

УТВЕРЖДЕН Приказом

от 09.12.2025 г. № 3-1-100/008813-25

ПОРЯДОК

реализации АО «Торговый дом «ПЕРЕКРЕСТОК»
функций аккредитованного удостоверяющего
центра и исполнения его обязанностей

Владелец	Начальник Управления криптографии Департамента информационной безопасности
Введен в действие	09.12.2025 г.
Срок действия	действует с даты введения в действие и до даты издания распорядительного документа, отменяющего действие
Проверка актуальности	1 раз в год



Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ	3
2. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ)	4
3. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	5
4. ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ, В ТОМ ЧИСЛЕ ТРЕБОВАНИЯ К ДОКУМЕНТАМ, ПРЕДОСТАВЛЯЕМЫМ В УДОСТОВЕРЯЮЩИЙ ЦЕНТР В РАМКАХ ПРЕДОСТАВЛЕНИЯ УСЛУГ	8
5. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА, УСТАНОВЛЕННЫХ ФЕДЕРАЛЬНЫМ ЗАКОНОМ ОТ 6 АПРЕЛЯ 2011 Г. № 63-ФЗ «ОБ ЭЛЕКТРОННОЙ ПОДПИСИ» И ПРИНИМАЕМЫМИ В СООТВЕТСТВИИ С НИМ НОРМАТИВНЫМИ ПРАВОВЫМИ АКТАМИ.....	19
6. Термины и сокращения	23
7. Связанные документы.....	24
Приложение № 1 Форма заявления на создание и выдачу квалифицированного сертификата.....	25
Приложение № 2 Форма заявления на подтверждение действительности электронной подписи	27
Приложение № 3 Форма заявления о прекращении действия квалифицированного сертификата	28
Приложение № 4 Форма заявления на смену ключа электронной подписи	29
Приложение № 5 Форма руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи	30

История изменений

Версия	Дата	Описание изменений	Разработчик
1.0	16.04.2024	Исходная версия	Литвинов Е.
2.0	07.11.2024	Актуализация	Литвинов Е.
3.0.	09.12.2025	В Порядок УЦ внесены изменения: - в соответствии с ФЗ от 21.04.2025 № 94-ФЗ «О внесении изменений в ФЗ «Об электронной подписи»; - технические правки: устранены технические ошибки, неточности и обеспечено единообразное оформление; - в части договорных отношений и условий присоединения к порядку.	Литвинов Е.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Присоединение к Порядку УЦ

1.1.1. Настоящий документ, в соответствии со статьей 435 Гражданского кодекса Российской Федерации (далее - ГК РФ), является официальным предложением (офертом) аккредитованного удостоверяющего центра АО «Торговый дом «ПЕРЕКРЕСТОК» (далее - УЦ).

1.1.2. Порядок реализации УЦ функций аккредитованного удостоверяющего центра и исполнения его обязанностей (далее – Порядок УЦ) является неотъемлемой частью договорных отношений по оказанию услуг (далее – Договор), размещенного на сайте УЦ в сети Интернет по адресу <https://cdp.x5.ru> (далее – сайт УЦ).

1.1.3. Сторонами Порядка УЦ являются УЦ, заявитель, владелец квалифицированного сертификата и доверенное лицо (далее – вместе именуемые «Стороны») присоединившиеся к настоящему Порядку УЦ.

1.1.4. Порядок УЦ распространяет свое действие на всех лиц, которые в силу Порядка УЦ, Договора или действующего законодательства обязаны соблюдать правила и выполнять все условия (требования), предусмотренные Порядком УЦ.

1.1.5. Присоединение (акцепт (безусловное принятие) условий публичной оферты) к Порядку УЦ производится в соответствии с условиями Договора.

1.1.6. Акцепт настоящей публичной оферты означает, что Сторона ознакомлена, соглашается с условиями Порядка УЦ, Договора, а также со всеми приложениями к указанным документам.

1.1.7. Сторона, присоединившееся к Порядку УЦ, принимает дальнейшие изменения (дополнения), вносимые в Порядок УЦ, в соответствии с условиями Порядка УЦ, Договора, самостоятельно отслеживает изменения (дополнения), вносимые в Порядок УЦ в виде его новой редакции путем самостоятельного ознакомления с текстом Порядка УЦ на сайте УЦ.

1.1.8. Уведомление Сторон, присоединившихся к Порядку УЦ, о внесении изменений (дополнений) в Порядок УЦ осуществляется УЦ путем размещения новой редакции Порядка УЦ на сайте УЦ.

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

1.1.10. Изменения (дополнения), вносимые УЦ в Порядок УЦ, кроме изменений (дополнений), вносимых в связи с изменениями законодательства Российской Федерации, вступают в силу и становятся обязательными для УЦ, Сторон, присоединившихся к Порядку УЦ, с даты их публикации на сайте УЦ.

1.1.11. Изменения (дополнения), вносимые УЦ в Порядок УЦ 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.

1.1.12. Любые изменения, вносимые в Порядок УЦ, с момента вступления в силу распространяются на все Стороны, присоединившиеся к Порядку УЦ, независимо от даты присоединения.

1.2. Предмет регулирования Порядка УЦ

1.2.1. Порядок УЦ регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок УЦ, оказании услуг УЦ, исполнении функций УЦ, при совершении иных юридически значимых действий УЦ, в том числе в случаях, установленных федеральными законами.

1.2.2. Порядок УЦ определяет услуги УЦ, правила, условия и порядок их предоставления, права и обязанности УЦ, Сторон, присоединившихся к Порядку УЦ.

1.3. Сведения об УЦ

1.3.1. Сведения о юридическом лице, осуществляющем функции УЦ:

Порядок реализации АО «Торговый дом «ПЕРЕКРЕСТОК» функций
аккредитованного удостоверяющего центра и исполнения его обязанностей
Страница 3 из 35



- полное наименование: АКЦИОНЕРНОЕ ОБЩЕСТВО «ТОРГОВЫЙ ДОМ «ПЕРЕКРЕСТОК»;
- сокращенное наименование: АО «ТОРГОВЫЙ ДОМ «ПЕРЕКРЕСТОК»;
- адрес место нахождения: г. Москва, ул. Средняя Калитниковская, д. 28, стр. 4;
- адрес для корреспонденции: 109029, г. Москва, ул. Средняя Калитниковская, д. 28, стр. 4;
- ОГРН: 1027700034493;
- ИНН: 7728029110;
- КПП 772201001.

График работы УЦ: понедельник-четверг с 09:00 до 18:00, пятница с 09:00 до 17:00. Продолжительность рабочего дня, непосредственно предшествующего нерабочему праздничному дню, уменьшается на один час. В субботу, воскресенье, а также в нерабочие праздничные дни УЦ не работает. В случае изменения графика работы информация размещается на сайте УЦ и/или по месту нахождения УЦ.

Обособленные подразделения (филиалы) УЦ: отсутствуют.

1.3.2. УЦ осуществляет свою деятельность на территории Российской Федерации на основании лицензии ФСБ России от № ЛСЗ № 0017469, размещенной на сайте УЦ.

1.4. Порядок информирования о предоставлении услуг УЦ

1.4.1. Справочный телефон УЦ: +7 (495) 662-88-88.

1.4.2. Адрес электронной почты: ic@x5.ru.

1.4.3. Адрес сайта УЦ в сети «Интернет»: <https://cdp.x5.ru> или резервный сайт <https://cdp.perekrestok.ru>.

1.4.4 Порядок получения информации заявителями по вопросам предоставления услуг УЦ.

