«Утверждаю»
Директор
ООО «Компания» Тензор»
_____ / С.В. Уваров /
«29» апреля 2025 г.

ПОРЯДОК
(Регламент)
реализации функций
и исполнения обязанностей
Удостоверяющего центра
ООО «Компания «Тензор»

Ярославль
2025 год

Термины и определения, используемые в настоящем Порядке (Регламенте) реализации функций и исполнении обязанностей Удостоверяющего центра

Термин	Определение
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.
Квалифицированный сертификат ключа проверки электронной подписи	Сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», 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, и являющийся в связи с этим официальным документом.
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.
Реестр сертификатов	Реестр выданных и аннулированных удостоверяющим центром Сертификатов, включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром Сертификатах, информацию о датах прекращения действия или аннулирования Сертификатов и об основаниях таких прекращения и аннулирования.
Удостоверяющий центр	Юридическое лицо или индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об 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.
Заявитель	Физическое лицо, обращающееся 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
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
Владелец сертификата ключа проверки электронной подписи	лицо, которому в установленном настоящим Регламентом порядке выдан сертификат ключа проверки электронной подписи, в соответствии с Федеральным законом № 63-ФЗ.
Регистрационный центр	обособленное подразделение (филиал) удостоверяющего центра или действующее на основании договора с Удостоверяющим центром юридическое лицо или индивидуальный

	предприниматель (доверенные лица), работники которых наделены полномочиями по приему заявлений на выдачу сертификатов ключей проверки электронной подписи, вручению сертификатов ключей проверки электронных подписей от имени этого удостоверяющего центра, а также обязанностями по идентификации заявителя при его личном присутствии.

Список сокращений

Сокращение	Значение
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СКПЭП, Сертификат	Сертификат ключа проверки электронной подписи
УЦ	Удостоверяющий центр
ЭП	Электронная подпись
КЭП	Квалифицированная электронная подпись
Владелец сертификата	Владелец квалифицированного сертификата ключа проверки электронной подписи
Регламент	Порядок (Регламент) реализации функций и исполнения обязанностей Удостоверяющего центра ООО «Компания «Тензор»

1. Общие положения

1.1. Предмет регулирования.

1.1.1. Настоящий Регламент разработан в соответствии с действующим законодательством Российской Федерации, в том числе с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», и устанавливает порядок реализации функций УЦ, условия предоставления и правила пользования услугами УЦ, включая права, обязанности и ответственность УЦ, Заявителя, организационные мероприятия, направленные на обеспечения работы УЦ.

1.1.2. Настоящий Регламент размещен для свободного доступа и ознакомления для всех заинтересованных лиц в электронной форме по сайте - https://tensor.ru/uc/license.

1.2. Сведения об Удостоверяющем центре.

Полное наименование: Общество с ограниченной ответственностью «Компания «Тензор»

ОГРН 1027600787994

ИНН/КПП: 7605016030/760401001

Юридический адрес: 150001, г. Ярославль, Московский пр-т, д.12

Фактический адрес: 150001, г. Ярославль, Московский пр-т, д.12

Адреса мест нахождения обособленных подразделений (филиалов) ООО «Компания «Тензор» указаны на сайте УЦ по адресу – https://tensor.ru/contacts?tab=offices.

УЦ осуществляет свою работу в круглосуточном режиме.

График работы УЦ и его обособленных подразделений по созданию и выдаче СКПЭП:

пн-пт — с 09.00 до 18.00, без обеда;

сб-вс — выходной.

График работы технической поддержки: круглосуточно.

1.3. Порядок информирования о предоставлении услуг удостоверяющего центра.

Контактные телефоны УЦ: тел./факс (4852) 262-000; 88002003015

e-mail: ca_tensor@tensor.ru

Электронный адрес: tensor.ru

Справочные телефоны, адреса сайтов, адреса электронной почты обособленных подразделений (филиалов) УЦ опубликованы на официальном сайте УЦ по адресу https://tensor.ru/contacts?tab=offices.

Информация о времени посещения офиса УЦ предоставляется при обращении Заявителя по контактным данным, указанным на официальном сайте УЦ по адресу – https://tensor.ru/branches.

Информирование Заявителя, Владельца сертификата производится на адрес электронной почты, контактный номер телефона (в том числе привязанные к нему мессенджеры, социальные сети), указанные при обращении в УЦ и/или ином взаимодействии с УЦ, и/или посредством размещения информации на сайте по адресу https://tensor.ru/uc.

1.4. Стоимость услуг Удостоверяющего центра.

УЦ осуществляет свою деятельность на платной основе.

Информация о стоимости услуг УЦ указана на сайте УЦ по адресу - https://tensor.ru/uc/tariffs (далее – Прайс).

Услуги выезда специалиста и доставки курьером осуществляется исключительно в офис организации в пределах черты населенного пункта, в котором расположено соответствующее обособленное подразделение УЦ, оборудованное специализированным рабочим местом, аттестованным на соответствие требованиям законодательства Российской Федерации по технической защите конфиденциальной информации.

Стоимость Услуг УЦ по формированию запросов может быть включена в стоимость иных договоров согласно тарифной политике ООО «Компания «Тензор».

Сроки и порядок расчётов за оказание услуг УЦ устанавливаются в соответствии с требованиями гражданского законодательства Российской Федерации. Оплата услуг может осуществляться как путем полной предоплаты (аванса), так и путем частичной предоплаты или в случае заключения контрактов по итогам проведения закупочных процедур - по факту оказания услуг.

При оплате услуг путем полной/частичной предоплаты, срок изготовления сертификата составляет 5 (пять) рабочих дней с момента осуществления следующих действий в совокупности:

а. представления всех документов, необходимых для выпуска сертификата;

б. зачисления перечисленных Заявителем денежных средств на расчетный счет УЦ.

При оказании услуг по итогам проведения закупочных процедур порядок и срок оказания услуг устанавливаются в соответствии с положениями заключенных контрактов.

Срок действия сертификата начинается с момента его изготовления согласно дате начала действия, указанной в нем.

В случае отказа заказчика от получения уже изготовленного на основании заявления сертификата, уплаченные денежные средства не возвращаются.

1.5. Присоединение к Регламенту.

1.5.1. Настоящий Регламент является договором присоединения на основании статьи 428 Гражданского кодекса РФ. Настоящий Регламент предназначен служить соглашением, налагающим обязанности на все вовлечённые стороны, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ.

1.5.2. Фактом присоединения Заявителя к настоящему Регламенту является наиболее ранний из моментов:

а. предоставление Заявителем документов, необходимых для выпуска сертификата, в том числе заявления на изготовление СКПЭП;

б. оплата счета.

1.5.3. С момента выполнения одного из требований, указанных в п.п. 1.5.2., Заявитель считается присоединившимся к Регламенту и является Стороной Регламента.

1.5.4. С момента присоединения Заявителя к настоящему Регламенту, Заявитель полностью и безоговорочно соглашается со всеми условиями настоящего Регламента и приложений к нему.

1.5.5. Заявитель, присоединившийся к настоящему Регламенту, самостоятельно отслеживает изменения (дополнения), вносимые в настоящий Регламент в виде его новой редакции путем самостоятельного ознакомления с текстом Регламента на сайте УЦ по адресу – https://tensor.ru/uc_data/reglament_uc.pdf .

1.5.6. Владелец сертификата имеет право в одностороннем порядке прекратить взаимодействие с УЦ в рамках Регламента, направив в УЦ заявление на прекращение действия выданного ему Сертификата.

1.6. Изменение (дополнение) Регламента.

1.6.1. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится УЦ в одностороннем порядке.

1.6.2. Уведомление Владельцев сертификатов о внесении изменений (дополнений) в Регламент осуществляется УЦ путем размещения новой редакции настоящего Регламента, включающей указанные изменения (дополнения), на сайте УЦ по адресу – https://tensor.ru/uc_data/reglament_uc.pdf.

1.6.3. Изменения (дополнения), вносимые УЦ в Регламент, кроме изменений (дополнений), вносимых в связи с изменениями законодательства Российской Федерации, вступают в силу и становятся обязательными для Сторон с даты их публикации на сайте по адресу: https://tensor.ru/uc_data/reglament_uc.pdf.

1.6.4. Изменения (дополнения), вносимые УЦ в Регламент в связи с изменением действующего законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу соответствующих нормативных правовых актов, повлекших изменения законодательства Российской Федерации.

1.6.5. Любые изменения, вносимые в Регламент, с момента вступления в силу распространяются на всех лиц, присоединившихся к Регламенту, независимо от даты присоединения.

В случае несогласия с изменениями Стороны настоящего Регламента имеют право на расторжение договора присоединения в соответствии с подп. 1.5.6. Регламента.

