



УТВЕРЖДАЮ

Генеральный директор
ООО «Кордон»

А.Е. Паиченко

РЕГЛАМЕНТ

Удостоверяющего центра ООО «Кордон»

г. Ростов-на-Дону

2020 г.

1. Сведения об Удостоверяющем центре

Общество с ограниченной ответственностью «Кордон», именуемое в дальнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в г. Ростов-на-Дону Инспекцией Федеральной налоговой службы за основным государственным регистрационным номером (ОГРН) 1086168002205, дата присвоения ОГРН «07» июня 2008 г.

Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации на основании действующего законодательства Российской Федерации и лицензий ФСБ России и Роскомнадзора, информация о которых размещена на официальном сайте ООО «Кордон» по адресу www.uckordon.ru (далее Официальный сайт).

Удостоверяющий центр является Аккредитованным Удостоверяющим центром. Реестр аккредитованных Министерством связи и массовых коммуникаций России Удостоверяющих центров находится в сети интернет по адресу: <http://minsvyaz.ru/ru/activity/govservices/2/>. Свидетельство об аккредитации Удостоверяющего центра размещено на Официальном сайте.

Адрес и реквизиты Удостоверяющего центра:

ИНН: 6168022453 КПП: 616801001

Юридический адрес: 344091, г. Ростов-на-Дону, ул. Малиновского, дом. 3 оф. 30

Почтовый адрес: 344091, г. Ростов-на-Дону, пр. Стачки 215Б.

Телефон: +7 (863) 322-01-45

E-mail: info@uckordon.ru

Web: www.uckordon.ru

Обособленные подразделения и офисы Удостоверяющего центра:

г. Ростов-на-Дону

1. Адрес г. 344091, г. Ростов-на-Дону, ул. Малиновского, 3 Д, 2 этаж, оф. 3

Телефон (863) 322-01-45 (многоканальный)

2. г. Ростов-на-Дону, ул. Серафимовича, д. 38

Телефон (863) 322-01-45 (доб. 11)

г. Таганрог

Адрес г. Таганрог, ул. Чехова, 64

Телефоны (8634) 37-83-33, 37-95-32

г. Волгодонск

Адрес г. Волгодонск, ул. Черникова, д. 10, офис 32

Телефоны (8639) 25-80-80, 24-80-84

г. Шахты

Адрес г. Шахты, пер. Шишкина 162, оф. 235

Телефон (8636) 22-70-45

г. Ставрополь

Адрес 355042, г. Ставрополь, ул. 50 лет ВЛКСМ, 35/5, оф.210

Телефоны (8652) 55-28-45, 72-44-58

г. Владикавказ

Адрес 362008, г. Владикавказ, пр-т Коста, 93, оф.530

Телефоны (8672) 25-44-05, 25-12-44

2. Термины и определения

Реестр Удостоверяющего центра - набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий следующую информацию:

- реестр заявлений на регистрацию в Удостоверяющем центре;
- реестр зарегистрированных пользователей Удостоверяющего центра;
- реестр заявлений на создание сертификатов ключей проверки электронной подписи;
- реестр заявлений на аннулирование (отзыв) сертификатов ключей проверки электронной подписи;
- реестр заявлений на подтверждение подлинности электронной цифровой подписи в электронном документе;
- реестр сертификатов ключей проверки электронной подписи;
- реестр изготовленных списков отозванных сертификатов;
- реестр квалифицированных сертификатов ключей проверки электронной подписи, выданные физическим лицам;

- реестр квалифицированных сертификатов ключей проверки электронной подписи, выданные юридическим лицам;
- реестр квалифицированных сертификатов ключей проверки электронной подписи, выданные физическим лицам, прекратившие свое действие;
- реестр квалифицированных сертификатов ключей проверки электронной подписи, выданные юридическим лицам, прекратившие свое действие;
- реестр аннулированных сертификатов ключей проверки электронной подписи, выданные физическим лицам;
- реестр аннулированных сертификатов ключей проверки электронной подписи, выданные юридическим лицам.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

Сертификат ключа проверки электронной подписи (далее СКПЭП) - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

Удостоверяющий центр - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

Аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;

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

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

Участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

Корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

Информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано;

Вручение сертификата ключа проверки электронной подписи - передача доверенным лицом удостоверяющего центра изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу;

Подтверждение владения ключом электронной подписи - получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной

подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата;

Администратор Удостоверяющего центра - ответственный сотрудник Удостоверяющего центра, наделенный Удостоверяющим центром полномочиями по осуществлению действий по регистрации, созданию и управлению сертификатами ключей проверки электронных подписей.

Простая электронная подпись - электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Неквалифицированная электронная подпись - электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

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

- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Список отозванных сертификатов (СОС) - 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 аннулированы или действие которых было приостановлено.

Средство криптографической защиты информации (СКЗИ) - средство вычислительной техники, осуществляющее криптографические преобразования информации для обеспечения ее безопасности.

Штамп времени электронного документа - электронный документ, подписанный электронной цифровой подписью и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе.

Уполномоченное лицо Удостоверяющего центра - физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов ключей проверки электронных подписей и списков отозванных сертификатов.

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган), и являющийся в связи с этим официальным документом;

Вручение сертификата ключа проверки электронной подписи - передача доверенным лицом удостоверяющего центра созданного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу;

Заявитель - коммерческая организация, некоммерческая организация, индивидуальный предприниматель, физическое лицо, не зарегистрированное в качестве индивидуального предпринимателя, но осуществляющее профессиональную деятельность, приносящую доход, в соответствии с федеральными законами на основании государственной регистрации и (или) лицензии, в силу членства в саморегулируемой организации, а также любое иное физическое лицо, лица, замещающие государственные должности Российской Федерации или государственные должности субъектов Российской Федерации, должностные лица государственных органов, органов местного самоуправления, работники подведомственных таким органам организаций, нотариусы и уполномоченные на совершение нотариальных действий лица (далее - нотариусы), обращающиеся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата

3. Общие положения

3.1 Статус Регламента

Регламент Удостоверяющего центра ООО «Кордон», именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров. Настоящий Регламент является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации. Настоящий Регламент определяет порядок предоставления услуг Удостоверяющего центра, а также права, обязанности, ответственность сторон. Регламент Удостоверяющего центра ООО «Кордон» доступен для ознакомления в форме электронного документа по адресу <http://uckordon.ru/>. Стороны понимают термины, применяемые в настоящем Регламенте, строго в контексте общего смысла Регламента.

3.2 Изменения (дополнения) Регламента

Все изменения (дополнения) Регламента, включая изменения (дополнения) приложений Регламента, производятся Удостоверяющим центром в одностороннем порядке. Уведомление о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром путем размещения указанных изменений (дополнений) на электронном ресурсе Удостоверяющего центра <http://uckordon.ru/> (далее электронный ресурс Удостоверяющего центра)

Любые изменения (дополнения) Регламента, вносимые Удостоверяющим центром по собственной инициативе, как связанные, так и не связанные с изменением законодательства РФ, осуществляются:

- с целью улучшений условий предоставления услуг Удостоверяющего центра;
- изменения видов предоставляемых услуг;
- изменения реквизитов Удостоверяющего центра;
- изменения структуры Удостоверяющего центра.

Изменения (дополнения) Регламента, вносимые Удостоверяющим центром по собственной инициативе, вступают в силу и становятся обязательными для всех Пользователей Удостоверяющего центра по истечении 30 (тридцати) календарных дней с даты опубликования таких изменений (дополнений) на электронном ресурсе Удостоверяющего центра.

Все изменения (дополнения) Регламента, вносимые Удостоверяющим центром в связи с изменением действующего законодательства Российской Федерации вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

Любые изменения и дополнения Регламента с момента вступления в силу распространяются на всех Пользователей Удостоверяющего центра, в том числе присоединившихся к Регламенту до даты вступления изменений (дополнений) в силу. В случае несогласия с изменениями (дополнениями), внесенными в Регламент, Сторона Регламента имеет право на прекращение действия Регламента в отношении такой Стороны до вступления в силу таких изменений (дополнений) в порядке, предусмотренном п.3.4 настоящего Регламента.

Все приложения, изменения и дополнения к настоящему Регламенту являются его составной и неотъемлемой частью.

3.3 Присоединение к Регламенту

Присоединение к настоящему Регламенту осуществляется путем предоставления заинтересованным лицом в Удостоверяющий центр соответствующего заявления о выпуске сертификата ключа подписи (Приложение №2), а также необходимых документов, указанных в приложении № 1 настоящего Регламента и заключения договора на оказание услуг Удостоверяющего центра с ООО «Кордон». Лицо, подавшее Заявление, считается присоединившемся к Регламенту и является Стороной Регламента с момента заключения договора на оказание услуг Удостоверяющего центра с ООО «Кордон». Факт присоединения лица к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент заключения договора на оказание услуг Удостоверяющего центра. Лицо, присоединившееся к Регламенту, принимает дальнейшие изменения (дополнения) Регламента, в соответствии с условиями настоящего Регламента.

3.4 Прекращение действия Регламента

Действие настоящего Регламента может быть прекращено по инициативе одной из Сторон в следующих случаях:

- по собственному желанию одной из Сторон в случае расторжения Договора на оказание услуг Удостоверяющего центра.
- нарушения одной из Сторон условий настоящего Регламента.
- нарушения одной из Сторон условий заключенного Договора на оказание услуг Удостоверяющего центра.

Каждая из Сторон вправе прекратить действие настоящий Регламент в отношении себя, при этом она обязана письменно известить другую Сторону об этом в срок не позднее, чем за 30 (тридцать) календарных дней до дня прекращения действия настоящего Регламента. После получения другой Стороной письменного уведомления об одностороннем отказе от настоящего Регламента, Стороны обязаны произвести взаиморасчеты между собой и исполнить надлежащим образом обязательства друг перед другом возникшие до даты прекращения его действия, при этом соответствующий договор на оказание услуг Удостоверяющего центра подлежит расторжению в порядке, предусмотренным этим Договором. Прекращение действия регламента не означает отказ Сторон от прав и обязанностей, возникших до даты его расторжения.

3.5 Прекращение деятельности

Деятельность Удостоверяющего центра может быть прекращена в порядке, установленном действующим законодательством Российской Федерации.

В случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим Удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты прекращения деятельности этого удостоверяющего центра. В указанном случае после завершения деятельности Удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть уничтожена. В случае прекращения деятельности Удостоверяющего центра с переходом его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций. В указанном случае после завершения деятельности Удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть передана лицу, к которому перешли функции Удостоверяющего центра, прекратившего свою деятельность.

В случае принятия решения о прекращении своей деятельности аккредитованный удостоверяющий центр обязан:

- 1) сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;
- 2) передать в уполномоченный федеральный орган в установленном порядке реестр квалифицированных сертификатов;
- 3) передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

3.6 Конфиденциальность информации

Перечень сведений, относящихся к конфиденциальной информации:

- Ключ электронной подписи, соответствующий сертификату ключа подписи, является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре. Удостоверяющий центр не осуществляет хранение закрытых ключей Пользователей Удостоверяющего центра.

- Персональная и корпоративная информация о лицах, зарегистрированных в Удостоверяющем центре, содержащаяся в Реестре Удостоверяющего центра, не подлежащая раскрытию в соответствии с действующим законодательством РФ.

Перечень сведений, не относящихся к конфиденциальной информации:

- Информация, включаемая в сертификаты ключей подписи (сертификаты ключей проверки электронных подписей) и в списки отозванных сертификатов, издаваемые Удостоверяющим центром.

- Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной. Открытая информация может публиковаться по решению Удостоверяющего центра. Место, способ и время публикации открытой информации определяется Удостоверяющим центром.