Любые заинтересованные лица могут получить информацию по вопросам предоставления услуг УЦ следующими способами:

- ознакомиться с информацией, опубликованной на сайте УЦ;
- обратиться в УЦ за получением информации по справочному телефону;
- направить запрос на адрес электронной почты УЦ.

1.5. Стоимость услуг УЦ

1.5.1. УЦ предоставляет свои услуги на возмездной основе.

1.5.2. Оказание услуг УЦ осуществляется на основании Договора.

1.5.3. Договор на условиях публичной оферты размещен на сайте УЦ.

1.5.4. Стоимость услуг УЦ, сроки и порядок расчетов за оказанные услуги УЦ определяются условиями Договора, заключенного Сторонами.

2. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ)

2.1. УЦ оказывает услуги:

2.1.1. создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты заявителям при условии идентификации заявителя. 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 либо посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность

гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы в порядке, установленном Федеральным законом от 29.12.2022 N 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (далее - 572-ФЗ). При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия отказывается от использования шифровальных (криптографических) средств, указанных в 572-ФЗ, УЦ обязан отказать такому лицу в проведении указанной идентификации.

2.1.2. осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи;

2.1.3. устанавливает сроки действия сертификатов ключей проверки электронных подписей;

2.1.4. аннулирует выданные УЦ сертификаты ключей проверки электронных подписей;

2.1.5. выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные УЦ) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

2.1.6. ведет реестр выданных и аннулированных УЦ сертификатов ключей проверки электронных подписей, в том числе включающий в себя информацию, содержащуюся в выданных УЦ сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;

2.1.7. устанавливает порядок ведения реестра сертификатов и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети «Интернет»;

2.1.8. создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;

2.1.9. проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

2.1.10. осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

2.1.11. осуществляет иную связанную с использованием электронной подписи деятельность.

3. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

УЦ осуществляет права и обязанности, предусмотренные статьями 13 - 15, 17 и 18 ФЗ «Об электронной подписи».

3.1. Права УЦ:

3.1.1. выдавать сертификаты ключей проверки электронных подписей как в форме электронных документов, так и в форме документов на бумажном носителе;

3.1.2. на основании заключенного с УЦ соглашения наделять третьих лиц (далее - доверенное лицо) полномочиями по приему заявлений на выдачу сертификатов ключей проверки электронной подписи, а также вручению сертификатов ключей проверки электронных подписей

от имени УЦ. При совершении порученных УЦ действий доверенное лицо идентифицирует заявителя при его личном присутствии;

3.1.3. отказать заявителю в принятии заявления в случае ненадлежащего оформления им заявления на создание сертификата ключа проверки электронной подписи и/или не предоставления им всех документов, необходимых для создания сертификата ключа проверки электронной подписи;

3.1.4. отказать владельцу квалифицированного сертификата в прекращении действия сертификата ключа проверки электронной подписи в случае ненадлежащего оформления им соответствующего заявления на прекращение действия сертификата ключа проверки электронной подписи;

3.1.5. осуществлять иные права, связанные с использованием электронной подписи, в рамках деятельности УЦ.

3.2. Обязанности УЦ:

3.2.1. информировать заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

3.2.2. обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

3.2.3. 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 сертификата ключа проверки электронной подписи;

3.2.4. обеспечивать конфиденциальность созданных УЦ ключей электронных подписей;

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

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

3.2.7. незамедлительно информировать владельца квалифицированного сертификата о выявленных случаях приостановления (прекращения) технической возможности использования ключа электронной подписи, не предусмотренных соглашением Сторон, или возникновения у УЦ обоснованных сомнений в получении поручения от уполномоченного соглашением сторон лица об использовании ключа электронной подписи (при осуществлении УЦ деятельности, предусмотренной частью 2.2 статьи 15 ФЗ «Об электронной подписи»).

3.2.8. до внесения в реестр сертификатов информации об аннулировании сертификата ключа проверки электронной подписи УЦ обязан уведомить владельца квалифицированного сертификата ключа проверки электронной подписи об аннулировании его сертификата ключа проверки электронной подписи путем направления документа на бумажном носителе или электронного документа;

3.2.9. хранить следующую информацию:

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

3.2.9.2. указанную в пункте 3.2.9.1. Порядка УЦ, 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.

3.2.10. для подписания от своего имени квалифицированных сертификатов обязан использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляют уполномоченный федеральный орган. УЦ запрещается использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляют уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами.

3.2.11. 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;

3.2.12. в случае принятия решения о прекращении своей деятельности УЦ обязан:

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

3.2.12.2. передать в уполномоченный федеральный орган в установленном порядке реестр выданных УЦ квалифицированных сертификатов;

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

3.2.13. УЦ обязан выполнять Порядок УЦ, установленный УЦ в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения обязанностей, а также с ФЗ «Об электронной подписи» и иными нормативными правовыми актами, принимаемыми в соответствии с ФЗ «Об электронной подписи»;

3.2.14. при выдаче квалифицированного сертификата УЦ обязан:

3.2.14.1. в порядке, установленном 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 либо посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном 572-ФЗ. 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 572-ФЗ, 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.

3.2.14.2. предложить использовать шифровальные (криптографические) средства, указанные в 572-ФЗ, физическому лицу, обратившемуся 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.

3.2.15. одновременно с выдачей квалифицированного сертификата должен предоставить владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

4. ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ, В ТОМ ЧИСЛЕ ТРЕБОВАНИЯ К ДОКУМЕНТАМ, ПРЕДОСТАВЛЯЕМЫМ В УДОСТОВЕРЯЮЩИЙ ЦЕНТР В РАМКАХ ПРЕДОСТАВЛЕНИЯ УСЛУГ

4.1. Процедура создания ключей электронных подписей и ключей проверки электронных подписей

4.1.1. Порядок создания ключей электронных подписей и ключей проверки электронных подписей с учетом следующих способов создания

4.1.1.1. Заявитель создает ключ электронной подписи и ключ проверки электронной подписи в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (зарегистрирован Министерством юстиции Российской Федерации 3 марта 2005 г., регистрационный N 6382), с изменениями, внесенными приказом ФСБ России 12 апреля 2010 г. N 173 «О внесении изменений в некоторые нормативные правовые акты ФСБ России» (зарегистрирован Министерством юстиции Российской Федерации 25 мая 2010 г., регистрационный N 17350).

4.1.1.2. УЦ создает ключ электронной подписи и ключ проверки электронной подписи для заявителя в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

4.1.1.3. Ключ электронной подписи и ключ проверки электронной подписи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 ФЗ «Об электронной подписи» создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным

федеральным органом исполнительной власти в области обеспечения безопасности. В отношении автоматизированного рабочего места УЦ, используемого для создания ключа электронной подписи и ключа проверки электронной подписи для заявителя, должны выполняться требования, установленные постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (Собрание законодательства Российской Федерации, 2012, N 7, ст. 863; 2016, N 26, ст. 4049).

4.1.2. Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи УЦ, а также порядок информирования владельцев квалифицированных сертификатов об осуществлении такой смены с указанием доверенного способа получения нового квалифицированного сертификата УЦ

4.1.2.1. Плановая смена ключей электронной подписи УЦ

4.1.2.1.1. В процессе организации деятельности УЦ осуществляется планирование мероприятий по осуществлению его деятельности, в том числе мероприятий по смене ключей электронной подписи УЦ и мероприятий по выводу ключей электронной подписи УЦ из эксплуатации.

4.1.2.2. Основания плановой смены ключей электронной подписи УЦ

4.1.2.2.1. Основаниями для выполнения процедуры плановой смены ключа электронной подписи УЦ и процедуры его вывода из эксплуатации являются скорое истечение срока действия ключа электронной подписи УЦ для создания сертификатов и (или) списков аннулированных сертификатов.