1.7. Разрешение споров.

Сторонами в споре, в случае его возникновения, считаются УЦ и Заявитель.

Стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путём переговоров.

Споры между сторонами, связанные с действием настоящего Регламента, не урегулированные в процессе переговоров, рассматриваются в судебном порядке в соответствии с действующим законодательством Российской Федерации.

2. Перечень реализуемых УЦ функций (оказываемых услуг)

В перечень реализуемых УЦ функций (оказываемых услуг) в соответствии с настоящим Регламентом, входят:

1) создание сертификатов ключей проверки электронных подписей и выдача таких сертификатов лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) при его личном присутствии либо посредством идентификации заявителя с применением информационных технологий без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата, либо 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 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2) осуществление в соответствии с правилами подтверждения владения ключом ЭП подтверждение владения заявителем ключом ЭП, соответствующим ключу проверки ЭП, указанному им для получения СКПЭП;

3) установление сроков действия СКПЭП;

4) аннулирование выданных УЦ СКПЭП;

5) выдача по обращению Заявителя средств ЭП, содержащих ключ ЭП и ключ проверки ЭП (в том числе созданные УЦ) или обеспечивающих возможность создания ключа ЭП и ключа проверки ЭП Заявителем;

6) ведение реестра выданных и аннулированных этим УЦ СКПЭП (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим УЦ СКПЭП, и информацию о датах прекращения действия или аннулирования СКПЭП и об основаниях таких прекращения или аннулирования;

7) создание по обращениям Заявителей ключей ЭП и ключей проверки ЭП;

8) проверка уникальности ключей проверки ЭП в Реестре сертификатов;

9) проверка ЭП по обращениям участников электронного взаимодействия;

10) осуществление иной деятельности, связанной с использованием ЭП;

3. Права и обязанности УЦ

3.1. УЦ обязан:

3.1.1. Информировать заявителей об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки.

3.1.2. Обеспечивать актуальность информации, содержащейся в реестре сертификатов, ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

3.1.3. 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 СКПЭП.

3.1.4. Обеспечивать конфиденциальность созданных УЦ ключей ЭП.

3.1.5. Отказать заявителю в создании СКПЭП в случае, если не было подтверждено то, что заявитель владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному заявителем для получения СКПЭП.

3.1.6. Отказать заявителю в создании СКПЭП в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки ЭП, указанного заявителем для получения СКПЭП.

3.1.7. Незамедлительно информировать владельца квалифицированного сертификата о выявленных случаях приостановления (прекращения) технической возможности использования ключа ЭП, не предусмотренных соглашением сторон, или возникновения у аккредитованного УЦ обоснованных сомнений в получении поручения от уполномоченного соглашением сторон лица об использовании ключа ЭП.

3.1.8. Не указывать в создаваемом УЦ СКПЭП ключ проверки ЭП, который содержится в СКПЭП, выданном УЦ любым другим УЦ.

3.1.9. Хранить следующую информацию: реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица.

3.1.10. Хранить информацию, указанную в ч. 1 ст. 15 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», 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.

3.1.11. Для подписания от своего имени квалифицированных сертификатов использовать квалифицированную ЭП, основанную на квалифицированном сертификате, выданном ему головным УЦ, функции которого осуществляет уполномоченный федеральный орган. Аккредитованному УЦ запрещается использовать квалифицированную ЭП, основанную на квалифицированном сертификате, выданном ему головным УЦ, функции которого осуществляет уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами.

3.1.12. Обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к реестру квалифицированных сертификатов УЦ в любое время в течение срока деятельности УЦ, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

3.1.13. В случае принятия решения о прекращении своей деятельности УЦ:

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 выданных этим УЦ квалифицированных сертификатов;

3) передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном УЦ. Ключи электронной подписи, хранимые аккредитованным удостоверяющим центром по поручению владельцев квалифицированных сертификатов электронной подписи, подлежат уничтожению в порядке, установленном федеральным органом исполнительной власти в области обеспечения безопасности.

3.1.14. Выполнять порядок реализации функций аккредитованного УЦ и исполнения его обязанностей, установленный таким аккредитованным УЦ в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций аккредитованного УЦ и исполнения обязанностей, а также с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и иными нормативными правовыми актами, принимаемыми в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3.1.15. При выдаче квалифицированного сертификата:

1) в порядке, установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», идентифицировать заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата. Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата, или путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года № 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 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», УЦ обязан отказать такому лицу в проведении указанной идентификации.

Устанавливаются 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.

2) предложить использовать шифровальные (криптографические) средства, указанные в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», физическим лицам, обратившимся к нему 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»), и указать страницу сайта в информационно-телекоммуникационной сети «Интернет», с которой безвозмездно предоставляются эти средства. 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.

3.1.16. Ознакомить Заявителя с информацией, содержащейся в квалифицированном сертификате при получении квалифицированного сертификата заявителем. 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.

3.1.17. Одновременно с выдачей квалифицированного сертификата предоставить владельцу квалифицированного сертификата руководство по обеспечению безопасности использования КЭП и средств ЭП - Правила использования СКЗИ и ЭП (Приложение №1 к настоящему Регламенту).

3.1.18. При выдаче квалифицированного сертификата направлять в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате. Требования к порядку предоставления владельцам квалифицированных сертификатов сведений о выданных им квалифицированных сертификатах с использованием единого портала государственных и муниципальных услуг устанавливаются Правительством Российской Федерации.

3.1.19. При выдаче квалифицированного сертификата по желанию владельца квалифицированного сертификата безвозмездно осуществлять его регистрацию в единой системе идентификации и аутентификации с проведением идентификации владельца при его личном присутствии.

3.2. УЦ имеет право:

3.2.1. Наделять третьих лиц (доверенных лиц) полномочиями по приему заявлений на выдачу СКПЭП, а также вручению СКПЭП от имени УЦ.

3.2.2. Выдавать СКПЭП как в форме электронных документов, так и в форме документов на бумажном носителе.

3.2.3. Направлять любым доступным способом (письма на электронную почту, смс-сообщения, сообщения в мессенджеры, социальные сети) Заявителю, Владельцу сертификата извещения, уведомления о применении СКПЭП, в том числе о выдаче, продлении и аннулировании.

3.2.4. Отказать в изготовлении СКПЭП Заявителю в случае непредставления документов, предоставления документов не в полном объеме или предоставления документов, подлинность которых вызывает сомнение.

3.2.5. Отказать в изготовлении сертификата ключа подписи Заявителю в случае, если использованное Заявителем для формирования запроса на сертификат СКЗИ не поддерживается УЦ.

3.2.6. Отказать в изготовлении сертификата ключа подписи Заявителю в случае невыполнения Заявителем обязанностей, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим Регламентом.

3.2.7. Взимать плату, размер которой не должен превышать предельный размер, порядок определения которого вправе установить Правительство Российской Федерации, за выдачу квалифицированного сертификата.

3.2.8. Подтверждать достоверность сведений, перечисленных в пунктах 1 и 2 части 1 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» 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, Фонда пенсионного и социального страхования Российской Федерации, Федерального фонда обязательного медицинского страхования, единой информационной системы нотариата;

3) с использованием единой системы идентификации и аутентификации

3.2.9. Самостоятельно устанавливать порядок реализации функций УЦ, осуществления его прав и исполнения обязанностей, определенных ст. 13 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

4. Права и обязанности Владельцев сертификатов

4.1. Владелец сертификата обязан:

4.1.1. Обеспечить конфиденциальность ключа ЭП. Не использовать ключ ЭП и немедленно обратиться в аккредитованный УЦ, выдавший сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа ЭП нарушена.

4.1.2. Извещать УЦ обо всех изменениях данных, внесенных в сертификат.

4.1.3. В заявление на СКПЭП указать действующие электронный почтовый адрес и номер телефона Владельца сертификата для получения извещений, уведомлений от УЦ, связанных с применением СКПЭП, в том числе с его аннулированием, продлением, выпуском.

4.1.4. Хранить в тайне личный закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

4.1.5. Применять для формирования электронной цифровой подписи только действующий личный закрытый ключ.

4.1.6. Не применять личный закрытый ключ, если ему стало известно, что этот ключ используется или использовался ранее другими лицами.

4.1.7. Применять личный закрытый ключ только в соответствии с областями использования, указанными в соответствующем данному закрытому ключу сертификате ключа подписи.

4.1.8. Немедленно обратиться в УЦ с заявлением на аннулирование действия СКПЭП в случае утери, кражи, а также в случае, если Владельцу сертификата стало известно, что ключ используется или использовался ранее другими лицами.

4.1.9. Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление, на аннулирование которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование сертификата по момент времени официального уведомления об аннулировании сертификата.