• Информация, содержащаяся в Реестрах Удостоверяющего центра, в соответствии с п. 21, 2.2 настоящего Регламента.

4. Права и обязанности сторон

4.1 Удостоверяющий центр:

- создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям);
- устанавливает сроки действия сертификатов ключей проверки электронных подписей;
- аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;
- прекращает действие выданных этим удостоверяющим центром сертификаты ключей проверки электронных подписей;
- выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;
- ведет реестр выданных и прекращенных, аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;
- устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";
- создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;
- проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;
- осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;
- осуществляет иную связанную с использованием электронной подписи деятельность.

4.1.1 Удостоверяющий центр обязан:

- информировать в письменной форме заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;
- обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании, прекращении действия сертификата ключа проверки электронной подписи;
- обеспечивать конфиденциальность созданных удостоверяющим центром ключей электронных подписей;
- отказать заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи;
- отказать заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата ключа проверки электронной подписи.

4.1.2 Аккредитованный Удостоверяющий центр обязан хранить следующую информацию:

- реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;

- сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;

- сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.

Аккредитованный Удостоверяющий центр должен хранить указанную информацию в течение срока его деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации. Хранение информации должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

Копии документов на бумажном носителе, полученные для формирования сведений, внесенных в сертификат ключа проверки электронной подписи, с резолюциями ответственных за выпуск сертификатов лиц Удостоверяющего центра, подлежат хранению в архивохранилище Удостоверяющего центра сроком не менее трех лет.

Аккредитованный Удостоверяющий центр обязан обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", к реестру квалифицированных сертификатов этого аккредитованного удостоверяющего центра в любое время в течение срока деятельности этого удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

Аккредитованный Удостоверяющий центр обязан обеспечить изготовление сертификата ключа проверки электронной подписи при личном присутствии владельца сертификата либо его уполномоченного представителя в Аккредитованный Удостоверяющий центр, при этом формирование ключа электронной подписи может быть осуществлено Удостоверяющим центром либо владельцем сертификата самостоятельно. При изготовлении сертификата ключа проверки электронной подписи Удостоверяющим центром должны быть оформлены в виде документов на бумажном носителе два экземпляра копии сертификата ключа проверки электронной подписи, которые заверяются собственноручными подписями владельца сертификата ключа проверки электронной подписи и ответственного лица Удостоверяющего центра, уполномоченного на осуществление указанного действия, а также печатью Удостоверяющего центра или его доверенного лица.

В случае принятия решения о прекращении своей деятельности аккредитованный удостоверяющий центр обязан:

- сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;

- передать в уполномоченный федеральный орган в установленном порядке реестр выданных этим аккредитованным удостоверяющим центром квалифицированных сертификатов;

- передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

При выдаче квалифицированного сертификата аккредитованный Удостоверяющий центр обязан:

- установить личность заявителя - физического лица, обратившегося к нему за получением квалифицированного сертификата;

- получить от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата.

Аккредитованный удостоверяющий центр одновременно с выдачей квалифицированного сертификата должен выдать владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

4.2. Обязанности Пользователя Удостоверяющего центра

При использовании усиленных электронных подписей Пользователи обязаны:

- обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;

- уведомлять Удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

- не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

- использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ от 6 апреля 2011 г.

При обращении в аккредитованный Удостоверяющий центр заявитель указывает на ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются) и представляет документы, подтверждающие достоверность информации, предоставленной заявителем для включения в квалифицированный сертификат, либо их надлежащим образом заверенные копии.

4.3 Права Удостоверяющего центра

Удостоверяющий центр имеет право:

- Отказать в изготовлении (создании) сертификата ключа подписи (квалифицированного сертификата, сертификата проверки электронной подписи) Пользователя Удостоверяющего центра в случае ненадлежащего оформления документов, необходимых для изготовления (создания) сертификата ключа подписи (квалифицированного сертификата, сертификата проверки электронной подписи), указанных в приложении № 1 к настоящему Регламенту.

- Отказать в изготовлении (создании) сертификата ключа подписи (квалифицированного сертификата, сертификата проверки электронной подписи) заявителю – гражданину РФ, в случае его идентификации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации *за пределами территории Российской Федерации*, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия отказывается от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", удостоверяющий центр обязан отказать такому лицу в проведении указанной идентификации;

- отказать заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи;

- отказать заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата ключа проверки электронной подписи.

- отказать заявителю в создании сертификата ключа проверки электронной подписи в случае, если достоверность сведений в документах заявителя не подтвердилась в соответствии с оригиналами документов и (или) надлежащим образом заверенных копий документов, или в соответствии с информацией, содержащейся в единой системе межведомственного электронного взаимодействия, информационных систем органов государственной власти, Пенсионного фонда Российской Федерации, Федерального фонда обязательного медицинского страхования, единой информационной системы нотариата, информационной системы налоговых и иных государственных и муниципальных органов, либо с использованием единой системы идентификации и аутентификации;

- Удостоверяющий центр вправе наделить третьих лиц (далее - доверенные лица) полномочиями по вручению сертификатов ключей проверки электронных подписей от имени этого удостоверяющего центра. При вручении сертификата ключа проверки электронной подписи доверенное лицо обязано установить личность получателя сертификата (заявителя) либо полномочия

лица, выступающего от имени заявителя, по обращению за получением данного сертификата в соответствии с порядком реализации функций удостоверяющего центра и исполнения его обязанностей, установленным наделившим указанное доверенное лицо полномочиями по вручению сертификатов ключей проверки электронной подписи удостоверяющим центром.

4.4 Права Пользователя Удостоверяющего центра

Пользователя Удостоверяющего центра имеет право:

- Применять список отозванных сертификатов ключей подписей, изготовленный Удостоверяющим центром.

- Применять сертификат ключа подписи Пользователя Удостоверяющего центра для проверки электронной цифровой подписи электронных документов в соответствии со сведениями, указанными в сертификате ключа подписи.

- Обратиться в Удостоверяющий центр с заявлением на изготовление (создание) сертификата ключа подписи (квалифицированного сертификата, сертификата проверки электронной подписи).

- Обратиться в Удостоверяющий центр с заявлением на прекращение действия сертификата ключа подписи, владельцем которого он является, в течение срока действия соответствующего закрытого ключа, на возобновление действия сертификата ключа подписи, владельцем которого он является, в течение срока действия соответствующего закрытого ключа и срока, на который действие сертификата было приостановлено.

- Обратиться в Удостоверяющий центр за получением информации о статусе сертификатов ключей подписей и их действительности на определенный момент времени, за подтверждением подлинности ЭП в электронном документе, сформированной с использованием сертификата ключа подписи, изданного Удостоверяющим центром.

5. Ответственность сторон и порядок разрешения споров

За неисполнение либо ненадлежащее исполнение условий настоящего Регламента виновная Сторона несет ответственность на основании и в порядке, предусмотренном действующим законодательством РФ и заключенным между Удостоверяющим центром и Пользователем Удостоверяющего центра соответствующим Договором.

6. Порядок предоставления и пользования услугами Удостоверяющего центра

6.1 Изготовление сертификата ключа подписи

Удостоверяющий центр осуществляет создание сертификатов ключей проверки электронных подписей юридическим и физическим лицам, индивидуальным предпринимателям, физическим лицам, не зарегистрированным в качестве индивидуального предпринимателя, но осуществляющее профессиональную деятельность, приносящую доход, в соответствии с федеральными законами на основании государственной регистрации и (или) лицензии, в силу членства в саморегулируемой организации, а также любому иному физическому лицу, лицу, замещающему государственные должности Российской Федерации или государственные должности субъектов Российской Федерации, должностному лицу государственных органов, органов местного самоуправления, работникам подведомственных таким органам организаций, нотариусам и уполномоченным на совершение нотариальных действий лица (далее - нотариусы), обращающиеся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата, только в том случае, если указанное лицо присоединилось к Регламенту в соответствии с пунктом 3.3. настоящего Регламента. Изготовление СКПЭП осуществляется на основании заявления на изготовление СКПЭП (Приложение №2) с приложением необходимых документов (Приложение №1):

при личном прибытии владельца (заявителя) уполномоченного представителя в офис Удостоверяющего центра,

либо без личного прибытия при наличии действующего квалифицированного сертификата,

либо без личного присутствия гражданина РФ путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и информации

из единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

Указанные документы предоставляются менеджеру Удостоверяющего центра, который проводит все необходимые и достаточные мероприятия по проверке предоставленных документов:

1) в порядке, установленном 63-ФЗ, идентифицировать заявителя - физическое лицо, обратившееся в Удостоверяющий центр за получением квалифицированного сертификата. Идентификация заявителя проводится:

- при его личном присутствии
- посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата

- посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации *за пределами территории Российской Федерации*, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации". При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы отказывается от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Удостоверяющий центр отказывает такому лицу в проведении указанной идентификации. Устанавливаются:

а) в отношении физического лица - фамилия, имя, а также отчество (при наличии), дата рождения, реквизиты документа, удостоверяющего личность, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования;

б) в отношении юридического лица, зарегистрированного в соответствии с законодательством Российской Федерации, - наименование, организационно-правовая форма, идентификационный номер налогоплательщика, а также основной государственный регистрационный номер и адрес юридического лица;

в) для юридического лица, зарегистрированного в соответствии с законодательством иностранного государства, - наименование, регистрационный номер, место регистрации и адрес юридического лица на территории государства, в котором оно зарегистрировано;

2) получить от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата;

3) в установленном порядке идентифицировать заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата (в целях получения от заявителя, выступающего от имени юридического лица, подтверждения правомочия обращаться за получением квалифицированного сертификата).

Идентификация заявителя проводится:

- при его личном присутствии
- посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата,

- информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации *за пределами территории Российской Федерации*, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений

из единой системы идентификации и аутентификации и информации из единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

4) Страницу сайта в информационно-телекоммуникационной сети "Интернет", с которой безвозмездно предоставляются шифровальные (криптографические) средства, указанные в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации" физическому лицу, обратившемуся к Удостоверяющему центру в целях проведения идентификации без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы (для предоставления биометрических персональных данных физического лица в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством сети "Интернет"): <http://uckordon.ru/support/download>.

При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством информационно-телекоммуникационной сети "Интернет" при выдаче сертификата ключа проверки электронной подписи отказывается от использования шифровальных (криптографических) средств, аккредитованный удостоверяющий центр обязан отказать такому лицу в проведении идентификации и выдаче сертификата ключа проверки электронной подписи.

1.1. Подтверждение достоверности сведений осуществляется одним из следующих способов:

1) с использованием оригиналов документов и (или) надлежащим образом заверенных копий документов;

2) с использованием единой системы межведомственного электронного взаимодействия, информационных систем органов государственной власти, Пенсионного фонда Российской Федерации, Федерального фонда обязательного медицинского страхования, единой информационной системы нотариата;

3) с использованием единой системы идентификации и аутентификации.

В случае, если полученные в соответствии с настоящим разделом сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и Удостоверяющим центром идентифицирован заявитель, Удостоверяющий центр осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В противном случае, а также в случаях, установленных пунктами 5 и 6 части 2 статьи 13 63-ФЗ, Удостоверяющий центр отказывает заявителю в выдаче квалифицированного сертификата.