4.1.2.2.2. Срок действия ключа электронной подписи УЦ составляет максимально допустимый срок действия, установленный в соответствии с технической и эксплуатационной документацией на средства УЦ и средства электронной подписи, с использованием которого данный ключ электронной подписи был создан.

4.1.2.2.3. Начало периода действия ключа электронной подписи УЦ исчисляется с даты и времени создания ключа электронной подписи УЦ.

4.1.2.3. Процедура плановой смены ключей электронной подписи УЦ

4.1.2.3.1. Плановая смена ключей электронной подписи УЦ осуществляется в следующем порядке:

а) уполномоченное лицо (администратор) УЦ с использованием сертифицированных по требованиям безопасности средств УЦ и средств электронной подписи создает новый ключ электронной подписи и запрос на издание сертификата. Одновременно с созданием вышеуказанных ключей производится формирование запроса на создание квалифицированного сертификата УЦ;

б) сформированный запрос на создание квалифицированного сертификата УЦ, а также иная информация, необходимая для получения квалифицированного сертификата УЦ, направляется в головной удостоверяющий центр;

в) после получения квалифицированного сертификата, созданного головным удостоверяющим центром, уполномоченное лицо (администратор) УЦ осуществляет:

- ввод в эксплуатацию и установку нового ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата УЦ;

- производит в соответствии с технической и эксплуатационной документацией настройку средств УЦ для использования нового ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата УЦ;

- обеспечивает хранение и использование ключей электронной подписи и сертификатов ключей проверки электронной подписи УЦ в соответствии с требованиями безопасности, в форме, позволяющей обеспечить целостность и конфиденциальность ключей электронной подписи УЦ.

4.1.2.4. Порядок информирования владельцев квалифицированных сертификатов о смене ключей электронной подписи УЦ

4.1.2.4.1. Информирование участников электронного взаимодействия о проведении плановой смены ключа электронной подписи УЦ осуществляется посредством размещения на сайте УЦ информации о новом квалифицированном сертификате УЦ.

4.1.2.4.2. Предыдущий ключ электронной подписи УЦ действует в течение срока действия до вывода его из эксплуатации и используется для создания и подписания списка аннулированных сертификатов, созданных УЦ в период действия предыдущего ключа электронной подписи.

4.1.2.5. Внеплановая смена ключей электронной подписи УЦ

4.1.2.5.1. Внеплановая смена ключа электронной подписи осуществляется УЦ в случаях нарушения его конфиденциальности, угрозы нарушения его конфиденциальности (далее - внеплановая смена ключа электронной подписи), по техническим причинам (неисправность СКЗИ), внесения изменений в национальные стандарты в области криптографической защиты информации.

4.1.2.5.2. УЦ прекращает действие его сертификата и действие квалифицированного сертификата ключа проверки электронной подписи, созданных с использованием ключа электронной подписи УЦ, с занесением сведений в реестр прекративших действие и аннулированных сертификатов УЦ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

4.1.2.5.3. Информирование участников электронного взаимодействия о проведении внеплановой смены ключа электронной подписи УЦ осуществляется посредством размещения на сайте УЦ информации о новом квалифицированном сертификате УЦ.

4.1.3. Порядок осуществления смены ключей электронной подписи УЦ в случаях нарушения их конфиденциальности, содержащий основание, процедуры и сроки осуществления такой смены ключей электронной подписи УЦ, порядок информирования владельцев квалифицированных сертификатов об осуществлении такой смены. Доверенный способ получения нового квалифицированного сертификата УЦ

4.1.3.1. Смена ключа электронной подписи УЦ осуществляется в случае нарушения конфиденциальности ключа электронной подписи или угрозы нарушения конфиденциальности такого ключа электронной подписи. Одновременно со сменой такого ключа электронной подписи прекращается действие всех квалифицированных сертификатов, созданных с использованием этого ключа электронной подписи, с занесением сведений об этих квалифицированных сертификатах в соответствующий реестр квалифицированных сертификатов.

4.1.3.2. К случаям нарушения конфиденциальности ключей электронной подписи УЦ относятся:

а) получение доступа неуполномоченного лица к ключу электронной подписи УЦ или к ключевому носителю, содержащему ключ электронной подписи УЦ;

б) утрата или хищение карт доступа к программно-аппаратному криптографическому модулю, где хранится ключ электронной подписи УЦ, в том числе с их последующим обнаружением;

в) нарушение правил хранения и использования ключа электронной подписи УЦ или правил эксплуатации программно-аппаратного криптографического модуля, которое привело или могло привести к компрометации ключа электронной подписи УЦ;

г) нарушение целостности программно-аппаратного криптографического модуля и/или пломбирующих (опечатывающих) устройств;

д) несанкционированное копирование ключа электронной подписи УЦ;

е) утрата ключей от сейфов (шкафов, хранилищ) в случае нахождения в них ключевых носителей, содержащих ключи электронной подписи УЦ;

ж) случаи, когда невозможно достоверно установить, что произошло с ключевым носителем, в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута

возможность того, что данный факт произошел в результате несанкционированных действий нарушителя.

4.1.3.3. К угрозам нарушения конфиденциальности ключа электронной подписи УЦ относятся:

а) угрозы, связанные с несанкционированным доступом в помещения, где размещаются технические средства УЦ, или доступу к программно-аппаратному криптографическому модулю;

б) угрозы, связанные с проведением нарушителем атак на технические средства УЦ, в том числе на носители защищаемой информации, средства вычислительной техники, среду функционирования средств криптографической защиты информации и средств УЦ, каналы (линии) связи;

в) нарушение правил хранения и эксплуатации ключа электронной подписи УЦ.

4.1.3.4. Информирование владельцев квалифицированных сертификатов о проведении смены ключей УЦ осуществляется посредством направления на адрес электронной почты владельца квалифицированного сертификата или посредством размещения информации на сайте УЦ соответствующего уведомления о создании УЦ нового сертификата ключа проверки электронной подписи УЦ. Все действующие и приостановленные на момент нарушения конфиденциальности ключа электронной подписи УЦ сертификаты ключей проверки электронной подписи подлежат внеплановой смене.

4.1.3.5. После информирования о прекращении действия сертификата ключа проверки электронной подписи УЦ, УЦ обращается за получением квалифицированного сертификата в головной удостоверяющий центр, в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»

4.1.3.6. Смена ключей электронной подписи УЦ в случаях нарушения их конфиденциальности осуществляется в срок, не превышающий 10 (десяти) рабочих дней со дня установления факта нарушения его конфиденциальности.

4.1.3.7. Доверенным способом получения нового квалифицированного сертификата УЦ, исключающими уничтожение, модификацию, блокирование при передаче и иные неправомерные действия с квалифицированным сертификатом, являются:

- получение заявителем квалифицированного сертификата УЦ непосредственно в УЦ, в том числе при получении квалифицированного сертификата, созданного УЦ для заявителя;

- получение заявителем квалифицированного сертификата на сайте УЦ.

4.1.4. Порядок осуществления УЦ смены ключа электронной подписи владельца квалифицированного сертификата

4.1.4.1. Смена ключа электронной подписи владельца квалифицированного сертификата осуществляется в случаях, указанных в пунктах 1, 2, 4 части 6 и части 6.1 статьи 14 ФЗ «Об электронной подписи».

4.1.4.2. Смена ключа электронной подписи владельца квалифицированного сертификата осуществляется на основании заявления на смену ключа электронной подписи владельца квалифицированного сертификата.