4.1.10. Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, который аннулирован.

4.1.11. Предоставлять в УЦ только достоверную информацию.

4.2. Владелец сертификата имеет право:

4.2.1. Владелец сертификата, выданного в форме электронного документа, вправе получить также копию СКПЭП на бумажном носителе, заверенную УЦ.

4.2.2. Обратиться в УЦ с заявлением на изготовление СКПЭП.

4.2.3. Обратиться в УЦ с заявлением на аннулирование/прекращение действия СКПЭП, владельцем которого он является, в течение срока действия соответствующего закрытого ключа. В случае, если СКПЭП выдавалось физическому лицу, которое является сотрудником юридического лица, осуществившего оплату за выдачу СКПЭП, владельцем признается наряду с физическим лицом-сотрудником, на чье имя выдан СКПЭП, юридическое лицо-работодатель.

4.2.4. Обратиться в УЦ за получением информации о статусе сертификатов ключей подписей и их действительности на определенный момент времени.

4.2.5. Обратиться в УЦ за подтверждением действительности ЭП в электронном документе, сформированной с использованием сертификата ключа подписи, изданного УЦ.

4.2.6. В одностороннем порядке прекратить взаимодействие с УЦ в рамках Регламента, направив в УЦ заявление на прекращение действия выданного ему Сертификата.

5. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг УЦ

5.1. Процедура создания ключей ЭП и ключей проверки ЭП.

5.1.1. Порядок создания ключей ЭП и ключей проверки ЭП.

Ключ ЭП и ключ проверки ЭП, предназначенные для создания и проверки усиленной КЭП, в соответствии с частью 4 статьи 5 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» создаются с использованием средства ЭП, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

Создание ключей ЭП и ключей проверки ЭП осуществляется аккредитованным УЦ одним из способов:

1) Создание Ключей ЭП и ключей проверки ЭП осуществляется в Регистрационном центре, имеющем Лицензию ФСБ Российской Федерации на соответствующие виды работ, в соответствии с постановлением Правительства российской Федерации от 16.04.2012 № 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)» (далее – лицензированный Регистрационный центр).

Ключ ЭП и соответствующий ему ключ проверки ЭП изготавливаются в УЦ на специализированном рабочем месте, аттестованном на соответствие требованиям законодательства Российской Федерации по технической защите конфиденциальной информации, которое размещено в аттестованном помещении лицензированного Регистрационного центра, доступ в которое ограничен.

Ключ ЭП и ключ проверки ЭП, предназначенные для создания и проверки усиленной квалифицированной ЭП, в соответствии с ч. 4 ст. 5 Федерального закона «Об электронной подписи» создаются с использованием средства ЭП, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности на автоматизированном рабочем месте УЦ, используемом для создания ключа ЭП и ключа проверки ЭП для заявителя, соответствующем требованиям, установленным постановлением Правительства Российской Федерации от 3 февраля 2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

2) Создание Ключей ЭП осуществляется Заявителем самостоятельно на своем рабочем месте, при этом Заявитель создает Ключ ЭП на своем рабочем месте с использованием предоставленных УЦ либо собственных Средств ЭП.

Ключ ЭП и ключ проверки ЭП, независимо от способа создания, записывается на ключевой носитель в соответствии с эксплуатационной документацией на используемое СКЗИ.

5.1.2. Планы, основание, процедуры, сроки и порядок смены ключей ЭП УЦ, порядок информирования владельцев квалифицированных сертификатов об осуществлении такой смены с указанием доверенного способа получения нового квалифицированного сертификата УЦ.

Плановая смена ключей ЭП УЦ выполняется в период действия ключа ЭП УЦ.

Плановая смена ключей ЭП производится по следующим основаниям:

1) истечение срока действия СКПЭП;

2) переход на использование новых стандартов ЭП и функции хеширования в соответствии с руководящими документами органа исполнительной власти, уполномоченного в сфере использования ЭП.

Процедура плановой смены ключей УЦ осуществляется в следующем порядке:

1) УЦ создает новый ключ ЭП и соответствующий ему ключ проверки ЭП;
2) УЦ направляет во ФГИС ГУЦ запрос на выдачу подчиненного сертификата аккредитованного удостоверяющего центра.
3) ФГИС ГУЦ изготавливает новый СКПЭП Уполномоченного лица УЦ и передает УЦ.
4) УЦ устанавливает в контейнер и формирует ключ ЭП

При плановой замене ключа ЭП УЦ все Владельцы сертификатов должны установить на своих компьютерах новый сертификат УЦ.

Информирование Заявителей/Владельцев сертификатов о проведении плановой смены ключей уполномоченного лица УЦ осуществляется посредством публикации информации на официальном сайте УЦ по адресу: http://tensor.ru/.

Доверенным способом получения нового квалифицированного сертификата УЦ является его публикация на официальном сайте УЦ по адресу: http://tensor.ru/, доступная для скачивания.

Старый ключ ЭП УЦ используется в течение своего срока действия для формирования списков аннулированных сертификатов, изданных УЦ в период действия старого ключа ЭП УЦ.

5.1.3. Порядок осуществления смены ключей ЭП УЦ в случаях нарушения их конфиденциальности.

Внеплановая смена ключей выполняется в следующих случаях:

1) ключ ЭП УЦ закончил свой срок действия, а плановая смена произведена не была;
2) произошла компрометация ключа ЭП УЦ;
3) есть подозрение, что ключ ЭП УЦ мог быть скомпрометирован;
4) ключ ЭП УЦ не доступен (ключевой носитель поврежден, уничтожен и т.д.);

5) в связи с необходимостью внести изменение в содержимое СКПЭП УЦ (введение новых Требований к форме или формату сертификата и т.д.);

6) по решению суда, вступившему в законную силу, по решению учредителя (учредителей) УЦ и т.д.

Смена ключа ЭП УЦ осуществляется в случае нарушения конфиденциальности ключа ЭП или угрозы нарушения конфиденциальности такого ключа ЭП.

Актуальными угрозами нарушения конфиденциальности (компрометации) ключа ЭП УЦ являются:

- угрозы несанкционированного доступа, связанные с действиями нарушителей, имеющих доступ к рабочим местам автоматизированной системы УЦ.

К случаям нарушения конфиденциальности (компрометации) ключа ЭП УЦ относятся в том числе:

а. физическая утеря/кража носителя ключа ЭП УЦ.

б. несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации или подозрение, что данные факты имели место (срабатывание сигнализации с подтверждением несанкционированного вскрытия помещения, повреждение устройств контроля несанкционированного доступа (слепков печатей), повреждение замков и т. п.)

в. иные случаи компрометации.

Процедура внеплановой смены ключей УЦ выполняется в порядке, определённом процедурой плановой смены ключей УЦ согласно п. 5.1.2.

Смена ключей ЭП УЦ в случаях нарушения их конфиденциальности осуществляется в срок, не превышающий 7 (семь) рабочих дней.

В случае компрометации ключа ЭП УЦ СКПЭП УЦ прекращает свое действие, Владельцы сертификатов уведомляются об указанном факте путем публикации информации о компрометации на сайте УЦ по адресу: http://tensor.ru/.

Все сертификаты, созданные с использованием скомпрометированного ключа ЭП УЦ, считаются прекратившими свое действие с занесением соответствующих сведений об этих квалифицированных сертификатах в реестр квалифицированных сертификатов.

Доверенным способом получения нового квалифицированного сертификата УЦ является его публикация на официальном сайте УЦ по адресу: http://tensor.ru/, доступная для скачивания и исключающая уничтожение, модифицирование, блокирование при передаче и иные неправомерные действия с квалифицированным сертификатом.

5.1.4. Порядок осуществления УЦ смены ключа ЭП Владельца квалифицированного сертификата.

5.1.4.1. Смена ключа ЭП Владельца сертификата осуществляется в случаях, указанных в пунктах 1, 2, 4 части 6 и части 6.1 статьи 14 Федерального закона «Об электронной подписи»:

1) истечения установленного срока действия СКПЭП;

2) на основании заявления Владельца сертификата о его аннулировании, подаваемого в форме документа на бумажном носителе или в форме электронного документа, и последующей подачей заявления на изготовление квалифицированного СКПЭП;

3) если не подтверждено, что Владелец сертификата владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в таком сертификате;

4) если установлено, что содержащийся в таком сертификате ключ проверки ЭП уже содержится в ином ранее созданном СКПЭП;

5) если вступило в силу решение суда, которым, в частности, установлено, что СКПЭП содержит недостоверную информацию;

6) иных случаях, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между УЦ и Владельцем сертификата.