Менеджер Удостоверяющего центра передает заявительные документы, которые прошли проверку на предмет достоверности инженеру ОКЗИ Удостоверяющего центра, который на основе предоставленных документов выполняет следующие действия:

- заносит регистрационную информацию в реестр Удостоверяющего центра;
- осуществляет средствами Удостоверяющего центра генерирование ключа электронной подписи;

- осуществляет создание СКПЭП;

- осуществляет запись ключа проверки электронной подписи на предоставленный сертифицированный ключевой носитель;

- Делает запись о создании сертификата ключа подписи в журнале учета выданных СКПЭП;

По окончании процедуры создания СКПЭП Заявителю выдаются:

- ключевой носитель, содержащий ключ электронной подписи, ключ проверки электронной подписи;

- сертификат ключа проверки электронной подписи;

- при получении квалифицированного сертификата заявителем он ознакомливается под расписку менеджером аккредитованного Удостоверяющего центра с информацией, содержащейся в квалифицированном сертификате. Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования заявителем квалифицированной электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы.

Указанное согласие, подписанное электронной подписью, в том числе простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного физического лица. Удостоверяющий центр обязан хранить информацию, подтверждающую ознакомление заявителя с информацией, содержащейся в квалифицированном сертификате, в течение всего срока осуществления своей деятельности.

- Аккредитованный удостоверяющий центр одновременно с выдачей квалифицированного сертификата выдает владельцу квалифицированного сертификата (его представителю) руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, в которое содержит также информацию об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

6.2 Плановая смена ключей пользователя (владельца СКПЭП) Удостоверяющего центра

Плановая смена сертификата ключа подписи (СКПЭП, квалифицированного сертификата) происходит по его заявлению (Приложение №2) и осуществляется согласно п. 6.1 настоящего Регламента.

6.3 Внеплановая смена ключей пользователя Удостоверяющего центра

Пользователь Удостоверяющего центра (владелец СКПЭП) самостоятельно принимает решение о факте или угрозе компрометации ключей подписи, владельцем которых он является. В случае компрометации или угрозы компрометации ключей Пользователь Удостоверяющего центра (владелец СКПЭП) предоставляет Администратору Удостоверяющего центра заявление на прекращение действия сертификата согласно п. 6.6 настоящего Регламента, после чего происходит изготовление ключей подписи (создание СКПЭП) согласно п. 6.1 настоящего Регламента.

6.4 Плановая смена ключей уполномоченного лица Удостоверяющего центра

Плановая смена ключей уполномоченного лица Удостоверяющего центра выполняется в период действия ключа Уполномоченного лица Удостоверяющего центра и осуществляется в следующем порядке:

- уполномоченное лицо Удостоверяющего центра создает новый ключ электронной подписи;
- уполномоченное лицо Удостоверяющего центра создает новый ключ проверки электронной подписи;
- уполномоченное лицо Удостоверяющего центра создает новый сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра.

Уведомление пользователей о проведении смены ключей уполномоченного лица Удостоверяющего центра осуществляется посредством размещения информации на Официальном сайте Удостоверяющего центра. Старые ключи уполномоченного лица Удостоверяющего центра используются в течение своего срока действия для формирования списков отозванных сертификатов, изданных Удостоверяющим центром в период действия ключа уполномоченного лица Удостоверяющего центра.

6.5 Внеплановая смена ключей уполномоченного лица Удостоверяющего центра

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации закрытого ключа и/или ключа электронной подписи Уполномоченного лица Удостоверяющего центра.

В случае компрометации или угрозы компрометации ключа Уполномоченного лица Удостоверяющего центра сертификат Уполномоченного лица Удостоверяющего центра отзывается, Пользователи Удостоверяющего центра уведомляются об указанном факте путем публикации информации о компрометации на Официальном сайте Удостоверяющего центра. Все сертификаты, подписанные с использованием скомпрометированного ключа уполномоченного лица Удостоверяющего центра, считаются отозванными.

После отзыва сертификата уполномоченного лица Удостоверяющего центра выполняется процедура внеплановой смены ключей уполномоченного лица Удостоверяющего центра. Процедура внеплановой смены ключей уполномоченного лица Удостоверяющего центра выполняется в порядке, указанном в п.6.4 настоящего Регламента.

Все действовавшие на момент компрометации закрытого ключа и/или ключа электронной подписи Уполномоченного лица Удостоверяющего центра сертификаты ключей подписей и/или СКПЭП, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

6.6 Прекращение действия сертификатов и аннулирование сертификатов.

6.6.1. Сертификат ключа проверки электронной подписи прекращает свое действие:

- 1) в связи с истечением установленного срока его действия;
- 2) на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- 3) в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам;
- 4) в иных случаях, установленных ФЗ-63, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между Удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи.

6.6.2. Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи в следующих случаях:

- 1) не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- 2) установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;
- 3) вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

6.6.3. Информация о прекращении действия сертификата ключа проверки электронной подписи вносится Удостоверяющим центром в реестр сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в настоящем пункте, или в течение двенадцати часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов, за исключением случая предусмотренного п.п.6.6.4. настоящего Регламента.

6.6.4. Удостоверяющий центр осуществлять публикацию списка отозванных сертификатов в течение 30 минут с момента поступления в Удостоверяющий центр заявления владельца сертификата о прекращении действия сертификата ключа проверки электронной подписи или сведений об иных оснований досрочного прекращения его действия (аннулирования).

6.6.5. Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключей подписей в расширение CRL Distribution Point сертификата ключа подписи.

Прекращение действия сертификата ключа подписи по заявлению (Приложение №5) владельца сертификата ключа осуществляется после получения, рассмотрения и обработки такого заявления Администратором Удостоверяющего центра.

В случае отказа в прекращении действия сертификата ключа подписи Удостоверяющий центр уведомляет об этом Пользователя Удостоверяющего центра.

При принятии положительного решения Администратор Удостоверяющего центра отзывает сертификат ключа подписи Пользователя Удостоверяющего центра.

6.6.6. Использование аннулированного сертификата ключа проверки электронной подписи не влечет юридических последствий, за исключением тех, которые связаны с его аннулированием. До внесения в реестр сертификатов информации об аннулировании сертификата ключа проверки электронной подписи удостоверяющий центр обязан уведомить владельца сертификата ключа проверки электронной подписи об аннулировании его сертификата ключа проверки электронной подписи путем направления документа на бумажном носителе или электронного документа.

6.7 Получение информации о статусе сертификата ключа подписи, изготовленного Удостоверяющим центром

Получение информации о статусе сертификата ключа подписи, изготовленного Удостоверяющим центром, в целях исполнения Федерального закона №63-ФЗ от 06 апреля 2011г., осуществляется на основании заявления Пользователя Удостоверяющего центра (Приложение №7). Данное заявление предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи. Данное заявление должно содержать следующую информацию:

- время и дата подачи заявления;
- время и дата (либо период времени), на момент наступления которых требуется установить статус сертификата ключа подписи;
- идентификационные данные пользователя Удостоверяющего центра, статус сертификата ключа подписи которого требуется установить;
- серийный номер сертификата ключа подписи, статус которого требуется установить.

По результатам проведения работ по заявлению оформляется справка, содержащая информацию о статусе сертификата ключа подписи, которая предоставляется Пользователю Удостоверяющего центра.

6.8 Подтверждение подлинности электронной цифровой подписи в электронном документе

По заявлению Стороны, присоединившейся к Регламенту, Удостоверяющий центр осуществляет проведение работ по подтверждению подлинности электронной цифровой подписи в электронном документе.

Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные пользователя, подлинность ЭП которого необходимо подтвердить в электронном документе;
- время и дата формирования ЭП электронного документа;
- время и дата, на момент наступления которых требуется установить подлинность ЭП.

К указанному заявлению (Приложение №8) в обязательном порядке прикладывается внешний носитель, содержащий:

- сертификат ключа подписи, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе (в виде файла стандарта CMS);
- электронный документ в виде либо одного файла стандарта CMS, содержащего данные и значение ЭП этих данных, либо двух файлов, один из которых содержит данные, а другой значение ЭП этих данных в формате стандарта CMS.

Проведение работ по подтверждению подлинности ЭП в электронном документе осуществляет Администратор Удостоверяющего центра. Заключение Удостоверяющего центра по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается Администратором и заверяется печатью Удостоверяющего центра. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

Срок проведения работ по подтверждению подлинности ЭП в одном электронном документе и предоставлению пользователю заключения по выполненной проверке составляет 5 (пять) рабочих дней с момента поступления заявления в Удостоверяющий центр.

6.9. Порядок формирования и ведения реестров квалифицированных сертификатов ключей проверки электронной подписи.

6.9.1. Формирование реестра квалифицированных сертификатов ключей проверки электронной подписи (далее квалифицированных сертификатов) осуществляется аккредитованным Удостоверяющим центром. Ведение реестра квалифицированных сертификатов включает в себя информацию:

- содержащуюся в выданных этим Удостоверяющим центром квалифицированных сертификатах;
- о датах прекращения действия или аннулирования квалифицированных сертификатов ключей и об основаниях таких прекращения или аннулирования;
- внесение изменений в реестр квалифицированных сертификатов в случае изменения сведений, содержащихся в квалифицированном сертификате;

6.9.2. Реестр квалифицированных сертификатов состоит из следующих разделов:

- квалифицированные сертификаты ключей проверки электронной подписи, выданные физическим лицам;
- квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам;
- квалифицированные сертификаты ключей проверки электронной подписи, выданные физическим лицам, прекратившие свое действие;
- квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам, прекратившие свое действие;
- аннулированные сертификаты ключей проверки электронной подписи, выданные физическим лицам;
- аннулированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам.

6.9.3. Раздел "квалифицированные сертификаты ключей проверки электронной подписи, выданные физическим лицам" содержит следующие обязательные поля:

- уникальный номер квалифицированного сертификата;
- даты начала и окончания действия квалифицированного сертификата;
- фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата;
- реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата (номер, серия, дата выдачи);
- страховой номер индивидуального лицевого счета владельца квалифицированного сертификата;
- сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.
- ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются);
- иная информация о владельце квалифицированного сертификата (по требованию заявителя).

6.9.4. Раздел "квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам" должен содержать следующие обязательные поля:

- уникальный номер квалифицированного сертификата;
- даты начала и окончания действия квалифицированного сертификата;
- наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата;
- идентификационный номер налогоплательщика владельца квалифицированного сертификата;
- реквизиты свидетельства о государственной регистрации юридического лица (для юридических лиц, зарегистрированных на территории Российской Федерации);
- реквизиты документов о государственной регистрации юридического лица в соответствии с законодательством иностранного государства (для иностранных юридических лиц);
- основные реквизиты (наименование, номер и дата выдачи) документа, подтверждающего право лица, выступавшего от имени заявителя, обращаться за получением квалифицированного сертификата
- сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат
- ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются);
- иная информация о владельце квалифицированного сертификата (по требованию заявителя).

6.9.5. Раздел "квалифицированные сертификаты ключей проверки электронной подписи, выданные физическим лицам, прекратившие свое действие" должен содержать следующие обязательные поля:

- уникальный номер квалифицированного сертификата;
- даты начала и окончания действия квалифицированного сертификата;
- фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата;
- дата прекращения действия квалифицированного сертификата;
- основание прекращения действия квалифицированного сертификата.

6.9.6. Раздел "квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам, прекратившие свое действие" должен содержать следующие обязательные поля:

- уникальный номер квалифицированного сертификата;
- даты начала и окончания действия квалифицированного сертификата;
- наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата;
- дата прекращения действия квалифицированного сертификата;
- основание прекращения действия квалифицированного сертификата.

6.9.7. Раздел "аннулированные квалифицированные сертификаты ключей проверки электронной подписи, выданные физическим лицам" должен содержать следующие обязательные поля:

- уникальный номер квалифицированного сертификата;
 - даты начала и окончания действия квалифицированного сертификата;
 - фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата;
 - дата аннулирования квалифицированного сертификата;
 - основание аннулирования квалифицированного сертификата.
- Раздел "аннулированные квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам" должен содержать следующие обязательные поля:
- уникальный номер квалифицированного сертификата;
 - даты начала и окончания действия квалифицированного сертификата;
 - наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата;
 - дата аннулирования квалифицированного сертификата;
 - основание аннулирования квалифицированного сертификата.