4.2.1.3. Форма заявления на смену ключа электронной подписи владельца квалифицированного сертификата приведена в Приложении № 4 настоящего Порядка УЦ.

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

4.1.4.5. Процедура выдачи квалифицированного сертификата и ключа электронной подписи (при необходимости) владельцу, может осуществляться в том числе в электронной форме в соответствии со статьей 18 ФЗ «Об электронной подписи».

4.2. ПРОЦЕДУРА СОЗДАНИЯ И ВЫДАЧИ КВАЛИФИЦИРОВАННЫХ СЕРТИФИКАТОВ

4.2.1. Порядок подачи заявления на создание и выдачу квалифицированных сертификатов

4.2.1.1. Создание и выдача квалифицированного сертификата осуществляется УЦ на основании заявления на создание и выдачу квалифицированного сертификата.

4.2.1.2. Форма заявления на создание и выдачу квалифицированного сертификата приведена в Приложении № 1 настоящего Порядка УЦ.

4.2.1.3. Заявление на создание и выдачу квалифицированного сертификата подается лично заявителем в УЦ либо доверенному лицу, с которым у УЦ заключено соглашение.

4.2.2. Требования к заявлению на создание и выдачу квалифицированных сертификатов

4.2.2.1. Заявление на создание и выдачу квалифицированного сертификата может быть оформлено как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью, 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, устанавливаемыми Постановлением Правительства Российской Федерации от 25 января 2013 г. N 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг», при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" (по тексту - единая система идентификации и аутентификации) в соответствии с Постановлением Правительства Российской Федерации от 28 ноября 2011 г. N 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» и информации из государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (по тексту - единая биометрическая система) в соответствии с пунктом 4 статьи 2 572-ФЗ.

4.2.2.2. В заявлении на создание и выдачу квалифицированного сертификата указываются сведения в соответствии с требованиями ФЗ «Об электронной подписи», иных федеральных законов и нормативно-правовых актов Российской Федерации.

4.2.2.3. Заявление должно содержать:

- реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;
- страховой номер индивидуального лицевого счета - физического лица;
- идентификационный номер налогоплательщика - физического лица.

4.2.3. Порядок идентификации заявителя с указанием следующих положений в соответствии со статьей 18 ФЗ «Об электронной подписи»

4.2.3.1. Идентификации заявителя осуществляется в соответствии с положением статьи 18 ФЗ «Об электронной подписи».

4.2.3.2. Идентификация гражданина Российской Федерации осуществляется:

1) при его личном присутствии по основному документу, удостоверяющему личность;

2) без его личного присутствия:

с использованием усиленной квалифицированной электронной подписи при наличии действующего квалифицированного сертификата;

путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные. Реализация данного способа осуществляется с учетом требований постановления Правительства Российской Федерации от 8 ноября 2019 г. N 1427 «О проведении эксперимента по совершенствованию применения технологии электронной подписи» (Собрание законодательства Российской Федерации, 2019, N 46, ст. 6493);

путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном 572-ФЗ.

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

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

4.2.4. Перечень документов, запрашиваемых Удостоверяющим центром у заявителя для создания и выдачи квалифицированного сертификата, в том числе для удостоверения личности заявителя, в соответствии с частью 2 статьи 17 и частью 2 статьи 18 ФЗ «Об электронной подписи»

4.2.4.1. Для создания и выдачи квалифицированного сертификата, в том числе для удостоверения личности заявителя, в соответствии с частью 2 статьи 17 и частью 2 статьи 18 ФЗ «Об электронной подписи», вместе с заявлением на создание сертификата ключа проверки электронной подписи заявителем предоставляются следующие документы, либо их надлежащим образом заверенные копии и (или) сведения из них:

- основной документ, удостоверяющий личность;
- страховой номер индивидуального лицевого счета заявителя - физического лица;
- идентификационный номер налогоплательщика заявителя - физического лица.

2.2. УЦ с использованием инфраструктуры осуществляет проверку достоверности документов и сведений, предоставленных заявителем в соответствии с пунктом 4.2.4.1. Порядка УЦ.

4.2.5. Порядок проверки достоверности документов и сведений, представленных заявителем

4.2.5.1. Для заполнения квалифицированного сертификата в соответствии с частью 2 статьи 17 ФЗ «Об электронной подписи» УЦ запрашивает и получает из государственных информационных ресурсов сведения, предусмотренные статьей 18 ФЗ «Об электронной подписи».

4.2.5.2. В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и УЦ идентифицировал заявителя - физическое лицо, УЦ осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В ином случае УЦ отказывает заявителю в выдаче квалифицированного сертификата.

4.2.6. Порядок создания квалифицированного сертификата

4.2.6.1. Создание квалифицированного сертификата осуществляется УЦ в соответствии с положениями статей 13 – 15, 17 и 18 ФЗ «Об электронной подписи» и настоящим Порядком УЦ.

Порядок реализации АО «Торговый дом «ПЕРЕКРЕСТОК» функций
аккредитованного удостоверяющего центра и исполнения его обязанностей
Страница 13 из 35



4.2.6.2. В случае, если проверка, произведенная в соответствии с пунктом 4.2.5. Порядка УЦ, подтверждает достоверность информации, представленной заявителем при обращении в УЦ за получением квалифицированного сертификата, и УЦ идентифицирован заявителем, УЦ осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В противном случае, УЦ отказывает заявителю в выдаче квалифицированного сертификата.

4.2.6.3. УЦ запрещается указывать в создаваемом им сертификате ключа проверки электронной подписи ключ проверки электронной подписи, который содержится в сертификате ключа проверки электронной подписи, выданном УЦ любым другим удостоверяющим центром.

4.2.7. Порядок выдачи квалифицированного сертификата

4.2.7.1. При получении квалифицированного сертификата заявителем он должен быть ознакомлен УЦ с информацией, содержащейся в квалифицированном сертификате. Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку или 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. УЦ обязан хранить информацию, подтверждающую ознакомление заявителя с информацией, содержащейся в квалифицированном сертификате, в течение всего срока осуществления своей деятельности.

4.2.7.2. УЦ одновременно с выдачей квалифицированного сертификата предоставляет владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, приведенного в приложении N 5 к настоящему Порядку УЦ.

4.2.7.3. При выдаче квалифицированного сертификата УЦ направляет 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. При выдаче квалифицированного сертификата УЦ по желанию владельца квалифицированного сертификата безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации с проведением идентификации владельца при его личном присутствии.

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

4.2.8.1. Создание и выдача квалифицированного сертификата осуществляется УЦ в течение не более 5 (пяти) рабочих дней со дня получения заявления на создание и выдачу квалифицированного сертификата.

4.2.8.2. Срок создания и выдачи квалифицированного сертификата заявителя с момента получения УЦ заявления на создание и выдачу квалифицированного сертификата, а также надлежащие оформленных документов и сведений, представленных заявителем в УЦ для получения квалифицированного сертификата, зависит от сроков и результатов получения сведений, запрашиваемых УЦ с использованием инфраструктуры в соответствии с частью 2.2 и частью 2.3 статьи 18 ФЗ «Об электронной подписи» из государственных информационных ресурсов. Срок Порядок реализации АО «Торговый дом «ПЕРЕКРЕСТОК» функций аккредитованного удостоверяющего центра и исполнения его обязанностей

создания и выдачи квалифицированного сертификата может быть увеличен до 30 (тридцати) рабочих дней в случае несвоевременного получения сведений, находящихся в распоряжении государственных органов, иных органов, необходимых для создания квалифицированного сертификата.

