием ЭЦП, в обязательном порядке производится экспертиза, для осуществления которой привлекается Удостоверяющий центр.

8.2. Экспертиза проводится в порядке, установленном договорами, регулирующими отношения Сторон настоящего Соглашения с Удостоверяющим центром.

9. БРЕМЯ ДОКАЗЫВАНИЯ ПРИ РАЗРЕШЕНИИ СПОРОВ

9.1. В случае возникновения споров о наличии ЭЦП в электронным документе бремя доказывания лежит на Стороне, не соглашающейся с наличием ЭЦП.

9.2. В случае возникновении споров о факте внесения изменений в электронный документ после его подписания ЭЦП бремя доказывания лежит на Стороне, утверждающей, что в данный электронный документ были внесены изменения после его подписания ЭЦП владельцем сертификата ключа подписи, который является уполномоченным представителем Стороны.

9.3. В случае возникновении споров о факте получения одной из Сторон какого-либо электронного документа, подписанного ЭЦП, от другой Стороны, бремя доказывания лежит на Стороне, не соглашающейся с фактом получения электронного документа, подписанного ЭЦП.

10. ПОРЯДОК ПРИСОЕДИНЕНИЯ К СОГЛАШЕНИЮ

10.1. Присоединение к настоящему Соглашению оформляется путём подписания Подписного листа.

10.2. Присоединение к Соглашению считается состоявшимся и вступившим в силу с момента подписания Стороной Подписного листа.

10.3. Организатор ИС публикует на своем официальном сайте в Сети Интернет список Сторон настоящего Соглашения в течение 1 (Одного) рабочего дня с даты присоединения любой новой Стороны.

11. ДЕЙСТВИЕ, ИЗМЕНЕНИЕ И ПРЕКРАЩЕНИЕ СОГЛАШЕНИЯ

11.1. Стороны выражают свое согласие с тем, что настоящим Соглашением в предусмотренном им порядке регулируются их отношения со всеми Сторонами настоящего Соглашения, в любое время присоединившимися к настоящему Соглашению.

11.2. Организатор КИС, имеет право внести в одностороннем порядке изменения в настоящее Соглашение, при условии уведомления Сторон настоящего Соглашения о вносимых изменениях не позднее чем за 30 дней до их вступления в силу.

11.3. Организатор ИС уведомляет Стороны настоящего Соглашения о вносимых изменениях путем публикации принятого решение о внесении изменений в настоящее Соглашение с текстом изменений на своем официальном сайте в Сети Интернет.

11.4. Настоящее Соглашение прекращается в случаях и порядке, предусмотренных законодательством Российской Федерации.

11.5. Настоящее Соглашение прекращается в отношении Стороны по настоящему Соглашению, в случае прекращения действия договора, регулирующего отношения Стороны по настоящему Соглашению с Удостоверяющим центром.

11.6. Прекращение настоящего Соглашения не освобождает Стороны от исполнения обязательств, возникших до его прекращения, а также от ответственности за неисполнение (ненадлежащее исполнение) условий настоящего Соглашения.

ПОДПИСНОЙ ЛИСТ

к Соглашению о применении электронной цифровой подписи в информационной системе

Для юр. лица:(полное наименование организации с указание организационно-правовой формы, зарегистрированн__ по адресу (место нахождения, указанное в учредительных документах)

Для физ. лица:(Ф.И.О., паспортные данные)

1)присоединяется к Соглашению о применении электронной цифровой подписи в информационной системе (далее - Соглашению) и является

Стороной Соглашения с момента предоставления Организатору ИС настоящего Подписного листа;

2)соглашается с возможностью использования в случаях и в порядке, предусмотренных Соглашением, электронной цифровой подписи при обмене электронными документами (в том числе - в процессе совершения каких-либо сделок) с любыми иными лицами, предоставившими Организатору ИС аналогичные подписные листы;

3)соглашается с тем, что изменения в Соглашение вносятся Организатором ИС в порядке, предусмотренном разделом 11 Соглашения.

Адрес для отправки сообщений об изменении редакции Соглашения или приложений к нему: _____.

Дата предоставления настоящего Подписного листа Организатору Системы КИС: _____.

Для юр. лица:

(Наименование должности и ФИО руководителя организации)

Подпись руководителя организации

Для физ. лица:

Ф.И.О

Подпись