6.9.8. Аккредитованный Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре квалифицированных сертификатов, а также обеспечивает защиту информации, содержащейся в реестре квалифицированных сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности. Хранение информации, содержащейся в Реестре, осуществляется в форме, позволяющей проверить ее целостность и достоверность. Формирование и ведение единого реестра осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему.

6.9.9. Информация о прекращении действия квалифицированного сертификата вносится Удостоверяющим центром в соответствующий раздел реестра квалифицированных сертификатов в течение 30 минут с момента поступления документов (сведений) в Удостоверяющий центр о наступлении обстоятельств, повлекших за собой прекращение действия квалифицированного сертификата. Действие квалифицированного сертификата прекращается с момента внесения записи об этом в реестр квалифицированных сертификатов.

6.9.10. Запись об аннулировании квалифицированного сертификата в соответствующий раздел реестра квалифицированных сертификатов вносится Удостоверяющим центром в реестр квалифицированных сертификатов в течение не более чем 30 минут с момента поступления документов (сведений) о вступлении решения суда, явившемся основанием для аннулирования сертификата, в законную силу. Квалифицированный сертификат считается аннулированным с момента внесения указанной записи в реестр квалифицированных сертификатов.

6.10. Порядок предоставления информации из реестров квалифицированных сертификатов ключей проверки электронной подписи.

Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей к реестру квалифицированных сертификатов в любое время в течение срока деятельности Удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами. Доступ заинтересованных лиц к реестру квалифицированных сертификатов с использованием информационно-телекоммуникационных сетей осуществляется путем размещения, формирования и ведения реестра квалифицированных сертификатов в информационной системе головного удостоверяющего центра, являющейся составной частью инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме.

Доступ заинтересованных лиц к информационной системе головного удостоверяющего центра с целью получения сведений из реестра квалифицированных сертификатов осуществляется с использованием единого портала государственных и муниципальных услуг (функций) на безвозмездной основе.

Удостоверяющий центр предоставляет безвозмездно любому лицу по его обращению информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи. Данная информация предоставляется в форме выписки из реестра квалифицированных сертификатов и направляется обратившемуся лицу как почтовым отправлением, так и с использованием информационно-телекоммуникационных сетей (по выбору лица, обратившегося за получением информации из реестра квалифицированных сертификатов).

Срок предоставления указанной информации составляет не более 7 дней, при направлении информации почтовым отправлением и 24 часов при направлении выписки посредством информационно-телекоммуникационных сетей.

7. Структура сертификатов ключей подписи (СКПЭП), изготавливаемых Удостоверяющим центром в электронной форме

Сертификат в электронной форме представляет собой электронный документ, имеющий структуру, соответствующую стандарту Международного союза телекоммуникаций ITU-T X.509 версии 3 и рекомендации IETF (Internet Engineering Task Force) RFC 2459.

При этом квалифицированный сертификат должен содержать следующую информацию:

- 1) уникальный номер квалифицированного сертификата, даты начала и окончания его действия;
- 2) фамилия, имя, отчество (если имеется) владельца квалифицированного сертификата - для физического лица, не являющегося индивидуальным предпринимателем, либо фамилия, имя, отчество (если имеется) и основной государственный регистрационный номер индивидуального предпринимателя - владельца квалифицированного сертификата - для физического лица, являющегося индивидуальным предпринимателем, либо наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата - для российского юридического лица, либо наименование, место нахождения владельца квалифицированного сертификата, а также идентификационный номер налогоплательщика (при наличии) - для иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации);
- 3) страховой номер индивидуального лицевого счета и идентификационный номер налогоплательщика владельца квалифицированного сертификата - для физического лица либо идентификационный номер налогоплательщика владельца квалифицированного сертификата - для юридического лица;
- 4) уникальный ключ проверки электронной подписи;
- 5) наименования средств электронной подписи и средств аккредитованного удостоверяющего центра, которые использованы для создания ключа электронной подписи, ключа проверки электронной подписи, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с настоящим Федеральным законом;
- 6) наименование и место нахождения аккредитованного удостоверяющего центра, который выдал квалифицированный сертификат, номер квалифицированного сертификата удостоверяющего центра;
- 7) идентификатор, однозначно указывающий на то, что идентификация заявителя при выдаче сертификата ключа проверки электронной подписи проводилась либо при его личном присутствии, либо без его личного присутствия одним из способов, указанных в абзаце первом пункта 1 части 1 статьи 18 настоящего Федерального закона.

7.1 Структура сертификата ключа подписи Уполномоченного лица Удостоверяющего центра

Сертификат Уполномоченного лица Удостоверяющего центра содержит следующие базовые поля:

Название	Описание	Содержание
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата в Реестре сертификатов открытых ключей УЦ
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	Идентифицирующие данные Уполномоченного лица УЦ
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	Идентифицирующие данные Уполномоченного лица УЦ
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2001)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012

Issuer Sign	ЭП сертификата издателя	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
-------------	-------------------------------	--

а также сведения об издателе сертификата:

- Наименование удостоверяющего центра: <commonName>
- Место нахождения удостоверяющего центра: <countryName>, <stateOrProvinceName>, <localityName>, <streetAddress>
- Доверенное лицо удостоверяющего центра: <surname>, <givenName>
- Номер квалифицированного сертификата удостоверяющего центра: <authorityKeyIdentifier.authorityCertSerialNumber>
- Наименование средства электронной подписи: <issuerSignTool.signTool>
- Реквизиты заключения о подтверждении соответствия средства электронной подписи: <issuerSignTool.signToolCert>
- Наименование средства удостоверяющего центра: <issuerSignTool.cATool>
- Реквизиты заключения о подтверждении соответствия средства удостоверяющего центра: <issuerSignTool.cAToolCert>
- Класс средств удостоверяющего центра: <certificatePolicies>

Дополнения сертификата Уполномоченного лица Удостоверяющего центра:

Название	Описание	Содержание
Key Usage (critical)	Использование ключа	Цифровая подпись, подписывание сертификатов, автономное подписывание списка отзыва (CRL), подписывание списка отзыва (CRL)
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа Уполномоченного лица УЦ, соответствующего данному сертификату
BasicConstraints	Основные ограничения	Тип субъекта = ЦС, ограничение на длину пути = отсутствует
SzOID_CertSrv_CA_Versio	Объектный	Версия сертификата

n	идентификатор версии сертификата	Уполномоченного Удостоверяющего центра	лица
---	-------------------------------------	---	------

7.2 Структура сертификата ключа подписи Пользователя Удостоверяющего центра
Сертификат Пользователя Удостоверяющего центра содержит следующие базовые поля:

Название	Описание	Содержание
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата в Реестре сертификатов открытых ключей УЦ
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	Идентифицирующие Уполномоченного лица УЦ
Validity Period	Срок сертификата действия	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	Идентифицирующие Владельца сертификата открытого ключа
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2001)

Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭП сертификата издателя	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
INN	ИНН владельца сертификата	Идентификационный номер налогоплательщика (10-12 цифр)
OID.1.2.643.3.141.1 .1	реестровый номер страхователя	10 цифр
OID.1.2.643.3.141.1 .2	Код подразделения ФСС	4 цифры

Расширения сертификата Пользователя Удостоверяющего центра:

Название	Описание	Содержание
Key Usage (critical)	Использование ключа	Неотрекаемость; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшенный ключ	Набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре
Subject Key Identifier	Идентификатор ключа владельца	Идентификатор закрытого ключа Уполномоченного лица УЦ, соответствующего

	сертификата	данному сертификату
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего Центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Адрес точки распространения списка отозванных сертификатов
Authority Information Access	Адрес актуальных сертификатов	Службы статусов
		URL адреса web-приложения Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OCSP
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280

Расширения Key Usage, Extended Key Usage сертификата ключа подписи содержат объектные идентификаторы (OID), определяющие отношения, при осуществлении которых электронный документ, подписанный ЭП, будет иметь юридическое значение.

Сертификат ключа подписи Пользователя Удостоверяющего центра в расширении Extended Key Usage должен содержать, включая, но, не ограничиваясь, следующие области использования:

- Пользователь Центра регистрации, HTTP, TLS client (1.2.643.2.2.34.6);
- Проверка подлинности клиента (1.3.6.5.5.7.3.2);

Сертификат ключа подписи пользователя Удостоверяющего центра с поддержкой сервисов Службы актуальных статусов сертификатов и Службы штампов времени в расширении Extended Key Usage или Application Policy должен содержать, включая, но, не ограничиваясь, следующие области использования:

- Пользователь Центра регистрации, HTTP, TLS client (1.2.643.2.2.34.6);
- Проверка подлинности клиента (1.3.6.5.5.7.3.2);
- Пользователь службы актуальных статусов (1.2.643.2.2.34.26);
- Пользователь службы штампов времени (1.2.643.2.2.34.25).

7.3 Структура сертификата ключа проверки электронной подписи

Сертификат ключа проверки электронной подписи содержит следующие базовые поля:

- Версия (version)
 - Серийный номер (serial number)
 - Алгоритм подписи (signature) — в поле algorithm должен содержаться идентификатор алгоритма подписи ГОСТ Р 34.11-2012/34.10-2012 (OID.1.2.643.7.1.1.3.2)
 - Имя издателя СКПЭП (issuer) — данные из поля «Имя владельца» соответствующего СКПЭП
- УЦ

- Дата и время начала действия СКПЭП (notBefore)
- Дата и время окончания действия СКПЭП (notAfter)
- Имя владельца СКЭП (subject)
- Открытый ключ (subjectPublicKeyInfo)
- Дополнения (расширения) сертификата (Extensions). Должны содержаться следующие дополнения (порядок данным документом не регламентируется):

- Authority Key Identifier, OID.2.5.29.35, идентификатор ключа УЦ
- Key Usage, OID.2.5.29.15, область использования ключа
- Certificate Policies, OID.2.5.29.32, политики сертификата
- Subject Sign Tool, OID.1.2.643.100.111, средство ЭП владельца сертификата
- Issuer Sign Tool, OID.1.2.643.100.112, средство ЭП УЦ
- ExtendedKeyUsage, OID.2.5.29.37, расширенное использования ключа. Состав дополнения зависит от информационной системы, в которой используется СКПЭП
- CDP, OID.2.5.29.31, точки распространения списков отзыва.

Кроме того, СКПЭП может содержать другие дополнения (не критические), в зависимости от требований конкретных информационных систем, в которых они используются.

В СКПЭП любой используемый русскоязычный текст должен быть представлен в формате UNICODE, где каждый символ кодируется двумя байтами (16 бит). Для непосредственной записи в СКПЭП текст должен быть закодирован по стандарту UTF-8 (RFC 3629).

7.4 Структура списка отозванных сертификатов (CRL) Удостоверяющего центра

Название	Описание	Содержание
Version	Версия	V2
Issuer	Издатель СОС	Идентифицирующие данные Уполномоченного лица УЦ
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер

		сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reason Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановка действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭП издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего Центра, на котором подписан СОС

n	SzOID_CertSrv_CA_Versio	Объектный идентификатор версии сертификата	Версия Уполномоченного Удостоверяющего центра	сертификата лица
---	-------------------------	--	---	---------------------

8. Список объектных идентификаторов, зарегистрированных в Удостоверяющем центре

Удостоверяющему центру ООО «Кордон» присвоен OID в Российском сегменте мирового пространства идентификаторов объектов — 1.2.643.3.110.