4.2.8.3. Выдача квалифицированных сертификатов, созданных УЦ, осуществляется при условии выполнения Стороной, присоединившейся к Порядку УЦ, своих обязанностей.

4.2.8.4. Для создания и выдачи квалифицированного сертификата в течение дня, в который в УЦ подано заявление на создание и выдачу квалифицированного сертификата, заявитель должен произвести дополнительную оплату срочного оказания услуги и представить в УЦ платежное поручение с отметкой банка о том, что платеж произведен.

4.2.8.5. Для срочного создания и выдачи квалифицированного сертификата, заявитель может обратиться в УЦ. Срочное создание и выдача такого сертификата возможно только после получения и проверки всех необходимых сведений, установленных ФЗ «Об электронной подписи», принимаемых в соответствии с ним нормативно-правовых актов, и настоящим Порядком УЦ.

4.3. Подтверждение действительности электронной подписи, использованной для подписания электронных документов

4.3.1. Подтверждение действительности электронной подписи в электронном документе осуществляется УЦ по обращению Стороной на основании заявления, которое оформляется в соответствии с Приложением № 2 к настоящему Порядку УЦ и предоставляется в УЦ посредством почтовой, курьерской связи, а также путем направления заявления на адрес электронной почты УЦ или путем обращения по адресу нахождения УЦ.

4.3.1. Требования к заявлению на подтверждение действительности электронной подписи, в том числе перечень прилагаемых к такому заявлению документов

4.3.1.1. Заявление должно содержать следующую информацию:

- дата подачи заявления;
- идентификационные данные заявителя, подлинность электронной подписи которого необходимо подтвердить в электронном документе;
- фамилия, имя и отчество (при наличии) владельца квалифицированного сертификата, с использованием которого создана электронная подпись, действительность которой требуется подтвердить;
- дата и время, по состоянию на которые требуется подтвердить действительность электронной подписи;
- адрес, на который необходимо направить результаты подтверждения действительности электронной подписи.

4.3.1.2. В случае подачи заявления лично, обязательным приложением к заявлению на проверку электронной подписи в электронном документе является носитель информации, содержащий электронный документ.

4.3.1.3. В ходе проведения работ по подтверждению действительности электронной подписи в электронном документе УЦ может запросить дополнительную информацию у обратившейся Стороны.

4.3.2. Срок предоставления услуги по подтверждению действительности электронной подписи в электронном документе

4.3.2.1. Срок предоставления услуги по подтверждению действительности электронной подписи в электронном документе не может превышать 5 (пять) рабочих дней с момента поступления и регистрации заявления в УЦ.

4.3.3. Порядок оказания услуги

4.3.3.1. Проверка действительности электронной подписи электронного документа осуществляется сертифицированными средствами электронной подписи.

4.3.3.2. Проверка действительности электронной подписи, используемой для подписания электронного документа, осуществляется посредством инфраструктуры УЦ и включает в себя проверку действительности всех квалифицированных сертификатов, включенных в последовательность проверки от проверяемого квалифицированного сертификата до квалифицированного сертификата УЦ, выданного ему головным удостоверяющим центром в соответствии с процедурой, установленной эксплуатационной документацией на средства УЦ, предназначенные для подтверждения подлинности электронной подписи в электронном документе.

4.3.3.3. Результатом проведения работ по подтверждению действительности электронной подписи в электронном документе является ответ УЦ обратившейся Стороне, направляемый по адресу, указанному в заявлении на подтверждение действительности электронной подписи.

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

4.4.1. Основания прекращения действия или аннулирования квалифицированного сертификата

4.4.1.1. Квалифицированный сертификат прекращает свое действие в случаях, установленных статьей 14 Федерального закона «Об электронной подписи».

4.4.1.2. УЦ признает квалифицированный сертификат аннулированным, если:

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

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

4.4.2.1. Прекращение действия квалифицированного сертификата осуществляется по заявлению его владельца, которое оформляется в соответствии с Приложением № 3 к настоящему Порядку УЦ.

4.4.2.2. Заявление о прекращении действия квалифицированного сертификата подается в УЦ как на бумажном носителе, так и направляется в форме электронного документа, подписанного усиленной квалифицированной электронной подписью, в том числе с использованием федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» (далее - Единый портал),

Заявление должно содержать:

- серийный номер квалифицированного сертификата;
- страховой номер индивидуального лицевого счёта (СНИЛС); - даты начала и окончания действия квалифицированного сертификата;
- наименование аккредитованного удостоверяющего центра, выдавшего квалифицированный сертификат;
- фамилия, имя, отчество (при наличии) владельца квалифицированного сертификата;
- причины прекращения действия квалифицированного сертификата, а также:

в отношении физического лица, не являющегося индивидуальным предпринимателем: фамилии, имени, отчества (при наличии), страхового номера индивидуального лицевого счета, идентификационного номера налогоплательщика;

в отношении физического лица, являющегося индивидуальным предпринимателем: фамилии, имени, отчества (при наличии), основного государственного регистрационного номера индивидуального предпринимателя, страхового номера индивидуального лицевого счета, идентификационного номера налогоплательщика;

в отношении иностранной организации: наименования организации и идентификационного номера налогоплательщика (при наличии).

- иные необходимые реквизиты, включая подпись.

4.4.2.3. УЦ осуществляет прием заявления на прекращение действия сертификата при условии установления личности лица, подающего заявление, в случае подачи заявления в форме документа на бумажном носителе, или при установлении действительности квалифицированной электронной подписи, которой подписано заявление, подаваемое в форме электронного документа.

4.4.2.4. При ошибках в оформлении заявления или несовпадении данных из представленного заявления с данными, хранящимися в реестре УЦ, УЦ имеет право отказать заявителю в регистрации заявления и прекращении действия сертификата или запросить дополнительные документы, подтверждающие изменение данных по своему усмотрению.

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

4.4.3.1. Внесение информации о прекращении действия или аннулировании сертификата в реестр квалифицированных сертификатов осуществляется путем внесения соответствующей информации в список аннулированных сертификатов.

4.4.3.2. Срок внесения информации о прекращении действия и (или) об аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов не может превышать 12 (двенадцать часов) с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона «Об электронной подписи», или в течение двенадцати часов с момента получения УЦ соответствующих сведений.

4.4.3.3. В случае направления Заявителем заявления о прекращении действия квалифицированного сертификата с использованием Единого портала принятого по такому заявлению решение УЦ в форме электронного документа, подписанного усиленной квалифицированной электронной подписью УЦ, размещается в личном кабинете Заявителя на Едином портале после проведения проверки действительности усиленной квалифицированной электронной подписи УЦ, которой такое решение подписано, и подтверждения ее действительности. В случае принятия по такому заявлению решения о прекращении действия квалифицированного сертификата УЦ после внесения соответствующей информации в реестр квалифицированных сертификатов направляет на Единый портал информацию о прекращении действия квалифицированного сертификата. Взаимодействие УЦ с Единым порталом в рамках реализации норм, предусмотренных настоящим абзацем, осуществляется посредством единой системы межведомственного электронного взаимодействия.

4.5. Порядок ведения реестра квалифицированных сертификатов

4.5.1. Реестр квалифицированных сертификатов ведется УЦ в электронной форме в соответствии с требованиями, установленными Порядком формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, включая требования к формату предоставления такой информации, утвержденным приказом Минцифры России от 08.11.2021 N 1138, и кроме информации, содержащейся в квалифицированных сертификатах, включает также информацию о датах прекращения действия или аннулирования

квалифицированных сертификатов и об основаниях прекращения действия или аннулирования, а также иную информацию, подлежащую включению в реестр в соответствии с требованиями нормативных правовых документов.