5.1.4.2. При смене сертификата Владелец сертификата подает заявление на изготовление квалифицированного СКПЭП в соответствии с требованиями к заявлению, указанными в п. 5.2.2. настоящего Регламента.

5.1.4.3. Заявление на смену ключа ЭП владельца квалифицированного сертификата может быть создано в форме электронного документа, подписанного усиленной квалифицированной ЭП владельца квалифицированного сертификата, при этом в случае, если смена ключа ЭП владельца квалифицированного сертификата связана с нарушением его конфиденциальности или угрозой нарушения конфиденциальности, соответствующее заявление должно быть подписано иной усиленной квалифицированной ЭП владельца квалифицированного сертификата.

5.1.4.3. При смене ключа ЭП Владельца сертификата заявление на изготовление СКПЭП может быть создано в форме электронного документа, подписанного усиленной КЭП Владельца сертификата. При этом, в случае, если смена ключа ЭП Владельца сертификата связана с нарушением его конфиденциальности или угрозой нарушения конфиденциальности, такое заявление должно быть подписано иной усиленной КЭП Владельца сертификата.

5.1.4.4. Процедура выдачи квалифицированного сертификата и ключа ЭП (при необходимости) Владельцу сертификата.

При выдаче квалифицированного сертификата УЦ:

1) в порядке, установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», идентифицирует заявителя - физическое лицо, обратившееся за получением квалифицированного сертификата;

2) предлагает использовать шифровальные (криптографические) средства, указанные в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», физическим лицам, обратившимся в УЦ 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»), и указывает страницу сайта в информационно-телекоммуникационной сети «Интернет», с которой безвозмездно предоставляются эти средства.

3) отказывает физическому лицу в проведении идентификации и выдаче СКПЭП, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения его идентификации в УЦ без его личного присутствия посредством информационно-телекоммуникационной сети «Интернет» при выдаче СКПЭП отказывается от использования шифровальных (криптографических) средств;

4) с использованием инфраструктуры осуществляет проверку достоверности документов и сведений, представленных заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

5) отказывает в создании СКПЭП, в случае:

- если не было подтверждено то, что заявитель владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному заявителем для получения СКПЭП;

- отрицательного результата проверки в реестре сертификатов уникальности ключа проверки ЭП, указанного заявителем для получения СКПЭП;

- отрицательного результата проверки с использованием инфраструктуры достоверности документов и сведений, предоставленных заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

6) создает СКПЭП, в случае положительного результата проверки с использованием инфраструктуры достоверности документов и сведений, предоставленных заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и идентификации заявителя;

7) ознакамливает с информацией, содержащейся в СКПЭП. Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования заявителем КЭП при наличии у него действующего квалифицированного сертификата;

8) предоставляет Владельцу сертификата руководство по обеспечению безопасности использования КЭП и средств ЭП, об условиях и о порядке использования ЭП и средств ЭП (СКЗИ), о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП - Правила использования СКЗИ и ЭП;

9) направляет в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате;

10) по желанию лица, которому выдан квалифицированный сертификат безвозмездно осуществляет регистрацию в единой системе идентификации и аутентификации с проведением идентификации владельца при его личном присутствии.

5.2. Процедура создания и выдачи квалифицированных СКПЭП.

5.2.1. Порядок подачи заявления на создание и выдачу квалифицированных сертификатов.

5.2.1.1. Заявитель обращается с заявлением на изготовление СКПЭП в Регистрационный центр. В Регистрационном центре принимаются представленные Заявителем документы, вручаются готовые СКПЭП от имени УЦ. Заявитель может заранее предоставить в УЦ электронные копии документов при условии последующего их сличения с оригиналами в Регистрационном центре.

5.2.1.2. УЦ в СКПЭП вносится информация на основании заявления.

5.2.1.3. УЦ проверяет данные в Заявлении на изготовление СКПЭП на соответствие данным, содержащимся в иных представленных Заявителем документах, и устанавливает:

1) факт принадлежности документов предоставившему их лицу;

2) факт соответствия сведений, указанных в заявлении, представленным документам и, в необходимых случаях в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», информации, полученной с использованием инфраструктуры;

3) факт отсутствия признаков подделки документов.

5.2.1.4. В случае внесения в Сертификат персональных данных физического лица, Заявитель - физическое лицо предоставляет свое согласие на обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Текст согласия включен в заявление на изготовление квалифицированного СКПЭП. Согласие должно быть подписано лицом, данные о котором вносятся в Сертификат (субъектом персональных данных).

5.2.2.Требования к заявлению на создание и выдачу квалифицированных сертификатов.

В качестве заявления на создание и выдачу квалифицированного сертификата в УЦ разработан шаблонная форма: «Заявление на изготовление сертификата ключа проверки электронной подписи». Заявление может быть оформлено как на бумажном носителе, подписанное Заявителем собственноручно, так и в форме электронного документа, подписанное КЭП. Собственноручное подписание Заявления на бумажном носителе производится чернилами (пастой) синего или черного цвета. Использование факсимиле (клише подписи) на заявлении не допускается.

Форма заявления предоставляется Заявителю в электронном виде. Актуальную форму заявления УЦ определяет самостоятельно и по своей инициативе вправе вносить в нее любые изменения без уведомления участников электронного взаимодействия.

Форма заявления на изготовление СКПЭП включает следующие сведения.

Для Владельца сертификата - физического лица:

1) ФИО;

2) паспортные данные - серия, номер паспорта, дата выдачи, код подразделения, дата рождения, кем выдан, пол;

3) СНИЛС;

4) ИНН;

5) адрес электронной почты;

6) область/регион.

5.2.3.Порядок идентификации Заявителя:

5.2.3.1. Идентификация гражданина Российской Федерации осуществляется:

а. При его личном присутствии по основному документу, удостоверяющему личность**;**

б. Без его личного присутствия:

- с использованием усиленной КЭП при наличии действующего квалифицированного сертификата;

• путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

5.2.3.2. Идентификация гражданина иностранного государства осуществляется по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства.

5.2.3.3. Идентификация беженца, вынужденного переселенца и лица без гражданства осуществляется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.

При идентификации заявителя устанавливаются 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.

5.2.3.4. Подтверждение достоверности сведений, перечисленных в п. 1 и 2 ч. 1 ст. 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» 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, Фонда пенсионного и социального страхования Российской Федерации, Федерального фонда обязательного медицинского страхования, единой информационной системы нотариата;

3) с использованием единой системы идентификации и аутентификации.

5.2.3.5. Заявитель при обращении в УЦ (Регистрационный центр) предоставляет следующие документы либо их надлежащим образом заверенные копии и (или) сведения из них:

1) основной документ, удостоверяющий личность;

2) страховой номер индивидуального лицевого счета заявителя - физического лица;

3) идентификационный номер налогоплательщика заявителя - физического лица.

5.2.3.6.Личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность - паспорту гражданина Российской Федерации.

5.2.3.7. Личность гражданина иностранного государства и лица без гражданства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства и лица без гражданства.

Документы, удостоверяющие личность иностранных граждан на территории РФ:

а. паспорт иностранного гражданина или иной документ, установленный федеральным законом или признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность иностранного гражданина – для иностранных граждан, если они постоянно проживают на территории РФ;

б. документ, выданный иностранным государством и признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность лица без гражданства;

в. временное удостоверение личности лица без гражданства в РФ;

г.иной документ, установленный федеральным законом или признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность иностранного гражданина или лица без гражданства;

д. разрешение на временное проживание является документом, удостоверяющим личность иностранного гражданина или лица без гражданства (оформленное в виде документа установленной формы, выдаваемого в РФ лицу без гражданства, не имеющему документа, удостоверяющего личность). Данный документ подтверждает право иностранного гражданина или лица без гражданства временно проживать в Российской Федерации до получения вида на жительство;

е. вид на жительство в РФ является документом, удостоверяющим личность лица без гражданства, подтверждающим его право на постоянное проживание в РФ;

ж. удостоверение беженца или свидетельство о рассмотрении ходатайства о признании беженцем на территории РФ является документом, удостоверяющим личность лица (иностранного гражданина или лица без гражданства), ходатайствующего о признании беженцем (статьи 4, 7 Федерального закона от 19.02.1993 № 4528-1 «О беженцах»).

Все документы на иностранном языке должны быть апостилированы в консульстве (посольстве) РФ за границей (на территории того государства, где эти документы выданы), либо в консульстве (посольстве) иностранного государства (выдавшего документы, удостоверяющие личность) на территории РФ и иметь заверенный перевод на русский язык.

5.2.3.8. Личность беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.

5.2.3.9. При получении ЭП Заявитель должен предоставить оригинал документа, удостоверяющего личность.