Список объектных идентификаторов, зарегистрированных в Удостоверяющем центре и определяющих отношения, возникающие между Пользователями Удостоверяющего центра - участниками конкретных информационных систем, устанавливается регламентирующими документами данной конкретной информационной системы.

OID	Область применения
1.2.643.2.2.34.6	Пользователь Центра Регистрации, HTTP, TLS клиент
1.2.643.2.2.34.25	Пользователь службы штампов времени
1.2.643.2.2.34.26	Пользователь службы актуальных статусов
1.3.6.5.5.7.3.2	Проверка подлинности клиента
1.3.6.1.5.5.7.3.4	Защищенная электронная почта
1.3.6.1.5.5.7.3.8	Установка штампа времени – формирование электронной цифровой подписи штампов времени, предоставляемых Службой штампов времени

1.3.6.1.5.5.7.3.9	Подпись ответа службы OCSP – формирование электронной цифровой подписи ответов Службы актуальных статусов сертификатов
-------------------	--

9. Сроки действия ключей и сертификатов

9.1 Срок действия ключей и сертификатов Уполномоченного лица Удостоверяющего центра

Срок действия закрытого ключа (ключа электронной подписи) Уполномоченного лица Удостоверяющего центра составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности удостоверяющего центра, и для средства электронной цифровой подписи, с использованием которого данный ключ был сформирован, но не превышает 30 (тридцать) лет. Время начала периода действия сертификата ключа подписи (сертификата ключа проверки электронной подписи) Уполномоченного лица Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

9.2 Сроки действия ключей и сертификатов Пользователей Удостоверяющего центра

Максимальный срок действия закрытого ключа Пользователя Удостоверяющего (ключа электронной подписи Владельца) составляет 1 (Один) год. Время начала периода действия сертификата ключа подписи Пользователя Удостоверяющего центра (сертификата ключа проверки электронной подписи Владельца) и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

10. Список приложений

Приложение №1 — Перечень документов, необходимых для получения сертификата ключа подписи в Удостоверяющем центре.

Приложение № 2 — Формы заявлений на изготовление сертификата ключа подписи, а также на создание сертификата ключа проверки электронной подписи.

Приложение № 3 — Формы доверенностей.

Приложение № 4 — Форма заявления на отзыв сертификата.

Приложение № 5 — Форма заявления на получение информации о статусе сертификата.

Приложение № 6 — Форма заявления на подтверждение подлинности ЭП.

Приложение № 7 — Требования ФСБ по обеспечению безопасности информации при ее защите по уровню “С” (на уровне потребителя).

Приложение № 8 — Инструкция по доказательству принадлежности ЭП при разборе конфликтных ситуаций.

Приложение № 9 — Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи Удостоверяющего центра ООО «Кордон»

Перечень документов/сведений из них, необходимых для получения сертификата ключа подписи (СКПЭП) в Удостоверяющем центре

1. Для юридических лиц:

- Заявление в Удостоверяющий центр о выпуске сертификата ключа подписи по установленной форме, подписанное собственноручно владельцем сертификата ключа подписи и руководителем юридического лица с приложением печати юридического лица;
- Надлежащим образом заверенная копия протокола общего собрания участников (акционеров) о назначении руководителя юридического лица на должность, для юридических лиц с одним участником (акционером) - копия решения единственного участника (акционера)), для государственных или муниципальных унитарных предприятий – участников размещения заказа – надлежащим образом заверенная копия приказа/распоряжения о назначении на должность руководителя;
- Надлежащим образом заверенная копия свидетельства о постановке на учет в налоговом органе юридического лица (ИНН);
- Надлежащим образом заверенная копия свидетельства о государственной регистрации юридического лица (ОГРН);
-
- Согласие на обработку персональных данных заявителя.

1.1. ДОПОЛНИТЕЛЬНО ПРЕДСТАВЛЯЕТСЯ:

1.1.1. В случае выдачи квалифицированного сертификата юридическому лицу, в котором в качестве владельца квалифицированного сертификата наряду с указанием наименования юридического лица указывается физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица без доверенности:

- Страховое свидетельство государственного пенсионного страхования - физического лица, действующее от имени юридического лица (СНИЛС)
- Паспорт гражданина Российской Федерации, на чье имя изготавливается сертификат ключа подписи, для предъявления (2,3,4,5 и 19 страницы)
- Согласие на обработку персональных данных лица, указанного в п.1.1.1 п.1.1. настоящего раздела.

1.1.2. В случае выдачи квалифицированного сертификата юридическому лицу, в котором в качестве владельца квалифицированного сертификата наряду с указанием наименования юридического лица указывается физическое лицо, действующее от имени юридического лица на основании доверенности:

- Паспорт гражданина Российской Федерации уполномоченного представителя для предъявления (2,3,4,5 и 19 страницы).
- Страховой номер индивидуального лицевого счета - физического лица, действующее от имени юридического лица (СНИЛС)
- Доверенность по установленной форме, удостоверенная подписью единоличного исполнительного органа юридического лица и печатью этого юридического лица.
- Согласие на обработку персональных данных физического лица, действующее от имени юридического лица на основании доверенности

1.1.3. Если от имени юридического лица ((государственного/муниципального предприятия, некоммерческой организации) за получением квалифицированного сертификата прибыл представитель по доверенности не владелец квалифицированного сертификата:

- Доверенность по установленной форме, удостоверенная подписью единоличного исполнительного органа юридического лица и печатью этого юридического лица.
- Паспорт для предъявления представителя и копии паспорта единоличного исполнительного органа, владельца сертификата ключа подписи для предъявления (2,3,4,5 и 19 страницы)
- Согласие на обработку персональных данных представителя.

1.1.4. Если полномочия единоличного исполнительного органа открытого/закрытого акционерного общества переданы управляющей организации/управляющему:

- Надлежащим образом заверенная копия решения общего собрания акционеров общества о передаче функций единоличного исполнительного органа управляющей организации/управляющему
- Надлежащим образом заверенная копия свидетельства о постановке на учет в налоговом органе юридического лица/физического лица – управляющей организации / управляющего (ИНН);
- Надлежащим образом заверенная копия первого, второго листов устава общества, листа устава, где предусмотрена возможность передачи полномочий единоличного исполнительного органа общества

управляющей организации/управляющему, а также последнего листа устава общества с отметкой налогового органа;

- Надлежащим образом заверенная копия свидетельства о государственной регистрации юридического лица –управляющей организации (ОГРН);

- Паспорт гражданина Российской Федерации управляющего /уполномоченного представителя управляющей компании для предъявления, а также его копия (2,3,4,5 и 19 страницы).

- Страховой номер индивидуального лицевого счета представителя юридического лица, если он наряду с юридическим лицом указан в качестве владельца ключа электронной подписи.

- Согласие на обработку персональных данных представителя управляющей компании/ руководителя управляющей компании/ управляющего.

1.1.5. Если юридическое лицо является иностранным юридическим лицом, оно представляет:

- заявление в Удостоверяющий центр о выпуске квалифицированного сертификата ключа проверки электронной подписи участника электронных аукционов;

- документ, подтверждающий правомочия представителя обращаться от имени юридического лица за получением квалифицированного сертификата;

- основной документ, удостоверяющий личность представителя юридического лица;

- номер свидетельства о постановке на учет в налоговом органе заявителя - иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) или идентификационный номер налогоплательщика заявителя - иностранной организации;

Все представляемые документы, исходящие от иностранного государственного органа, должны содержать легализацию и/или апостиль с нотариальным переводом (Гаагская конвенция 1961 г.)

- Нотариальная копия документа, свидетельствующая о создании и регистрации такого иностранного юридического лица на территории иностранного государства,

- Нотариальная копия документа, содержащая регистрационный номер в стране регистрации,

- Нотариальная копия документа, содержащая код налогоплательщика в стране регистрации или его аналог,

- Нотариальная копия документа, подтверждающая правоспособность юридического лица - выписку из торгового реестра страны происхождения или иного эквивалента доказательства юридического статуса, признаваемого в качестве таковых законодательством страны учреждения.

1.1.6. Если иностранное юридическое лицо имеет филиал или представительство иностранного юридического лица на территории Российской Федерации дополнительно к документам, указанным в п.1.1.5 предоставляется:

- Нотариальная копия Свидетельства об аккредитации на территории Российской Федерации представительств (филиалов) иностранных компаний, выданное ФНС России.

1.1.7. Если единоличный исполнительный орган / владелец сертификата ключа подписи / иной уполномоченный представитель юридического лица является иностранным гражданином или лицом без гражданства дополнительно предоставляются:

- Нотариальную копию паспорта иностранного государства с нотариальным переводом — только для иностранного гражданина;

- вид на жительство (для лица без гражданства это документ удостоверяющий личность), либо разрешение на временное проживание, либо визу и (или) миграционную карту, либо иные предусмотренные федеральным законом или международным договором Российской Федерации документы, подтверждающие право иностранного гражданина на пребывание (проживание) в Российской Федерации;

- нотариальную копию разрешения на привлечение и использование иностранных работников и лиц без гражданства, выданное Федеральной миграционной службой, органами исполнительной власти субъектов Российской Федерации, осуществляющими переданные полномочия Российской Федерации в области содействия занятости населения, Федеральным агентством морского и речного транспорта и Федеральным агентством по рыболовству, а иностранный гражданин или лицо без гражданства предоставляет нотариальную копию разрешения на работу.

В случае, если в силу Федерального закон от 25.07.2002 № 115-ФЗ «О правовом положении иностранных граждан в Российской Федерации» иностранный гражданин или лицо без гражданства и/или юридическое лицо – Работодатель иностранного гражданина или лица без гражданства вправе не получать указанные разрешения, они предоставляют в ООО «Кордон» официальное письмо на фирменном бланке о таком праве со ссылкой на норму Федерального закон от 25.07.2002 № 115-ФЗ «О правовом положении иностранных граждан в Российской Федерации», подписанное единоличным исполнительным органом юридического лица и его главным бухгалтером с приложением печати этого юридического лица.

2. Для индивидуальных предпринимателей и лиц к ним приравненных в соответствии с действующим законодательством РФ (фермерские (крестьянские) хозяйства, адвокаты, нотариусы и т.д.):

- Заявление в Удостоверяющий центр о выпуске сертификата ключа подписи по установленной форме, подписанное собственноручно владельцем сертификата ключа подписи и индивидуальным предпринимателем с печатью индивидуального предпринимателя;
- Надлежащим образом заверенная копия свидетельства о постановке на учет в налоговом органе индивидуального предпринимателя (ИНН);
- Надлежащим образом заверенная копия свидетельства о государственной регистрации индивидуального предпринимателя (ОГРНИП)/ иного свидетельства, подтверждающего статус заявителя;
- Паспорт гражданина Российской Федерации — индивидуального предпринимателя, на чье имя изготовлен сертификат ключа подписи, а также его копия (2,3,4,5 и 19 страницы);
- Согласие на обработку персональных данных владельца сертификата ключа подписи/ заявителя.
- Страховой номер индивидуального лицевого счета.

2.1. Дополнительно предоставляются:

2.1.1. Если сертификат ключа подписи изготавливается на имя уполномоченного представителя индивидуального предпринимателя:

- Доверенность, подтверждающую полномочия владельца ключа подписи, заверенная подписью индивидуального предпринимателя и печатью индивидуального предпринимателя, в случае отсутствия печати у индивидуального предпринимателя нотариальная доверенность.
- Согласие на обработку персональных данных владельца сертификата ключа ЭП.
- Страховой номер индивидуального лицевого счета представителя индивидуального предпринимателя, если он наряду с юридическим лицом указан в качестве владельца ключа электронной подписи.