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

4.5.1. Формы ведения реестра квалифицированных сертификатов

4.5.1.1. Формирование и ведение реестра квалифицированных сертификатов включает в себя:

- внесение информации о квалифицированных сертификатах в реестр квалифицированных сертификатов;
- внесение изменений в реестр квалифицированных сертификатов в случае изменения содержащихся в нем сведений о квалифицированных сертификатах;
- внесение в реестр квалифицированных сертификатов сведений о прекращении действия или об аннулировании квалифицированных сертификатов;
- хранение информации, содержащейся в реестре квалифицированных сертификатов;
- предоставление сведений из реестра квалифицированных сертификатов.

4.5.1.2. УЦ обеспечивает актуальность информации, содержащейся в реестре квалифицированных сертификатов.

4.5.1.3. Информация о квалифицированном сертификате вносится УЦ в реестр квалифицированных сертификатов не позднее указанной в нем даты начала действия такого квалифицированного сертификата.

4.5.1.4. Информация, внесенная в реестр квалифицированных сертификатов, подлежит хранению в течение всего срока деятельности УЦ, если иной срок не установлен законодательством Российской Федерации.

4.5.1.5. Хранение информации, содержащейся в реестре квалифицированных сертификатов, осуществляется в форме, позволяющей проверить ее целостность и достоверность.

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

4.5.1.7. УЦ обеспечивает любому лицу безвозвратный доступ с использованием информационно-телекоммуникационных сетей к реестру квалифицированных сертификатов в любое время в течение срока деятельности УЦ, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

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

4.5.2.1. Информация о выданных УЦ квалифицированных сертификатах вносится в реестр сертификатов одновременно с их выдачей, но не позднее даты начала действия квалифицированного сертификата, указанной в квалифицированном сертификате.

4.5.2.2. Информация о прекращении действия и аннулировании квалифицированного сертификата вносится в реестр сертификатов УЦ не позднее 12 (двенадцати) часов с момента наступления обстоятельств, приводящих к аннулированию квалифицированного сертификата, или в течение 12 (двенадцати) часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств.

4.5.2.3. Срок внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов не может превышать двенадцать часов с момента наступления обстоятельств, указанных в частях 6 и 6.1

статьи 14 Федерального закона «Об электронной подписи», или в течение двенадцати часов с момента получения УЦ соответствующих сведений.

4.5.2.4. УЦ до внесения в реестр сертификатов информации об аннулировании сертификата ключа проверки электронной подписи уведомляет владельца квалифицированного сертификата ключа проверки электронной подписи об аннулировании его сертификата ключа проверки электронной подписи путем направления документа на бумажном носителе или электронного документа.

4.6. Порядок технического обслуживания реестра квалифицированных сертификатов

4.6.1. Плановые технические работы по обслуживанию реестра сертификатов, в том числе процедуры резервного копирования, проводятся УЦ в выходные дни либо в ночное время (с учетом часовых поясов на территории Российской Федерации, Москва UTC+3).

4.6.2. Внеплановые технические работы по обслуживанию реестра сертификатов проводятся в оперативном режиме при выявлении такой необходимости.

4.6.1. Максимальные сроки проведения технического обслуживания

4.6.1.1. Техническое обслуживание реестра сертификатов при проведении плановых технических работ осуществляется не более 8 (восеми) часов с момента их начала.

Техническое обслуживание реестра сертификатов при проведении внеплановых технических работ осуществляется не более 24 (двадцати четырех) часов с момента их начала.

4.6.1.2. Время проведения технического обслуживания может быть увеличено при наличии оснований и причин, но не более чем на 10 (десять) дней со дня их начала.

4.6.2. Порядок уведомления участников информационного взаимодействия о проведении технического обслуживания

4.6.2.1. Перед проведением плановых (внеплановых) работ по техническому обслуживанию реестра сертификатов, если такие работы могут повлиять на возможность создания или проверки электронной подписи участниками электронного взаимодействия, УЦ оповещает о проведении вышеуказанных работ посредством публикации соответствующей информации на сайте УЦ и (или) направления уведомления в электронной форме с использованием информационно-телекоммуникационных сетей, в том числе с использованием электронной почты.

5. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА, УСТАНОВЛЕННЫХ ФЕДЕРАЛЬНЫМ ЗАКОНОМ ОТ 6 АПРЕЛЯ 2011 Г. N 63-ФЗ «ОБ ЭЛЕКТРОННОЙ ПОДПИСИ» И ПРИНИМАЕМЫМИ В СООТВЕТСТВИИ С НИМ НОРМАТИВНЫМИ ПРАВОВЫМИ АКТАМИ

5.1 информирование заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки

5.1.1. УЦ информирует всех участников электронного взаимодействия об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки следующими способами:

5.1.1.1 путем размещения настоящего Порядка УЦ на сайте УЦ, а также руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи, которое приведено в приложении № 5 к настоящему Порядку УЦ, отдельным документом в электронной форме на сайте УЦ;

5.1.1.2 путем ознакомления с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенного в приложении № 5 к настоящему Порядку УЦ, в момент присоединения к Порядку УЦ;

5.2 Выдача по обращению заявителя средств электронной подписи

5.2.1. Средства электронной подписи, используемые заявителем, должны соответствовать требованиям части 4 статьи 6 и статьи 12 Федерального закона «Об электронной подписи», Требованиям к средствам электронной подписи, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796, а также обеспечивать возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подпавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями.

5.2.2. Порядок использования средств электронной подписи определяется эксплуатационной документацией на средство электронной подписи и лицензионным соглашением, условия которой определяет правообладатель.

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

5.3.1. УЦ обеспечивает актуальность информации, содержащейся в реестре сертификатов, а также защиту информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

5.3.2. Актуальность информации, содержащейся в реестре сертификатов, обеспечивается путем соблюдения порядка формирования и ведения реестра сертификатов в соответствии с условиями настоящего Порядка УЦ.

5.3.3. Защита информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий обеспечивается путем реализации комплекса организационных и технических мер по обеспечению информационной безопасности инфраструктуры УЦ, обеспечению защиты информации, обрабатываемой с использованием средств УЦ, которые в том числе включают меры по защите информации, содержащейся в реестре сертификатов, путем реализации следующих мероприятий:

- обеспечивается контроль доступа в помещения, где размещены технические средства УЦ;
- реализована ролевая модель доступа к компонентам средств УЦ, обеспечивается идентификация, аутентификация и разграничение доступа уполномоченных лиц к программным и техническим средствам УЦ и защищаемой информации;
- обеспечивается контроль действий уполномоченных лиц УЦ и обслуживающего персонала, принятые меры по предотвращению несанкционированного доступа к средствам УЦ и защищаемой информации;
- формирование и ведение реестра сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему;
- осуществляется регулярное резервное копирование информации, содержащейся в реестре сертификатов с соблюдением требований к защите от несанкционированного доступа к средствам резервного копирования и резервируемой информации;
- для хранения информации используются опечатываемые хранилища информации (металлические шкафы, сейфы, пеналы).

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

5.4.1 УЦ в соответствии с пунктом 3 части 2 статьи 13 и частью 3 статьи 15 Федерального закона «Об электронной подписи» обеспечивает безвоздемный круглосуточный доступ к реестру сертификатов, при обращении к нему любого лица с использованием сети «Интернет» в любое время, за исключением периодов технического обслуживания реестра сертификатов, проводимых УЦ в соответствии с условиями настоящего Порядка УЦ.

5.4.2. Информация, содержащаяся в реестре квалифицированных сертификатов УЦ, доступна на сайте УЦ или предоставляется путем подачи заявки по адресу электронной почты УЦ.