5.2.3.10.Требования к документу, удостоверяющему личность:

1) документ не должен быть просрочен;
2) документ не должен быть поврежден или испорчен;
3) документ не может содержать неточности и орфографические ошибки.

5.2.3.11. Обязательным критерием идентификации при личном присутствии заявителя – физического лица, при наличии не менее чем в трех четвертях субъектов Российской Федерации одного или более филиала или представительства УЦ, наряду с удостоверяющим личность документом, является фото Заявителя. С целью исключения противоправных мошеннических действий с СКПЭП, исполнения Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (при выдаче квалифицированного сертификата УЦ обязан идентифицировать заявителя - физическое лицо, обратившегося к нему за получением квалифицированного сертификата (п. 1 ч. 1 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»), для подтверждения осуществления определенных действий, а именно получение квалифицированного СКПЭП конкретным лицом, при выдаче СКПЭП УЦ (Регистрационный центр) ведет фотофиксацию Заявителя - физического лица:

При выдаче СКПЭП Заявителю – физическому лицу УЦ берет согласие с Заявителя на обработку его персональных данных. Заявитель вправе собственноручно написать отказ от фотофиксации: *“Отказываюсь от фотофиксации. Число. ФИО. Подпись”.*

5.2.4. Перечень документов, запрашиваемых УЦ у Заявителя для изготовления и выдачи квалифицированного сертификата, в том числе для удостоверения личности заявителя.

Заявитель, присоединяясь к настоящему Регламенту, предоставляет в УЦ следующие документы либо их надлежащим образом заверенные копии и (или) сведения из них:

1) заявление на изготовление СКПЭП, содержащее в том числе фамилию, имя отчество (если имеется) владельца сертификата;
2) основной документ, удостоверяющий личность Владельца сертификата;
3) страховой номер индивидуального лицевого счета заявителя - физического лица (Заявитель вправе по собственной инициативе представить копии документов, содержащих данные сведения);
4) идентификационный номер налогоплательщика заявителя (Заявитель вправе по собственной инициативе представить копии документов, содержащих данные сведения);

В случае если для подтверждения сведений, вносимых в квалифицированный сертификат, законодательством Российской Федерации установлена определенная форма документа, заявитель представляет в УЦ документ соответствующей формы.

5.2.5. Порядок проверки достоверности документов и сведений, представленных заявителем

5.2.5.1. Для заполнения квалифицированного сертификата в соответствии с частью 2 статьи 17 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» УЦ осуществляет с использованием инфраструктуры проверку достоверности документов и сведений, представленных заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

5.2.5.2. В случае, если УЦ идентифицировал заявителя - физическое лицо, УЦ осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата.

В ином случае УЦ отказывает Заявителю в выдаче квалифицированного сертификата.

5.2.6. Порядок создания квалифицированного сертификата.

5.2.6.1. Регистрация Заявителя и изготовление сертификата.

Под регистрацией Заявителей понимается внесение регистрационной информации о Заявителях в Реестр УЦ.

Процедура регистрации Заявителя применяется в отношении лиц, обращающихся к услугам УЦ в части изготовления СКПЭП Заявителей и/или формирования ключей ЭП и ключей проверки ЭП Заявителей с записью их на ключевой носитель.

5.2.6.2. Процедура создания ключей ЭП и выпуска СКПЭП:

1) Процедура изготовления ЭП в лицензированном Регистрационном центре:

а. получение от Владельца сертификата заявления на изготовление СКПЭП;

б. проверка сведений, указанных в заявлении на изготовление СКПЭП и представленных документов;

в. в случае подтверждения достоверности сведений проводится проверка будущего носителя ключа типа Token, допустимого эксплуатационной документацией к СКЗИ, на вирусы, при необходимости производится инициализация и создание ключа ЭП;

г. формирование запроса на СКПЭП;

д. предоставление запроса на сертификат в УЦ для выпуска СКПЭП;

е. проверка сведений в запросе;

ж. выпуск СКПЭП в УЦ;

з. размещение сертификата на token;

и. внесение данных о выпущенных СКПЭП и ключевых носителях в журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

к. осуществление конвертования носителя с ключевой парой;

л. передача Владельцу сертификата носителя типа Token с ключевой парой под подпись в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

м. ознакомление Владельца сертификата со сведениями, содержащимися в сертификате.

2) Процедура создания клиентом самостоятельно:

а. получение от Владельца сертификата заявления на изготовление СКПЭП;

б. проверка сведений, указанных в заявлении на изготовление СКПЭП и представленных документов;

в. в случае подтверждения достоверности сведений Владельцу сертификата рекомендуется приступить к созданию ключа ЭП и запроса на сертификат на его персональном компьютере с использованием сертифицированных ФСБ России средств СКЗИ.

г. предоставление запроса на сертификат в УЦ для выпуска СКПЭП;

д. проверка сведений в запросе;

е. выпуск СКПЭП в УЦ;

ж. ознакомление Владельца сертификата со сведениями, содержащимися в СКПЭП;

з. передача Владельцу сертификата;

и. размещение сертификата Владельцем сертификата на носитель.

5.2.7. Порядок выдачи квалифицированного сертификата.

5.2.7.1. При личной идентификации владельца квалифицированного сертификата:

1) Работник Регистрационного центра приглашает Владельца сертификата для вручения СКПЭП в офис.

2) Работник Регистрационного центра выполняет процедуру идентификации лица, проходящего процедуру регистрации, путем установления личности по основному документу, удостоверяющему личность, и проверке подлинности документов.

3) Документы на электронных и бумажных носителях выдаются Заявителю с соблюдением требований по обеспечению конфиденциальности.

4) При получении квалифицированного сертификата Заявитель знакомится 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. Заявителю выдается лист ознакомления с данными СКПЭП (в 2 экземплярах), на котором он ставит свою подпись, а работник Регистрационного центра собственноручной подписью подтверждает факт ознакомления Заявителя с информацией, содержащейся в сертификате. Один экземпляр листа ознакомления передается заявителю, второй экземпляр передается в УЦ.

5) По запросу владельца сертификата УЦ может выдать бланк сертификата на бумажном носителе, подписанный Уполномоченным лицом УЦ.

6) УЦ одновременно с выдачей СКПЭП предоставляет руководство по обеспечению безопасности использования КЭП и средств ЭП, об условиях и о порядке использования ЭП и средств ЭП (СКЗИ), о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП - Правила использования СКЗИ и ЭП.

7) При выдаче квалифицированного сертификата Заявитель получает:

- ключ ЭП и СКПЭП;
- лист ознакомления, подписанный собственноручной подписью владельца сертификата и собственноручной подписью работника Регистрационного центра.

5.2.7.2. При идентификации владельца квалифицированного сертификата без его личного присутствия с использованием квалифицированной ЭП владельца сертификата при наличии действующего квалифицированного сертификата, ранее выданного УЦ:

1) Формирование ключа ЭП и СКПЭП владельца сертификата осуществляется на основании Заявления на изготовление квалифицированного СКПЭП, запроса на сертификат, подписанных усиленной КЭП с использованием ключа ЭП и СКПЭП владельца сертификата. Для подписания заявления на изготовление СКПЭП и запроса на сертификат должен использоваться СКПЭП ранее выданный УЦ, срок действия которого не истек на момент подписания.

2) УЦ с использованием инфраструктуры осуществляет проверку достоверности сведений, представленных заявителем в соответствии с частями 2 и 2.1 ст. 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3) При получении положительных результатов проверки данных в запросе на сертификат УЦ выпускает новый СКПЭП, направляет лист ознакомления по защищенным каналам связи.

4) Заявитель проверяет данные в выпущенном сертификате, если все данные внесены верно, то подписывает лист ознакомления с информацией, содержащейся в квалифицированном СКПЭП действующей на момент подписания усиленной квалифицированной ЭП, ранее выданной УЦ, с использованием ключа ЭП и СКПЭП, владельцем которых является Заявитель и направляет подписанный документ в УЦ, тем самым подтверждая свое согласие с данными внесенными в сертификат и обеспечивая неотрекаемость от сертификата.

5) УЦ направляет Заявителю СКПЭП.

6) По запросу владельца сертификата УЦ может выдать бланк сертификата на бумажном носителе, подписанный Уполномоченным лицом УЦ.

7) При выдаче квалифицированного сертификата Заявитель получает:

- ключ ЭП и СКПЭП.

5.2.7.3.При идентификации владельца квалифицированного сертификата без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»:

1) Заявление на изготовление СКПЭП подается через личный кабинет УЦ, который интегрирован с единой системой идентификации и аутентификации и единой биометрической системой.