2.1.2. Если сертификат ключа подписи получает не владелец сертификата, а его уполномоченный представитель:

- Паспорт гражданина Российской Федерации уполномоченного представителя для предъявления;
- Доверенность на представителя индивидуального предпринимателя, уполномоченного на получение изготовленного сертификата ключа подписи, заверенную подписью индивидуального предпринимателя и печатью индивидуального предпринимателя;
- Согласие на обработку персональных данных уполномоченного представителя.

1.1.5. Если индивидуальный предприниматель / владелец сертификата ключа подписи / иной уполномоченный представитель индивидуального предпринимателя является иностранным гражданином или лицом без гражданства:

- Нотариальную копию паспорта иностранного государства с нотариальным переводом — только для иностранного гражданина;
- вид на жительство (для лица без гражданства это документ удостоверяющий личность), либо разрешение на временное проживание, либо визу и (или) миграционную карту, либо иные предусмотренные федеральным законом или международным договором Российской Федерации документы, подтверждающие право иностранного гражданина на пребывание (проживание) в Российской Федерации;
- нотариальную копию разрешения на привлечение и использование иностранных работников и лиц без гражданства, выданное Федеральной миграционной службой, органами исполнительной власти субъектов Российской Федерации, осуществляющими переданные полномочия Российской Федерации в области содействия занятости населения, Федеральным агентством морского и речного транспорта и Федеральным агентством по рыболовству, а иностранный гражданин или лицо без гражданства предоставляет нотариальную копию разрешения на работу.

В случае, если в силу Федерального закон от 25.07.2002 № 115-ФЗ «О правовом положении иностранных граждан в Российской Федерации» иностранный гражданин или лицо без гражданства и/или юридическое лицо — Работодатель иностранного гражданина или лица без гражданства вправе не получать указанные разрешения, они предоставляются в ООО «Кордон» официальное письмо на фирменном бланке о таком праве со ссылкой на норму Федерального закон от 25.07.2002 № 115-ФЗ «О правовом положении иностранных граждан в Российской Федерации», подписанное единоличным исполнительным органом юридического лица и его главным бухгалтером с приложением печати этого юридического лица.

• Для физических лиц.

- Заявление в Удостоверяющий центр о выпуске сертификата ключа подписи по установленной форме, подписанное владельцем сертификата ключа подписи;
- Паспорт гражданина Российской Федерации, на чье имя изготовлен сертификат ключа подписи, а также его копия (2,3,4,5 и 19 страницы).

- ИНН физического лица.
- Согласие на обработку персональных данных владельца сертификата ключа подписи/ заявителя.
- Страховой номер индивидуального лицевого счета.

3.1. Дополнительно предоставляются:

3.1.1. Если сертификат ключа подписи получает не владелец сертификата ключа подписи, а его уполномоченный представитель:

- Паспорт гражданина Российской Федерации уполномоченного представителя для предъявления;
- Нотариальную доверенность на представителя физического лица, уполномоченного на получение изготовленного сертификата ключа подписи;
- Согласие на обработку персональных данных уполномоченного представителя.

3.1.2. Если физическое лицо / его уполномоченный представитель является иностранным гражданином или лицом без гражданства:

- Нотариальную копию паспорта иностранного государства с нотариальным переводом – только для иностранного гражданина;
- Вид на жительство (для лица без гражданства это документ удостоверяющий личность), либо разрешение на временное проживание, либо визу и (или) миграционную карту, либо иные предусмотренные федеральным законом или международным договором Российской Федерации документы, подтверждающие право иностранного гражданина на пребывание (проживание) в Российской Федерации.

3.1.3. Если физическое лицо является несовершеннолетним, достигшим возраста 14 лет и не достигшим возраста 18 лет:

3.1.3.1. Если несовершеннолетний, приходит с законным представителем - родителем, опекуном, попечителем дополнительно:

- согласие на обработку персональных данных законного представителя

3.1.3.2. Если несовершеннолетний, приходит с бабушкой/дедушкой, которые не являются законными представителями ребенка, дополнительно:

- Доверенность, заполненную родителем по установленной форме. Если они приносят Согласие на совершение сделки от родителя, то доверенность не требуется.

- Согласие на обработку персональных данных на ребенка и на представителя.

3.1.3.3. Если несовершеннолетний приходит самостоятельно, дополнительно:

- Согласие на совершение сделки от законного представителя
- Согласие на обработку персональных данных законного представителя

ВНИМАНИЕ! При создании квалифицированного сертификата для применения на портале www.gosuslugi.ru в качестве владельца сертификата должно быть указано должностное лицо юридического лица, имеющее полномочия действовать без доверенности от имени юридического лица.

Формы заявлений на изготовление сертификата ключа подписи

Генеральному директору
ООО «Кордон»
Панченко А.Е.

ЗАЯВЛЕНИЕ

на создание квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи

(полное фирменное наименование юридического лица, включая организационно-правовую форму/ИП/ФИО физ. ли		
(должность, фамилия, имя, отчество)		
действующего	на	основании

просит создать квалифицированный ключ ЭП и квалифицированный сертификат ключа проверки электронной подписи на имя владельца квалифицированного сертификата ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении данными:

Наименование организации/ИП/ Ф.И.О. физ. лица	
Наименование подразделения (при наличии)	
Должность	
Фамилия	
Имя	
Отчество	
Наименование населенного пункта	
Название улицы, номер дома (юр.адрес компании)	
Область (Наименование субъекта РФ)	
Страна	RU
ИНН	
КПП	
ОГРН	
СНИЛС	
Адрес электронной почты	
Перечень ЭТП	
☐ РТС (6-фед площадок)	☐ ЭТП Фабрикант
☐ Сайт www.zakupki.gov.ru в целях 223-ФЗ	☐ АЭТП
☐ ЭТП В2В	☐ ЭТП ТЭК-Торг ОАО "НК Роснефть"
☐ ЭТП Автодор-Торговые Системы	☐ ЭТП Газнефтеторг

☐ ЭТП АСТ ГОЗ	☐ ЭТП ГПБ
Перечень Государственных систем	
☐ Универсальный сертификат	☐ ФСРАР
☐ ЕФРСБ, ЕФРСДЮЛ	☐ Система электронных паспортов (АС СЭП)
☐ ФТС России	☐ ЕГАИС
☐ ФИС ФРДО	☐ Росреестр
☐ ГАС РФ "Правосудие"	☐ nalog.ru, gosuslugi.ru
☐ ФГИС Меркурий	☐ Для поступления в учебные учреждения
☐ Честный знак	☐ Электронные больничные и ЕГИСЗ
Для подключения к сдаче отчетности	
☐ Первичное подключение к системе	☐ Регенерация (продление) ключа ЭП
☐ Подключение дополнительного направления сдачи отчетности (дополнительной НИ)	
☐ Смена владельца ключа ЭП	☐ Восстановление ключа
Перечень подключаемых органов	
☐ ИФНС	☐ ПФР
☐ Статистика	☐ ФСС
☐ ФСРАР	☐ ЕГАИС
Коды подключаемых налоговых инспекций	
Орган подключаемой Гос. статистики	
Рег. номер ПФР	
Данные соглашения с ПФР	1 : лата « » 20 г.

Контактное лицо:

Моб. _____ телефон _____ контактного _____ лица: _____

Настоящим

 (фамилия, имя, отчество заявителя)

 (серия и номер паспорта, кем и когда выдан, кол. подразделение)

даю согласие ООО «Кордон», ОГРН 1086168002205, дата присвоения ОГРН: 7 июня 2008 г. на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 части первой статьи 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», с информацией, необходимой ООО «Кордон», в связи с договорными отношениями по изготовлению касающееся меня - владельца ключа квалифицированного сертификата в Удостоверяющем центре ООО «Кордон» и полученные у меня лично, в том числе на основании предъявленных мной в ООО «Кордон» документов: паспорта, ИНН, СНИЛС, необходимых для изготовления квалифицированного сертификата и признаю, что персональные данные, заносимые в ООО «Кордон» в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Настоящим

(фамилия, имя, отчество заявителя)

(серия и номер паспорта, кем и когда выдан, кол. подразделений)

даю согласие ООО «Кордон», ОГРН **1086168002205**, дата присвоения ОГРН: 7 июня 2008 г. на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 части первой статьи 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», с информацией, необходимой ООО «Кордон», в связи с договорными отношениями по изготовлению касающееся меня - владельца ключа квалифицированного сертификата в Удостоверяющем центре ООО «Кордон» и полученные у меня лично, в том числе на основании предъявленных мной в ООО «Кордон» документов: паспорта, ИНН, СНИЛС, необходимых для изготовления квалифицированного сертификата и признаю, что персональные данные, заносимые в ООО «Кордон» в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Об ответственности за достоверность представленных сведений предупрежден (предупреждена).

Настоящее согласие действует со дня его подписания до дня истечения срока хранения квалифицированного сертификата в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Настоящим

(фамилия, имя, отчество заявителя)

(серия и номер паспорта, кем и когда выдан, кол. подразделений)

даю согласие ООО «Кордон», ОГРН **1086168002205**, дата присвоения ОГРН: 7 июня 2008 г. на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 части первой статьи 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», с информацией, необходимой ООО «Кордон», в связи с договорными отношениями по изготовлению касающееся меня - владельца ключа квалифицированного сертификата в Удостоверяющем центре ООО «Кордон» и полученные у меня лично, в том числе на основании предъявленных мной в ООО «Кордон» документов: паспорта, ИНН, СНИЛС, необходимых для изготовления квалифицированного сертификата и признаю, что персональные данные, заносимые в ООО «Кордон» в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Настоящим

(фамилия, имя, отчество владельца квалифицированного сертификата)

(серия и номер паспорта, кем и когда выдан, кол. подразделений)

даю согласие ООО «Кордон», ОГРН **1086168002205**, дата присвоения ОГРН: 7 июня 2008 г. на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 части первой статьи 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», с информацией, необходимой ООО «Кордон», в связи с договорными отношениями по изготовлению касающееся меня - владельца ключа квалифицированного сертификата в Удостоверяющем центре ООО «Кордон» и полученные у меня лично, в том числе на основании предъявленных мной в ООО «Кордон» документов: паспорта, ИНН, СНИЛС, необходимых для изготовления квалифицированного сертификата и признаю, что персональные данные, заносимые в ООО «Кордон» в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Об ответственности за достоверность представленных сведений предупрежден (предупреждена).

Настоящее согласие действует со дня его подписания до дня истечения срока хранения квалифицированного сертификата в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Настоящим

(фамилия, имя, отчество заявителя)

(серия и номер паспорта, кем и когда выдан, кол. подразделений)

уведомляет и гарантирует, что в соответствии с Учредительными и внутренними документами

(полное фирменное наименование юридического лица, включая организационно-правовую форму/ИП/ФИО)

мои полномочия как единоличного исполнительного органа не ограничены, и я имею право действовать от имени

(полное фирменное наименование юридического лица, включая организационно-правовую форму/ИП/ФИО)

без доверенности, с правом участия в качестве участника размещения заказа на электронных площадках, отобранных для проведения открытых аукционов в электронной форме в соответствии с Федеральным закон от 05.04.2-13г. №44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», с правом подачи соответствующих документов для участия в открытом аукционе, с правом подписания шаблона государственного контракта, государственного контракта с правом передоверия указанных полномочий.*

* Заполняется в случае приобретения подписи для электронных торговых площадок

« ____ » _____ 20 ____ г.

Владелец

СКПЭП

(КЭП): _____

(подпись)

расшифровка подписи Ф.И.О. полностью

Заявитель Руководитель организации/ИП/физическое лицо

Указать должность (при наличии)
полностью

(подпись)

расшифровка подписи Ф.И.О.