5. Порядок обеспечения конфиденциальности созданных УЦ ключей электронных подписей

5.5.1. Конфиденциальность ключей электронных подписей, а также ключа электронной подписи УЦ, обеспечивается путем реализации комплекса организационных и технических мер по обеспечению информационной безопасности инфраструктуры УЦ, обеспечению защиты информации, обрабатываемой с использованием средств УЦ.

5.5.2. Хранение и использование ключей электронной подписи УЦ и ключей электронной подписи уполномоченных лиц УЦ осуществляется в соответствии с требованиями 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», в форме, позволяющей обеспечить целостность и конфиденциальность ключей электронной подписи УЦ.

5.5.3. Средства УЦ, с использованием которых осуществляется использование и хранение ключей электронной подписи УЦ и ключей электронной подписи уполномоченных лиц УЦ, имеют документ, подтверждающий оценку соответствия по требованиям безопасности информации и соответствуют Требованиям к средствам электронной подписи и Требованиям к средствам удостоверяющего центра, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796.

5.5.4. Владелец, получивший квалифицированный сертификат в УЦ, обеспечивает конфиденциальность ключей электронных подписей и обязан:

- хранить в тайне ключ электронной подписи, принимать все возможные меры для предотвращения его утраты, раскрытия, искажения и несанкционированного использования;
- не допускать использование принадлежащих ему ключей электронных подписей без своего согласия;
- уведомлять УЦ и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- не использовать ключ электронной подписи, если ему стало известно, что этот ключ используется или использовался ранее другими лицами;
- обеспечивать незамедлительное уничтожение принадлежащих им ключей электронных подписей по истечении сроков действия данных ключей в отношении усиленных квалифицированных электронных подписей. Для уничтожения ключей электронных подписей должны применяться прошедшие в установленном порядке процедуру оценки соответствия средства электронной подписи, в составе которых реализована функция уничтожения информации;
- не использовать ключ электронной подписи и немедленно обратиться в УЦ, выдавший квалифицированный сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена.

5.5.5. Ключи электронной подписи УЦ и уполномоченных лиц УЦ выводятся из эксплуатации при окончании срока их действия.

5.5.6. УЦ не осуществляет хранение (в том числе временное хранение) ключей электронной подписи, а также носителей ключевой информации, содержащих ключи электронной подписи владельца квалифицированного сертификата.

5.5.7. В случае аннулирования или досрочного прекращения действия квалифицированного сертификата, выданного УЦ, выдавшему квалифицированный сертификат заявителю, либо в случае досрочного прекращения или истечения срока аккредитации УЦ квалифицированный сертификат, выданный УЦ заявителю, прекращает свое действие.

5.6 Осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 ФЗ «Об электронной подписи»

5.6.1. УЦ при выдаче квалифицированного сертификата владельцу квалифицированного сертификата осуществляет регистрацию квалифицированного сертификата в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 ФЗ «Об электронной подписи».

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

5.7.1. При выдаче квалифицированного сертификата УЦ с использованием специализированного программного обеспечения и инфраструктуры УЦ, по желанию владельца квалифицированного сертификата безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации и (или) осуществляет подтверждение учетной записи в единой системе идентификации и аутентификации.

5.8. 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

5.8.1. УЦ предоставляет безвозмездно любому лицу доступ к информации, содержащейся в реестре сертификатов УЦ, по соответствующему запросу.

5.8.2. УЦ предоставляет безвозмездно любому лицу по его обращению сведения, содержащиеся в реестре сертификатов, в том числе информацию об аннулировании квалифицированного сертификата.

5.8.3. УЦ предоставляет безвозмездно любому лицу доступ к информации о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, путем публикации актуального перечня прекративших свое действие (аннулированных) квалифицированных сертификатов в виде электронного документа (списка аннулированных сертификатов), включающий в себя список серийных номеров квалифицированных сертификатов, которые аннулированы или действие которых было прекращено.

5.8.4. В целях обеспечения гарантированного доступа участников электронного взаимодействия к списку аннулированных сертификатов УЦ обеспечивается публикация списка аннулированных сертификатов на сайте УЦ.

5.8.5. Внесение информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов осуществляется УЦ в соответствии с условиями настоящего Порядка УЦ.

6. ТЕРМИНЫ И СОКРАЩЕНИЯ

№	Термин / сокращение	Определение
1.	Аkkредитация удостоверяющего центра	признание соответствия удостоверяющего центра требованиям Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»
2.	Владелец квалифицированного сертификата ключа проверки электронной подписи	лицо, которому в установленном Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» порядке выдан квалифицированный сертификат ключа проверки электронной подписи
3.	Доверенное лицо удостоверяющего центра	третьи лица на основании заключенного с удостоверяющим центром соглашения или на основании нормативного правового акта Российской Федерации наделенные полномочиями по приему заявлений на выдачу сертификатов ключей проверки электронной подписи, а также вручению сертификатов ключей проверки электронных подписей от имени удостоверяющего центра
4.	Информация	сведения (сообщения, данные) независимо от формы их представления
5.	Заявитель	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
6.	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 квалифицированного сертификата ключа проверки электронной подписи
7.	Средства удостоверяющего центра	программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра
8.	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
9.	Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат)	сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 6 апреля 2011 г. № 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
10.	Ключ электронной подписи	уникальная последовательность символов, предназначенная для создания электронной подписи
11.	Ключ проверки электронной подписи	уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи
12.	Порядок реализации АО «Торговый дом «ПЕРЕКРЕСТОК» функций аккредитованного удостоверяющего центра и исполнения его обязанностей	документ, определяющий условия предоставления услуг, включая права, обязанности Удостоверяющего центра АО «Торговый дом «ПЕРЕКРЕСТОК»

№	Термин / сокращение	Определение
13.	Реестр квалифицированных сертификатов ключей проверки электронных подписей	реестр выданных и аннулированных удостоверяющим центром сертификатов ключей проверки электронных подписей в том числе включающий в себя информацию, содержащуюся в выданных удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования
14.	Удостоверяющий центр	АО «Торговый дом «ПЕРЕКРЕСТОК», осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»
15.	Электронный документ	информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах
16.	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

7. СВЯЗАННЫЕ ДОКУМЕНТЫ

№	Наименование документа
	Внешние документы (источники права, стандарты и др.)
1.	Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»
2.	Приказ Минцифры России от 13.11.2020 N 584 «Об утверждении Требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей»

Приложение № 1 к Порядку УЦ

Форма заявления на создание и выдачу квалифицированного сертификата

Заявитель:

ФИО:

Фамилия Имя Отчество Заявителя

Паспорт: серия

№

Дата выдачи:

Выдан:

Электронная почта

Заявление на создание и выдачу квалифицированного сертификата

Прошу изготовить мне (Заявителю) квалифицированный сертификат ключа проверки электронной подписи (сертификат) в УЦ, в соответствии со следующими идентификационными данными:

1. commonName Фамилия Имя Отчество Заявителя

2. surname Фамилия Заявителя

3. givenName Имя Отчество Заявителя

4. eMail Адрес электронной почты

5. localityName Наименование населенного пункта Заявителя

6. stateOrProvinceName Код региона с указанием названия региона через пробел

■ [View Address Book](#)

7. streetAddress Название улицы, номер дома, корпуса, строения, квартиры

© INNOMILIS

8. ИНН ИНН заявителя

2. СНИЛС. Справочный листок с информацией о выданной единой лицензии лечащего врача (СНИЛС). Заполните

9. SNILS Страховой номер индивидуального лицевого счета (СНИЛС) заявителя

10. Настоящим подтверждаю, что:



- 10.1.** приведенные выше данные являются достоверными, в заявлении указаны правильно, мною также представлены документы, подтверждающие сведения, указанные в заявлении или их надлежащим образом заверенные копии;
- 10.2.** ознакомлен со всеми условиями Договора, обязуюсь полностью и безусловно их соблюдать;
- 10.3.** ознакомлен с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи;
- 10.4.** в соответствии со статьей 428 ГК РФ полностью и безусловно присоединяюсь к Порядку УЦ, соглашаюсь со всеми его условиями, обязуюсь соблюдать все его положения;
- 10.5.** ознакомлен с Порядком УЦ размещенным на сайте УЦ в сети Интернет по адресу <https://cdp.x5.ru>.