2) Специалист УЦ с использованием инфраструктуры осуществляет проверку достоверности сведений, представленных заявителем в соответствии с частями 2 и 2.1 ст. 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», при положительной проверке представленной в Заявлении информации Специалист УЦ через информационную систему направляет запрос на аутентификацию Заявителя в ЕСИА, при положительной авторизации Заявителя, запрашивается маркер идентификации по биометрическим данным, на основании которого при положительных результатах идентификации Заявителя и проверки сведений, представленных Заявителем, специалист УЦ заверяет (подписывает) запрос на сертификат своим действующим квалифицированным ключом ЭП, выпускает новый СКПЭП, направляет лист ознакомления по защищенным каналам связи.

3) Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования заявителем квалифицированной ЭП при наличии у него действующего квалифицированного сертификата либо посредством простой ЭП заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой ЭП 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 ЭП, в том числе простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного физического лица. УЦ обязан хранить информацию, подтверждающую ознакомление заявителя с информацией, содержащейся в квалифицированном сертификате, в течение всего срока осуществления своей деятельности.

4) УЦ направляет Заявителю СКПЭП.

5) По запросу владельца сертификата УЦ может выдать бланк сертификата на бумажном носителе, подписанный Уполномоченным лицом УЦ.

6) При выдаче квалифицированного сертификата Заявитель получает:

- ключ ЭП и СКПЭП.

5.2.8. Срок создания и выдачи квалифицированного сертификата с момента получения Удостоверяющим центром соответствующего заявления, а также условия для срочного создания и выдачи квалифицированного сертификата заявителю.

Создание Сертификата производится в срок не более пяти рабочих дней с момента подачи заявления, при условии подтверждения всех фактов соответствия сведений в заявлении и соблюдения порядка оплаты за услуги.

Возможно создание сертификата в течение двадцати минут с момента подачи заявления, при условии подтверждения всех фактов соответствия сведений в заявлении на изготовление СКПЭП, предоставлении полного пакета запрашиваемых документов, осуществления полной предоплаты за услуги срочного изготовления.

5.3. Подтверждение действительности ЭП, использованной для подписания электронных документов.

5.3.1. Требования к заявлению на подтверждение действительности ЭП, в том числе перечень прилагаемых к такому заявлению документов.

Подтверждение подлинности ЭП УЦ осуществляется на основании заявления Заявителя в свободной форме.

5.3.2. К заявлению прикладывается электронный документ, подписанный КЭП, а также СКПЭП, подтверждение подлинности ЭП которого производится.

5.3.3. Срок предоставления услуги по подтверждению действительности ЭП в электронном документе.

Срок проведения экспертизы составляет 30 (тридцать) рабочих дней с момента поступления заявления в УЦ и при условии поступления оплаты данной услуги на расчетный счет УЦ.

5.3.4. Порядок оказания услуги.

При проведении работ УЦ может быть запрошена дополнительная информация.

Процедура подтверждения действительности ЭП осуществляется с использованием специализированного программного обеспечения, входящего в состав сертифицированного средства УЦ, комиссией, состоящей из уполномоченных лиц УЦ. По согласованию сторон в комиссию могут входить представители заявителя или уполномоченные сотрудники правоохранительных органов. В ходе процедуры подтверждения действительности ЭП комиссией осуществляется проверка всех квалифицированных СКПЭП, на основании которых были сформированы ЭП на документах, определение даты формирования каждой ЭП в документах, проверку каждого квалифицированного СКПЭП в цепочке до квалифицированного СКПЭП Головного УЦ, проверку действительности всех квалифицированных СКПЭП на момент проверки и отсутствие их в CRL. Результатом работы комиссии является протокол проверки ЭП в электронном документе, в общем случае включающий в себя:

а. результат проверки квалифицированного СКПЭП или нескольких квалифицированных СКПЭП, необходимых для проверки ЭП;

б. проверка ЭП электронного документа с использованием одного или нескольких квалифицированных СКПЭП;

в. проверка действительности каждого квалифицированного СКПЭП в цепочке до квалифицированного СКПЭП Головного УЦ.

5.4. Процедуры, осуществляемые при прекращении действия и аннулировании квалифицированного сертификата.

5.4.1. Основания прекращения действия квалифицированного сертификата.

Квалифицированный сертификат прекращает свое действие в случаях, установленных статьей 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»:

1) Истечение установленного срока его действия.

2) По заявлению Владельца сертификата, подаваемому в форме документа на бумажном носителе или в форме электронного документа, при:

- смене/увольнении сотрудника юридического лица, если СКПЭП был выдан в целях выполнения сотрудником юридического лица своих должностных обязанностей по заявлению владельца физического лица – сотрудника организации или владельца юридического лица-работодателя;
- смене реквизитов Владельца сертификата;
- поломке ключевого носителя;
- утере, краже и иной компрометации ключа;
- ошибки в реквизитах;
- иные случаи.

3) В случае прекращения деятельности УЦ без перехода его функций другим лицам.

4) иных случаях, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между УЦ и Владельцем сертификата.

5.4.2. УЦ признает квалифицированный сертификат аннулированным, если:

1) не подтверждено, что Владелец сертификата владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в таком сертификате;

2) установлено, что содержащийся в таком сертификате ключ проверки ЭП уже содержится в ином ранее созданном СКПЭП;

3) вступило в силу решения суда, которым, в частности, установлено, что СКПЭП содержит недостоверную информацию.

5.4.3. Порядок действий УЦ при прекращении действия (аннулировании) квалифицированного сертификата.

Заявление на прекращение сертификата может подаваться в УЦ в бумажной форме при личном прибытии Владельца сертификата в УЦ либо почтовой или курьерской службой, а также в форме электронного документа, подписанного усиленной КЭП владельца сертификата, в том числе с использованием федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)».

Подтверждения полномочий Владельца сертификата осуществляется на основании предоставляемых Заявителем документов.

Заявление о прекращении действия квалифицированного СКПЭП должно содержать:

- фамилию, имя, отчество (если имеется) владельца квалифицированного сертификата;
- страховой номер индивидуального лицевого счета и идентификационный номер налогоплательщика владельца квалифицированного сертификата - для физического лица;
- серийный номер квалифицированного СКПЭП;
- даты начала и окончания действия квалифицированного СКПЭП;
- причины прекращения действия квалифицированного сертификата;
- наименование аккредитованного удостоверяющего центра, выдавшего квалифицированный СКПЭП.

В случае направления заявителем заявления о прекращении действия квалифициованного сертификата с использованием федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» принятое по заявлению решение удостоверяющего центра в форме электронного документа, подписанного усиленной КЭП УЦ направляется в указанную государственную информационную систему для размещения решения после проведения проверки действительности усиленной КЭП УЦ, которой решение подписано, и подтверждения ее действительности в личном кабинете заявителя. В случае принятия положительного решения по заявлению УЦ направляет информацию в федеральную государственную информационную систему «Единый портал государственных и муниципальных услуг (функций)» о прекращении действия квалифицированного сертификата после внесения соответствующей информации в реестр квалифицированных сертификатов. Направление указанных решений и информации осуществляется посредством единой системы межведомственного электронного взаимодействия».

5.4.4. Порядок внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов.

Срок внесения информации о прекращении действия или аннулировании квалифицированного сертификата в Реестр сертификатов не может превышать двенадцать часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие СКПЭП прекращается с момента внесения записи об этом в реестр сертификатов.

5.5. Порядок ведения реестра квалифицированных сертификатов.

5.5.1. Формы ведения реестра квалифицированных сертификатов.

5.5.1.1. Реестр СКПЭП ведётся в электронной форме.

Ведение реестра квалифицированных сертификатов включает в себя:

- внесение изменений в реестр квалифицированных сертификатов в случае изменения сведений;
- внесение в реестр квалифицированных сертификатов сведений о прекращении действия или об аннулировании квалифицированных сертификатов.

5.5.1.2. Информация, внесенная в реестр квалифицированных сертификатов, подлежит хранению в течение всего срока деятельности аккредитованного УЦ, если более короткий срок не установлен законодательством Российской Федерации.

5.5.1.3. Хранение информации, содержащейся в реестре квалифицированных сертификатов, должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

5.5.1.4. Аккредитованный УЦ обеспечивает актуальность информации, содержащейся в реестре квалифицированных сертификатов.

5.5.1.5. Аккредитованный УЦ обеспечивает защиту информации, содержащейся в реестре квалифицированных сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

5.5.1.6. Формирование и ведение реестра квалифицированных сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему.

5.5.1.7. Для предотвращения утраты сведений о квалифицированных сертификатах, содержащихся в реестре, формируется его резервная копия.

5.5.2. Сроки внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов.