М.П. (при наличии)

Приложение №3 к Регламенту

Формы доверенностей

(Форма доверенности, в случае если: Руководитель организации и владелец сертификата ключа подписи - два разных лица и ключ получает сам владелец сертификата ключа подписи)

ФИРМЕННЫЙ БЛАНК ДОВЕРИТЕЛЯ

Доверенность № ____

_____ две тысячи _____ года
г. _____

_____ ОГРН _____

(полное фирменное наименование юридического лица, включая организационно-правовую форму)

(далее именуемое «Общество»), в лице _____,
(должность, фамилия, имя отчество полностью)

действующего на основании Устава, паспорт: _____,
(серия, номер документа, кем выдан, дата выдачи, код подразделения)

настоящей доверенностью уполномочивают владельца сертификата ключа подписи _____,
(должность, фамилия, имя отчество полностью), паспорт: _____,
(серия, номер документа, кем выдан, дата выдачи, код подразделения)

подразделения)

зарегистрирован по адресу: _____, совершать от имени и в интересах Общества и владельца сертификата ключа подписи нижеследующие распорядительные действия:

- представлять интересы Общества в Удостоверяющем центре ООО «Кордон»;
- вести переговоры от имени Общества по заключению договора **об оказании услуг по созданию квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи** от имени Общества с ООО «Кордон», заключить его и исполнить с правом подписи указанного договора, всех приложений к нему, в том числе актов выполненных работ и приема-передачи СКЗИ в эксплуатацию, актов приема-передачи неисключительных прав на программное обеспечение, а так же иных документов необходимых для заключения и исполнения указанного договора и получения одного подлинного экземпляра указанных документов;
- с правом подачи заявки (заявления) на изготовление квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи, подписанной его собственноручной подписью;
- с правом присутствия при изготовлении его квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи;
- с правом получения квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи, ключевого носителя;
- с правом подписи регистрационных журналов, а также совершать все действия и формальности, связанные с выполнением данного поручения

(фамилия, имя отчество полностью)

имеет право подписи на всех необходимых для осуществления указанных полномочий документах, в том числе право подписать с использованием квалифицированной электронной подписи.

Полномочия по настоящей доверенности не могут быть переданы другим лицам.

Настоящая доверенность выдана сроком на _____ (_____) _____.

Образец подписи _____ удостоверяю.

Генеральный директор

М.П.

(Форма доверенности, в случае если: Руководитель организации и владелец сертификата ключа подписи - два разных лица и ключ получает сам владелец сертификата ключа подписи)

<фирменный бланк доверителя>

Доверенность № _____

_____ две тысячи _____ года

г. _____

_____ ОГРН _____,

(полное фирменное наименование юридического лица, включая организационно-правовую форму)

(далее именуемое «Общество»), в лице _____,

(должность, фамилия, имя отчество полностью)

действующего на основании Устава, паспорт: _____,

(серия, номер документа, кем выдан, дата выдачи, код подразделения)

настоящей доверенностью уполномочивают владельца сертификата ключа подписи _____

_____, паспорт: _____,

(должность, фамилия, имя отчество полностью)

(серия, номер документа, кем выдан, дата выдачи, код подразделения)

зарегистрирован по адресу: _____, совершать от имени и в интересах
Общества и владельца сертификата ключа подписи нижеследующие распорядительные действия:

- представлять интересы Общества в Удостоверяющем центре ООО «Кордон»;
- вести переговоры от имени Общества по заключению договора **об оказании услуг по созданию квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи** от имени Общества с ООО «Кордон», заключить его и исполнить с правом подписи указанного договора, всех приложений к нему, в том числе актов выполненных работ и приема-передачи СКЗИ в эксплуатацию, актов приема-передачи неисключительных прав на программное обеспечение, а так же иных документов необходимых для заключения и исполнения указанного договора и получения одного подлинного экземпляра указанных документов;
- с правом подачи заявки (заявления) на изготовление квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи, подписанной его собственноручной подписью и подписью руководителя;
- с правом присутствия при изготовлении его квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи;
- с правом получения квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи, ключевого носителя;
- с правом подписи регистрационных журналов, а также совершать все действия и формальности, связанные с выполнением данного поручения _____

(фамилия, имя отчество полностью)

имеет право подписи на всех необходимых для осуществления указанных полномочий документах, в том числе право подписи с использованием квалифицированной электронной подписи.

Полномочия по настоящей доверенности не могут быть переданы другим лицам.

Настоящая доверенность выдана сроком на _____ (_____) _____.

Образец подписи _____ удостоверяю.

Руководитель организации

М.П.

(Форма доверенности, в случае если: Руководитель организации и владелец сертификата ключа подписи - два разных лица, и ключ получает третье уполномоченное лицо)

<<ФИРМЕННЫЙ БЛАНК ДОВЕРИТЕЛЯ>>

Доверенность № _____

_____ две тысячи _____ года
г. _____

_____ ОГРН _____,
(полное фирменное наименование юридического лица, включая организационно-правовую форму)

(далее именуемое «Общество»), в лице _____,
(должность, фамилия, имя отчество полностью)

действующего на основании Устава, и владелец сертификата ключа подписи
_____,
(должность, фамилия, имя отчество полностью)

паспорт: _____,
(серия, номер документа, кем выдан, дата выдачи, код подразделения)

настоящей доверенностью уполномочивают _____,
(должность, фамилия, имя отчество полностью)

паспорт: _____,
(серия, номер документа, кем выдан, дата выдачи, код подразделения)

зарегистрирован по адресу: _____, совершать от имени и в интересах Общества и владельца сертификата ключа подписи нижеследующие распорядительные действия:

• представлять интересы Общества и владельца сертификата ключа подписи в Удостоверяющем центре ООО «Кордон»;

• вести переговоры от имени Общества по заключению договора об оказании услуг по созданию квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи от имени Общества с ООО «Кордон», заключить его и исполнить с правом подписи указанного договора, всех приложений к нему, в том числе актов выполненных работ и приема-передачи СКЗИ в эксплуатацию, актов приема-передачи неисключительных прав на программное обеспечение, а так же иных документов необходимых для заключения и исполнения указанного договора и получения одного подлинного экземпляра указанных документов;

• с правом подачи заявки (заявления) на квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи для _____, подписанной собственноручной подписью владельца сертификата ключа подписи от его имени;

• с правом присутствия от имени и в интересах владельца сертификата ключа подписи при изготовлении его квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи для _____;

• с правом получения квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи для _____ владельца сертификата ключа подписи, ключевого носителя;

• с правом подписи регистрационных журналов от имени владельца квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи, а также совершать все действия и формальности, связанные с выполнением данного поручения _____ имеет право подписи на всех необходимых

(фамилия, имя отчество полностью)

для осуществления указанных полномочий документах в том числе право подписи с использованием квалифицированной электронной подписи.

Полномочия по настоящей доверенности не могут быть переданы другим лицам.

Настоящая доверенность выдана сроком на _____ (_____) _____.

Образец подписи _____ удостоверяю.

Владелец сертификата
ключа подписи _____

Генеральный директор _____

М.П.

(Форма доверенности, в случае если: Руководитель организации - владелец сертификата ключа подписи, ключ получает доверенное лицо)

<фирменный бланк доверителя>

Доверенность № _____

_____ две тысячи _____ года

г. _____

_____ ОГРН _____,

(полное фирменное наименование юридического лица, включая организационно-правовую форму)

(далее именуемое «Общество»), в лице _____,

(должность, фамилия, имя отчество полностью)

действующего на основании Устава, паспорт: _____,

(серия, номер документа, кем выдан, дата выдачи, код подразделения)

настоящей доверенностью уполномочивают сотрудника Общества _____

_____, паспорт: _____,

(должность, фамилия, имя отчество полностью)

(серия, номер документа, кем выдан, дата выдачи, код подразделения)

зарегистрирован по адресу: _____, совершать от имени и в интересах Общества и владельца сертификата ключа подписи нижеследующие распорядительные действия:

• представлять интересы Общества в Удостоверяющем центре ООО «Кордон»;

• вести переговоры от имени Общества по заключению договора об оказании услуг по подключению к системе электронного документооборота от имени Общества с ООО «Кордон», заключить его и исполнить с правом подписи указанного договора, всех приложений к нему в том числе актов выполненных работ и приема-передачи СКЗИ в эксплуатацию, актов приема-передачи неисключительных прав на программное обеспечение, а так же иных документов необходимых для заключения и исполнения указанного договора и получения одного подлинного экземпляра указанных документов;

• с правом подачи заявки (заявления) на изготовление квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи, подписанной его собственноручной подписью;

• с правом присутствия при изготовлении его квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи;

• с правом получения квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи, ключевого носителя;

• с правом подписи регистрационных журналов, а также совершать все действия и формальности, связанные с выполнением данного поручения

(фамилия, имя отчество полностью)

имеет право подписи на всех необходимых для осуществления указанных полномочий документах, в том числе право подписи с использованием квалифицированной электронной подписи.

Полномочия по настоящей доверенности не могут быть переданы другим лицам.

Настоящая доверенность выдана сроком на _____ (_____) _____.

Образец подписи _____ удостоверяю.

Генеральный директор

М.П.

Доверенность

_____ две тысячи _____ года
г. _____

(Ф.И.О. полностью)

являющийся (аяся) законным представителем (мать, отец, опекун, попечитель (нужное подчеркнуть)
несовершеннолетнего

_____.200__ года рождения
(ФИО полностью)

действующего на основании паспорта: _____
(серия, номер документа, кем выдан, дата выдачи, код подразделения)

настоящей

доверенностью

уполномачиваю

(ФИО полностью)

паспорт: _____,

(серия, номер документа, кем выдан, дата выдачи, код подразделения)

зарегистрированного по адресу: _____, совершать следующие действия :

- представлять интересы несовершеннолетнего

(фамилия, имя отчество полностью)

в Удостоверяющем центре ООО «Кордон»;

- вести переговоры от имени Общества по заключению договора по созданию квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи от имени несовершеннолетнего

(фамилия, имя отчество полностью)

с ООО «Кордон», заключить его и исполнить с правом подписи указанного договора, всех приложений к нему, в том числе актов выполненных работ и приема-передачи СКЗИ в эксплуатацию, актов приема-передачи неисключительных прав на программное обеспечение, а так же иных документов необходимых для заключения и исполнения указанного договора и получения одного подлинного экземпляра указанных документов, а так же иных документов необходимых для заключения и исполнения указанного договора и получения одного подлинного экземпляра указанных документов;

- с правом подачи заявки (заявления) на изготовление квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи, подписанной его собственноручной подписью;

- с правом присутствия при изготовлении его квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи;

- с правом получения квалифицированного ключа ЭП и квалифицированного сертификата ключа проверки электронной подписи, ключевого носителя;

- с правом подписи регистрационных журналов, а также совершать все действия и формальности, связанные с выполнением данного поручения

(фамилия, имя отчество полностью)

имеет право подписи на всех необходимых для осуществления указанных полномочий документах.

Полномочия по настоящей доверенности не могут быть переданы другим лицам.

Настоящая доверенность выдана сроком на _____ (_____) _____.

Образец подписи _____ удостоверяю.

Законный представитель:

Подпись

(расшифровка подписи: Ф.И.О.)

Форма заявления на аннулирование (отзыв) сертификата

Заявление

на аннулирование (отзыв) сертификата ключа подписи

Пользователя Удостоверяющего центра ООО «Кордон»

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

_____,

(фамилия, имя, отчество)

действующего на основании _____

Просит аннулировать (отозвать) сертификат ключа подписи своего уполномоченного представителя –
Пользователя Удостоверяющего центра ООО «Кордон»:

(фамилия, имя, отчество)

содержащий следующий серийный номер: _____

Пользователь Удостоверяющего центра

ООО «Кордон» _____

« ____ » _____ 20 ____ г.

м.п.

Форма заявления на получение информации о статусе сертификата

Заявление на получение информации о статусе сертификата ключа подписи, изданного Удостоверяющим центром ООО «Кордон»

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность руководителя)

(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит предоставить информацию о статусе следующего сертификата ключа подписи:

(серийный номер сертификата)

Время (период времени) на момент наступления которого требуется установить статус сертификата: с
« _____ » по « _____ ».

(Время и дата должны быть указаны по Московскому времени. Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром)

Пользователь Удостоверяющего центра

ООО «Кордон»

« _____ » _____ 20 _____ г.

М.П.

Форма заявления на подтверждение подлинности ЭП

Заявление на подтверждение подлинности электронной цифровой подписи в электронном документе

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность руководителя)

(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит подтвердить подлинность ЭП в электронном документе на основании следующих данных:

1. Файл формата CMS, содержащий сертификат ключа подписи, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе на прилагаемом к заявлению носителе – рег. № ;

2. Файл, содержащий подписанные ЭП данные и значение ЭП формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение ЭП формата CMS, на прилагаемом к заявлению носителе – рег. №.

3. Время на момент наступления которых требуется подтвердить подлинность ЭП: « ____ : ____ »
« ____ / ____ / ____ »;
Час минута день месяц год

(Время и дата должны быть указаны по Московскому времени. Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром)

Пользователь Удостоверяющего центра

ООО «Кордон» _____

« ____ » _____ 20 ____ г.

м.п.

**Требования ФСБ по обеспечению безопасности информации
при ее защите по уровню “С” (на уровне потребителя)**

Защита информации по уровню “С” означает применение процедур электронной цифровой подписи и хеширования, сертифицированных ФСБ средств криптографической информации, реализующих алгоритмы ГОСТ Р34.11-94, ГОСТ Р34.10-94 и ГОСТ 28147-89.

1. Требования по организационному обеспечению эксплуатации СКЗИ

1.1. На предприятии выделяются (определяются) должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СКЗИ.

1.2. На предприятии разрабатываются нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ.

1.3. К работе со СКЗИ допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации СКЗИ.

2. Требования по размещению СКЗИ и режиму охраны

2.1. Помещения, в которых размещаются программно-технические средства со встроенными СКЗИ, являются режимными и должны обеспечивать конфиденциальность проводимых работ.

2.2. Размещение режимных помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств.

2.3. Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

2.4. Входные двери режимных помещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время.

2.5. Окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией.

2.6. Размещение технических средств в режимном помещении должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается, через окна.

2.7. В режимные помещения допускаются Руководство Пользователя, сотрудники подразделения безопасности и исполнители, имеющие прямое отношение к обработке, передаче и приему конфиденциальных документов.

2.8. Системные блоки ЭВМ со СКЗИ оборудуются средствами контроля вскрытия.

2.9. Ремонт и/или последующее использование системных блоков осуществляется после удаления с них программного обеспечения СКЗИ (возможно согласование с Удостоверяющим центром).

3. Требования по обеспечению безопасности ключевой информации

3.1. Носители секретных ключей ЭП, шифрования и инсталляционные дискеты с ПО СКЗИ на предприятии берутся на поэкземплярный учет в выделенных для этих целей журналах.

3.2. Учет и хранение секретных ключей поручается руководством предприятия, специально выделенным сотрудникам.

3.3. Для хранения носителей секретных ключей ЭП и шифрования выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации.

3.4. Хранение ключей и инсталляционных дискет с ПО СКЗИ допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение.

3.5. Рабочие (актуальные) и резервные ключи хранятся отдельно, с обеспечением условия невозможности их одновременной компрометации.

3.6. При транспортировке носителей секретной ключевой информации обеспечиваются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.

Примечание: требования по размещению СКЗИ определяются условиями лицензирования ФСБ, правилами эксплуатации сертифицированных СКЗИ и могут уточняться при подготовке Пользователя к включению в Систему.

**Инструкция по доказательству
принадлежности ЭП при разборе конфликтных ситуаций**

В настоящей Инструкции под Пользователем понимается Заказчик, а под Удостоверяющим центром понимается Удостоверяющий центр по Договору.

Для проведения разбора конфликтной ситуации необходимы:

- Заверенный Удостоверяющим Центром (УЦ) сертификат открытого ключа ЭП Пользователя, подписавшего документ, подлинность или авторство которого оспаривается.

- Файл, содержащий текст документа и ЭП его автора, в отношении которого возникает конфликтная ситуация.

Для разбора конфликтной ситуации необходимо выполнить следующие действия:

- Произвести операцию проверки подписи электронного документа, авторство подписи которого оспаривается на рабочем месте Администратора УЦ.

- Распечатать протокол проверки подписи.

- Распечатать сертификат открытого ключа ЭП из базы данных (реестра) Удостоверяющего Центра.

- Сравнить сертификат открытого ключа ЭП представленного Стороной и распечатанный сертификат открытого ключа ЭП из базы данных Удостоверяющего Центра.

Авторство подписи под документом считается установленным, если совпадают открытые ключи ЭП представленного Стороной сертификата и сертификат открытого ключа ЭП из базы данных Удостоверяющего Центра, и в протоколе проверки подписи Пользователя сформирована запись “Подпись верна”.

РУКОВОДСТВО

по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи Удостоверяющего центра ООО «Кордон»

Настоящее Руководство составлено в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», постановлением Правительства РФ от 16 апреля 2012 г. №313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

1. Основные понятия.

Для целей настоящего Руководства используются следующие основные понятия:

1.1. электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

1.2. сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

1.3. квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

1.4. владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

1.5. ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

1.6. ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

1.7. удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

1.8. аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;

1.9. средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

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

1.11. участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

1.12. корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

1.13. информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

1.14. Заявитель — лицо, обратившиеся за получением сертификата ключа проверки электронной подписи.

2. Условия и порядок использования электронных подписей и средств электронных подписей

2.1. Эксплуатация средств электронной подписи должна проводиться в соответствии с эксплуатационной документацией.

2.2. Порядок обеспечения информационной безопасности при использовании средств электронной подписи определяется участниками электронного взаимодействия на основе требований по организационно-техническим мерам защиты, изложенным в эксплуатационной документации на СКЗИ.

2.3. Порядок проверки электронных подписей определяется организатором информационной системы электронного взаимодействия.

2.4. Ключевая информация является конфиденциальной.

2.5. Средства электронной подписи должны использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.

2.6. На предприятии выделяются (определяются) должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СКЗИ.

2.7. На предприятии разрабатываются нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации средств электронной подписи и СКЗИ.

2.8. К работе со СКЗИ допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации СКЗИ.

3. Требования по размещению СКЗИ и режиму охраны

3.1. Помещения, в которых размещаются программно-технические средства со встроенными СКЗИ, являются режимными и должны обеспечивать конфиденциальность проводимых работ.

3.2. Размещение режимных помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств.

3.3. Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

3.4. Входные двери режимных помещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время.

3.5. Окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией.

3.6. Размещение технических средств в режимном помещении должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается, через окна.

3.7. В режимные помещения допускаются Руководство Пользователя, сотрудники подразделения безопасности и исполнители, имеющие прямое отношение к обработке, передаче и приему конфиденциальных документов.

3.8. Системные блоки ЭВМ со СКЗИ оборудуются средствами контроля вскрытия.

3.9. Ремонт и/или последующее использование системных блоков осуществляется после удаления с них программного обеспечения СКЗИ (возможно согласование с Организатором Системы).

4. Требования по обеспечению безопасности ключевой информации

4.1. Носители ключей электронных подписей и установочные диски с ПО СКЗИ на предприятии берутся на поэкземплярный учет в выделенных для этих целей журналах.

4.2. Учет и хранение ключей электронных подписей поручается руководством предприятия, специально выделенным сотрудникам.

4.3. Для хранения носителей ключей электронных подписей выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации.

4.4. Хранение ключей и установочных дисков с ПО СКЗИ допускается в одном хранилище с другими документами при условии, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение.

4.5. Рабочие (актуальные) и резервные ключи хранятся отдельно, с обеспечением условия невозможности их одновременной компрометации.

4.6. При транспортировке носителей ключей электронных подписей обеспечиваются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.

4.7. Владелец сертификата ключа проверки электронной подписи самостоятельно принимает решение о факте или угрозе компрометации ключей подписи, владельцем которых он является. В случае компрометации или угрозы компрометации ключей владелец сертификата ключа проверки электронной подписи

Удостоверяющего центра предоставляет администратору Удостоверяющего центра заявление на аннулирование сертификата.

5. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи

5.1. Обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия.

5.2. Применять для формирования электронной подписи только действующий ключ электронной подписи.

5.3. Не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

5.4. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.

5.5. Немедленно обратиться в Удостоверяющий центр с заявлением на аннулирование сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

5.6. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на аннулирование действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.

5.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия.

5.8. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено.

5.9. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

5.10. Уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении.

5.11. Предоставить достоверную и полную информацию для создания ключа электронной подписи и сертификата ключа проверки электронной подписи.

6. Риски, связанные с использованием электронных подписей.

6.1. В случае указания Заявителем недостоверных сведений о заявителе, владельце квалифицированного сертификата, допущения ошибки в них Удостоверяющий центр не несет ответственности за убытки, которые могут быть понесены вследствие недостоверности сведений, содержащихся в квалифицированных сертификатах, ключе ЭП. В таком случае все риски и убытки лежат на владельце квалифицированного сертификата.

6.2. Владелец сертификата ключа проверки электронной подписи обязан сообщить Удостоверяющему центру в случае изменения сведений о нем, уполномоченном представителе Заказчика, содержащихся в Заявке (заявлении), ключе ЭП и квалифицированном сертификате в течение срока действия квалифицированного сертификата Заказчика, в срок не позднее 1 (одного) рабочего дня с момента возникновения указанных изменений с подачей соответствующей заявки (заявления) на создание нового ключа ЭП и квалифицированного сертификата. При этом Заявитель уведомлен и согласен, что с момента изменения сведений о нем, о владельце квалифицированного сертификата, уполномоченного представителя Заявителя, содержащихся в Заявке (заявлении), ключе ЭП и квалифицированном сертификате он не вправе использовать в Системе по назначению ключ ЭП и квалифицированный сертификат. В случае, если Заявитель, владелец квалифицированного сертификата не исполнил в срок указанные в настоящем пункте обязанности и/или продолжает использовать ключ ЭП и/или квалифицированный сертификат, Удостоверяющий центр не несет ответственности за убытки, которые могут быть понесены Заказчиком вследствие недостоверности сведений, содержащихся в квалифицированном сертификате, ключе ЭП. В таком случае все риски и убытки лежат на владельце квалифицированного сертификата.

6.3. Удостоверяющий центр не несет ответственности за последствия компрометации используемого ключа проверки электронной подписи, иных нарушений Регламента Удостоверяющего центра, Руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи допущенных Заказчиком (владельцем квалифицированного сертификата), эксплуатационной документации.

6.4. Владелец сертификата ключа проверки электронной подписи обязан немедленно уведомлять Удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

6.5. Владелец сертификата ключа проверки электронной подписи обязан не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

6.6. Для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, должны использоваться средства электронной подписи, имеющие подтверждение установленным требованиям в соответствии с Федеральным законом Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".

6.7. В случае, если Заявитель, владелец квалифицированного сертификата не исполнил обязанности, указанные в разделе 6 настоящего Руководства, Удостоверяющий центр не несет ответственности за убытки, которые могут быть понесены владельцем квалифицированного сертификата. В таком случае все риски и убытки лежат на владельце квалифицированного сертификата.