Информация о прекращении действия или аннулировании квалифицированного сертификата вносится УЦ в реестр квалифицированных сертификатов в течение двенадцати часов с момента наступления обстоятельств, повлекших за собой прекращение действия квалифицированного сертификата или в течение двенадцати часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие квалифицированного сертификата прекращается с момента внесения записи об этом в реестр квалифицированных сертификатов.

5.6. Порядок технического обслуживания реестра квалифицированных сертификатов.

5.6.1. Максимальные сроки проведения технического обслуживания.

Плановое техническое обслуживание Реестра сертификатов осуществляется не чаще одного раза в месяц и не может превышать 12 (двенадцати) часов.

Внеплановое техническое обслуживание Реестра сертификатов осуществляется в случае необходимости и невозможности дождаться срока наступления планового обслуживания, не может превышать 12 (двенадцати) часов.

5.6.2. Порядок уведомления участников информационного взаимодействия о проведении технического обслуживания.

УЦ оповещает лиц, использующих Реестр сертификатов, о проведении планового или внепланового технического обслуживания Реестра сертификатов на официальном сайте УЦ.

6. Порядок исполнения обязанностей УЦ

6.1. Информирование заявителей об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки.

Данная обязанность реализуется посредством предоставления Владельцу сертификата, одновременно с самой подписью, Правил использования СКЗИ и ЭП, сущность которых сводится к определению обязанностей Владельца сертификата, в том числе по обеспечению режима конфиденциальности информации.

6.2. Выдача по обращению заявителя средств ЭП.

6.2.1. УЦ по обращению заявителя выдает средства ЭП, отвечающие требованиям:

1) средства ЭП позволяют установить факт изменения подписанного электронного документа после момента его подписания;

2) средства ЭП обеспечивают практическую невозможность вычисления ключа ЭП из ЭП или из ключа ее проверки;

3) средства ЭП позволяют создать ЭП в формате, устанавливаемом федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, и обеспечивающем возможность ее проверки всеми средствами ЭП.

6.2.2. При создании ЭП средства ЭП должны (не относится к средствам ЭП, используемым для автоматического создания ЭП):

1) показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписываемой с

использованием указанных средств, лицу, осуществляющему создание ЭП, содержание информации, подписание которой производится;

2) создавать ЭП только после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭП;

3) однозначно показывать, что ЭП создана.

6.2.3. При проверке ЭП средства ЭП должны (не относится к средствам ЭП, используемым для автоматической проверки ЭП):

1) показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписанной с использованием указанных средств, содержание электронного документа, подписанного ЭП, включая визуализацию данной ЭП, содержащую информацию о том, что такой документ подписан ЭП, а также о номере, Владельце сертификата и периоде действия СКПЭП;

2) показывать информацию о внесении изменений в подписанный ЭП электронный документ;

3) указывать на лицо, с использованием ключа ЭП которого подписаны электронные документы.

6.2.4. Средства ЭП, предназначенные для создания ЭП в электронных документах, содержащих информацию ограниченного доступа (в том числе персональные данные), не должны нарушать конфиденциальность такой информации.

6.2.5. Средство ЭП должно противостоять угрозам, представляющим собой целенаправленные действия с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемой средством ЭП информации или с целью создания условий для этого.

6.2.6. Средство ЭП должно проводить аутентификацию субъектов доступа (лиц, процессов) к этому средству, при этом:

1) при осуществлении доступа к средству ЭП аутентификация субъекта доступа должна проводиться до начала выполнения первого функционального модуля средства ЭП;

2) механизмы аутентификации должны блокировать доступ этих субъектов к функциям средства ЭП при отрицательном результате аутентификации.

6.2.7. Средство ЭП должно проводить аутентификацию лиц, осуществляющих локальный доступ к средству ЭП.

6.2.8. Средства ЭП должны обеспечивать возможность проверки всех усиленных КЭП в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной КЭП, или в случае, если электронный документ подписан несколькими усиленными КЭП.

6.2.9. Средства ЭП аккредитованного УЦ и средства ЭП Заявителя/Владельца ЭП должны соответствовать требованиям Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и требованиям Приказа ФСБ РФ от 27.12.2011 г. № 796.

6.3. Обеспечение актуальности информации, содержащейся в реестре сертификатов и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий.

УЦ обеспечивает актуальность информации, содержащейся в реестре квалифицированных сертификатов, защиту информации от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий. Актуальность обеспечивается путем своевременного внесения записи о выпуске и аннулировании СКПЭП в реестр квалифицированных сертификатов. Режим защиты является общим требованием в отношении всей сферы применения ЭП, он обеспечивается посредством применения специальных шифровальных средств, способствующих защите информации от несанкционированного проникновения.

6.4. Обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети «Интернет» в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов.

Аккредитованный УЦ обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» по адресу https://tensor.ru/uc/check, к реестру квалифицированных сертификатов УЦ в любое время в течение срока деятельности УЦ, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

6.5. Порядок обеспечения конфиденциальности созданных УЦ ключей ЭП.

6.5.1. Требования к обеспечению конфиденциальности.

Необходимо немедленно обратиться в УЦ с заявлением на прекращение действия квалифицированного сертификата в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа ЭП.

Запрещается:

1) оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, средства усиленной КЭП, после ввода ключевой информации;

2) вносить какие-либо изменения в ПО СКЗИ;

3) осуществлять несанкционированное копирование ключевых носителей;

4) разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным;

5) использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;

6) записывать на ключевые носители постороннюю информацию;

7) использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ;

8) защищать ключи ЭП на ключевом носителе паролем (пин-кодом);

9) оставлять без присмотра ключи ЭП на ключевом носителе (на столе, подключенным к ПЭВМ и пр.)

10) применять ключ КЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

6.5.2. Условия временного хранения ключей ЭП.

1) при хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Владелец сертификата несет персональную ответственность за хранение личных ключевых носителей;

2) запрещается оставлять без контроля вычислительные средства с установленным СКЗИ после ввода ключевой информации;

3) в случае централизованного хранения ключевых носителей в организации, эксплуатирующей СКЗИ, администратор безопасности (если он имеется) несет персональную ответственность за хранение личных ключевых носителей пользователей.

6.5.3.Сроки уничтожения ключей ЭП.

Ключи на ключевых носителях (включая Touch Memory и смарт-карты), в том числе срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации. Срок уничтожения Владелец сертификата устанавливает самостоятельно.

6.6. Осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации.

При выдаче квалифицированного сертификата аккредитованный УЦ направляет в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате.

6.7. Осуществление по желанию лица, которому выдан квалифицированный сертификат, безвозмездной регистрации указанного лица в единой системе идентификации и аутентификации.

При выдаче квалифицированного сертификата аккредитованный УЦ по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществляет регистрацию указанного лица в единой системе идентификации и аутентификации.

6.8. Предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, в том числе путем публикации перечня прекративших свое действие (аннулированных) квалифицированных сертификатов.

Информация, содержащаяся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, предоставляется безвозмездно. Обращение подается при личном прибытии Владельца сертификата в УЦ (Регистрационный центр) в соответствии с графиком работы УЦ и его обособленных подразделений по созданию и выдаче СКПЭП УЦ, либо почтовой или курьерской службой, или круглосуточно через форму на сайте УЦ https://tensor.ru/yaroslavl/uc (по выбору лица, обратившегося за получением информации из реестра квалифицированных сертификатов), за исключением периодов планового или внепланового технического обслуживания реестра сертификатов.

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).

Выписка из Реестра позволяет определить действительность СКПЭП Владельцев сертификатов. Доступ к информации организован в соответствии с защитой персональных данных согласно требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и предоставляется при условии владения необходимыми данными из сертификата.

Для получения информации необходимо предоставить:

- серийный номер сертификата;

или

- ИНН Заявителя;
- СНИЛС Владельца сертификата;
- даты начала и окончания действия квалифицированного сертификата.

Также УЦ публикует **перечень прекративших свое действие (аннулированных) квалифицированных сертификатов**, позволяющий определить действительность СКПЭП Владельцев сертификатов на официальном сайте https://tensor.ru.

Срок предоставления информации не превышает семи дней для направления информации почтовым отправлением и 24 часов для направления выписки посредством информационно-телекоммуникационных сетей.

7. Персональные данные

7.1. Обработка персональных данных Заявителей/Владельцев сертификатов:

7.1.1. Цель обработки персональных данных в УЦ – исполнение требований Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»; изготовление и хранение СКПЭП, изготовление списков аннулированных сертификатов, ведение реестра выданных и аннулированных сертификатов, подтверждение неотрекаемости от подачи заявления и запроса на сертификат, от получения СКПЭП, установление личности заявителя - физического лица, обратившегося за получением СКПЭП и подтверждения правомочия обращаться за получением СКПЭП.

7.1.2. Обработка персональных данных в УЦ осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

7.1.3. Персональные данные, обрабатываемые УЦ: фамилия, имя, отчество, реквизиты основного документа, удостоверяющего личность (серия, номер, орган его выдавший, дата выдачи, код подразделения), дата рождения, место работы, должность, телефон, СНИЛС, ИНН,

фотоизображение физического лица (владельца сертификата), которому выдан СКПЭП, адрес электронной почты и иные сведения, необходимые для исполнения целей Регламента.

7.1.4. УЦ осуществляет действия по сбору, записи, систематизации, накоплению, использованию, хранению, уточнению, обновлению, изменению, использованию, извлечению, блокированию, удалению, уничтожению, передаче персональных данных Заявителя в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

7.1.5. Обработка персональных данных Заявителей/Владельцев сертификатов осуществляется обособленными подразделениями (филиалами) ООО «Компания «Тензор» и Регистрационными центрами (на основании договора с УЦ).

7.1.6. УЦ не раскрывает третьим лицам и не распространяет персональные данные Заявителя без наличия его письменного согласия на раскрытие данной информации, за исключением случаев, прямо установленных действующим законодательством Российской Федерации.

7.1.7. Согласие на обработку персональных данных Заявителя может быть отозвано по письменному заявлению в бумажном виде при личном прибытии Заявителя, при удовлетворении которого впоследствии УЦ аннулируются все выпущенные сертификаты данного Заявителя, при этом УЦ вправе не прекращать обработку персональных данных при наличии иных правовых оснований для обработки персональных данных, установленных законодательством РФ или документами Оператора, регламентирующими вопросы обработки персональных данных.

7.1.8. Согласие вступает в силу с момента его подписания, действует до истечения срока хранения информации, установленного нормами Федерального закона от 04.06.2011 № 63-ФЗ «Об электронной подписи».

7.2. Архивное хранение информации и сведений УЦ.

На основании Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (ч. 1 ст. 15) Аккредитованный УЦ хранит следующие документы и (или) сведения:

1) заявление на изготовление сертификата ключа подписи;
2) реквизиты основного документа, удостоверяющего личность Владельца сертификата – физического лица;
3) СКПЭП;
4) лист ознакомления с данными СКПЭП.

Хранение информации осуществляется в соответствии с ч. 1 ст. 15, ч. 7 статьи 13 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»:

7.2.1. Архив ведется в электронном виде. Архив формируется из сканов документов и электронных документов. Сотрудник УЦ лично сверяет сканы документов с оригиналами документов. В целях осуществления деятельности УЦ сканы документов приравниваются к документам, имеющим юридическую значимость.

8.Ответственность

8.1. Стороны несут ответственность за соблюдение положений настоящего Регламента в соответствии с действующим законодательством РФ.

8.2. Владелец сертификата несет ответственность за достоверность документов и сведений, предоставляемых в УЦ, неисполнение обязанностей, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», настоящим Регламентом.

8.3. УЦ в соответствии с законодательством Российской Федерации несет ответственность за вред, причиненный третьим лицам в результате:

1) неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг УЦ;

2) неисполнения или ненадлежащего исполнения обязанностей, предусмотренных Федеральным законом № 63-ФЗ «Об электронной подписи».

8.4. Аккредитованный УЦ (работник аккредитованного УЦ) несет гражданско-правовую, административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим Регламентом.

9. Список приложений.

9.1. Приложение № 1. Правила использования СКЗИ и ЭП.

Приложение № 1
к Порядку (Регламенту)
реализации функций и
исполнения обязанностей
Удостоверяющего центра
ООО «Компания «Тензор»

Правила использования средств криптографической защиты информации и электронной подписи

1.Средства электронной подписи - шифровальные (криптографические) средства (СКЗИ), используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи, имеющие подтверждение соответствия требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» СКЗИ и средства ЭП могут использоваться для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

2.Ключ электронной подписи (ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи.

3. Пользователи СКЗИ несут персональную ответственность за:

а. сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;

б. сохранение в тайне содержания ключей ЭП и СКЗИ;

в. сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями.

4. Юридическим лицом, ИП, владельцем сертификата должны быть обеспечены условия хранения ключевых носителей ключей ЭП, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

5. Владелец сертификата несет ответственность за то, чтобы на компьютере, на котором установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе, - вирусы), которые могут нарушить функционирование программных СКЗИ. При обнаружении на рабочем месте, оборудованном СКЗИ, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.

6. Организация - обладатель конфиденциальной информации обязана вести журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов в соответствии с п. 26 Приказа ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну». Неиспользованные или выведенные из действия ключевые документы подлежат уничтожению обладателем конфиденциальной информацией на месте, путем переформатирования ключевых носителей средствами ПО СКЗИ. Ключи квалифицированных электронных подписей по истечении сроков действия данных ключей подлежат незамедлительному уничтожению. Для уничтожения ключей электронных подписей должны применяться прошедшие в установленном порядке процедуру оценки соответствия средства электронной подписи, в составе которых реализована функция уничтожения информации.

7. Не допускается:

а. разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;

б. вставлять ключевой носитель в ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной подписи и т.д.), а также в другие ПЭВМ;

в. записывать на ключевом носителе постороннюю информацию;

г. вносить какие-либо изменения в СКЗИ и ключ ЭП;

д. использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей);

е. оставлять без контроля аппаратные средства, на которых эксплуатируются средства электронной подписи;

ж. оставлять без контроля носители ключевой информации;

з. сообщать PIN – код к ключевому носителю кому бы то ни было;

8. Действия в случае компрометации ключей:

а. под компрометацией ключей ЭП понимается их утрата (в том числе с их последующим обнаружением), хищение, разглашение, несанкционированное копирование, передача их по линии связи в открытом виде, увольнение по любой причине сотрудника, имеющего доступ к ключевым носителям или к ключевой информации на данных носителях, любые другие виды разглашения ключевой информации, в результате которых ключи ЭП могут стать доступными несанкционированным лицам и (или) процессам;

б. Владелец сертификата (уполномоченное лицо) самостоятельно должен определить факт компрометации ключа ЭП и оценить значение этого события для Владельца сертификата. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует и осуществляет сам Владелец сертификата;

в. при компрометации ключа ЭП, Владелец сертификата должен немедленно поставить в известность представителей Удостоверяющего центра о факте компрометации. Заявление на аннулирование сертификата может подаваться в УЦ в бумажной форме при личном прибытии Заявителя в офис удостоверяющего центра, либо почтовой или курьерской доставкой, а также в электронной форме через личный кабинет, с подписью лица, имеющего право действовать от имени организации без доверенности. Не позднее 1 часа после поступления заявления на аннулирование ключа ЭП, сертификат проверки ключа ЭП будет аннулирован. Последующая разблокировка аннулированного сертификата ключа проверки ЭП невозможна.

Для получения новых ключей уполномоченный представитель Заявителя, у которого были скомпрометированы ключи, должен обратиться в УЦ, имея при себе документы, необходимые для выпуска нового ключа ЭП. За выдачу новых ключей взимается оплата в соответствии с действующими тарифами на день оплаты.

9.PIN-код Владельца сертификата на носителе.

PIN-код для Рутокен, Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0 по умолчанию - 12345678.

PIN-код для JaCarta LT по умолчанию - 1234567890.

PIN-код для Jacarta PKI/ГОСТ и Jacarta-2 PKI/ГОСТ – 0987654321.

Владелец сертификата обязан изменить PIN-код при первом использовании ключевого носителя.

Надежный PIN-код должен состоять из смешанного набора цифровых и буквенных символов.

10.Порядок установки и эксплуатации СКЗИ допускается в четком соответствии с документацией на используемое СКЗИ: https://www.cryptopro.ru/.

11. В случае отсутствия у пользователя СКЗИ установочного модуля СКЗИ «КриптоПро CSP», последний может быть получен одним из ниже перечисленных способов:

1. Дистрибутив на носителе (за дополнительную плату).
2. Посредством загрузки через Интернет.

На странице загрузки вместе с дистрибутивом и документацией размещается отделенная электронная подпись, для проверки которой необходимо использовать утилиту cpverify, полученную доверенным образом и содержащую ключ проверки данной электронной подписи. Средство контроля целостности (cpverify.exe) первоначально должно быть получено пользователем на физическом носителе в офисе компании ООО «КРИПТО-ПРО», либо у официального дилера. Далее полученной доверенным образом признается очередная версия утилиты, полученная любым образом, например, скачанная с сайта www.cryptopro.ru.

12. Пользователи допускаются к работе с СКЗИ после соответствующего обучения.

Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники органа криптографической защиты – Лицензиата ФСБ (в соответствии с тарифами) или обладателя конфиденциальной информации.