Заявитель

Ф.И.О. полностью

подпись

дата, время подачи

Форма заявления на подтверждение действительности электронной подписи

Заявитель:

ФИО:

Фамилия Имя Отчество Заявителя

Паспорт: серия

№

Дата выдачи:

Выдан:

Электронная почта

Заявления на подтверждение действительности электронной подписи

1. Прошу подтвердить действительность электронной подписи на основании следующих данных:
- фамилия, имя и отчество (при наличии) владельца квалифицированного сертификата, с использованием которого создана электронная подпись, действительность которой требуется подтвердить

- дата и время, по состоянию на которые требуется подтвердить действительность электронной подписи

- файл, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № _____;
- файл, содержащий подписанные электронной подписью данные и значение электронной подписи, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи, на прилагаемом к заявлению носителе – рег. № _____.

Прошу направить результаты подтверждения действительности электронной подписи на адрес электронной почты.

Заявитель

Ф.И.О. полностью

подпись

дата, время подачи

Форма заявления о прекращении действия квалифицированного сертификата

Заявитель:

ФИО:

Фамилия Имя Отчество Заявителя

Паспорт: серия

№

Дата выдачи:

Выдан:

Электронная почта

Заявление о прекращении действия квалифицированного сертификата

Прошу прекратить действие моего сертификата ключа проверки электронной подписи выданного УЦ, содержащего следующие данные:

причина прекращения действия квалифицированного сертификата	
уникальный серийный номер квалифицированного сертификата	
страховой номер индивидуального лицевого счёта (СНИЛС)	
даты начала и окончания действия квалифицированного сертификата	
фамилия, имя, отчество (при наличии) владельца квалифицированного сертификата	
идентификационный номер налогоплательщика	
наименование аккредитованного удостоверяющего центра, выдавшего квалифицированный сертификат	

Заявитель

Ф.И.О. полностью

подпись

дата, время подачи

Приложение 4 к Порядку УЦ

Форма заявления на смену ключа электронной подписи

Заявитель:

ФИО:

Фамилия Имя Отчество Заявителя

Паспорт: серия

№

Дата выдачи:

Выдан:

Электронная почта

Заявление на смену ключа электронной подписи

Ф.И.О. полностью, СНИЛС

в связи с

(указывается причина смены ключа электронной подписи (например, истечение срока действия сертификата, его отзыве и т.д.)

прошу взамен ранее созданного ключа электронной подписи и ключа проверки электронной подписи, указанного в созданном УЦ квалифицированном сертификате ключа проверки электронной подписи с серийным номером _____, изготовить новый ключ электронной подписи и ключ проверки электронной подписи.

Заявитель

Ф.И.О. полностью

подпись

дата, время подачи

Форма руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

1 Общие положения

1.1. Настоящее руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (далее – руководство) подготовлено в соответствии с частью 4 статьи 18 ФЗ «Об электронной подписи».

1.2. Руководство предназначено для официального информирования владельца квалифицированного сертификата ключа проверки электронной подписи, выдаваемого УЦ, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

2. Риски, связанных с использованием электронных подписей

2.1. Основными рисками, связанными с использованием электронной подписи, являются:

2.1.1. риски, связанные с нарушением целостности электронного документа и возможностью отказа от него.

Данные риски могут быть связаны с внесенными в электронный документ изменениями, произведенными после его подписания. Лицо, подписавшее электронный документ квалифицированной электронной подписью, или лицо, осуществляющее проверку такой электронной подписи, может заявить о том, что содержание электронного документа было изменено после его подписания и электронный документ не соответствует тому документу, который был подписан квалифицированной электронной подписью;

2.1.2. риски, связанные с проверкой принадлежности ключа электронной подписи, с помощью которой подписан электронный документ, владельцу квалифицированного сертификата ключа проверки электронной подписи (далее – владелец квалифицированного сертификата).

Лицо, владеющее сертификатом ключа проверки электронной подписи и соответствующим ключом электронной подписи, которым был подписан электронный документ, может заявить о том, что квалифицированная электронная подпись, содержащаяся в электронном документе, не принадлежит данному владельцу квалифицированного сертификата;

2.1.3. риски, связанные с признанием юридической силы электронного документа, подписанного квалифицированной электронной подписью.

Одна из Сторон может заявить о том, что подписанный квалифицированной электронной подписью документ не может порождать юридически значимых последствий или считаться достаточным доказательством в суде;

2.1.4. риски, связанные с нарушением конфиденциальности ключей электронной подписи (использование ключей электронной подписи без согласия владельца).

В случае нарушения конфиденциальности ключей электронной подписи, в том числе компрометации ключей, несанкционированного доступа к ключевым носителям или средствам электронной подписи, участником электронного взаимодействия может быть принят в исполнение подписаны квалифицированной электронной подписью документ, порождающий юридически значимые последствия.

Нарушение конфиденциальности ключа электронной подписи (в том числе нарушение правил хранения ключа электронной подписи, несоблюдение требований Порядка УЦ в случаях прекращения либо аннулирования действия сертификата ключа подписи) или нарушение правил

эксплуатации средств квалифицированной электронной подписи может привести к нарушению прав и законных интересов владельца квалифицированного сертификата и/или третьих лиц.

2.1.5. риски, связанные с использованием несертифицированных средств, предназначенных для защиты информации.

Использование для создания и проверки квалифицированных электронных подписей, создания ключа электронной подписи и ключа проверки электронной подписи несертифицированных в соответствии с правилами сертификации Российской Федерации средств электронной подписи, и применение этих средств в нарушение правил, установленных нормативными правовыми актами Российской Федерации, а также эксплуатационной документации к средствам электронной подписи, может повлечь административную ответственность.

2.1.6. риски, связанные с определением полномочий лица, подписавшего электронной подписью документ.

В случае, если участниками электронного взаимодействия не определены лица, участвующие в электронном взаимодействии, полномочия данных лиц по подписанию электронных документов от имени участника электронного взаимодействия, а также в случае, если полномочия лица по подписанию электронных документов прекращены, одна из Сторон может заявить, что полученный электронный документ содержит квалифицированную электронную подпись лица, не уполномоченного на подписание данного документа и не может быть принят в исполнение.

2.1.7. риски, связанные с использованием сертификатов ключей проверки электронной подписи и ключей электронной подписи, прекративших своё действие.

В случае использования для подписания электронных документов ключа электронной подписи, прекратившего своё действие на момент подписания, либо, если момент подписания электронного документа не определен, а также в случае использования сертификата ключа проверки электронной подписи, который стал недействующим на день проверки электронной подписи, сторона, получившая подписанный квалифицированной электронной подписью документ, может заявить о непризнании такого электронного документа.

2.1.8. риски, связанные с неактуальностью данных в сертификате.

В случае, если в период действия сертификата персональных данных владельца произошли изменения, необходимо обратиться в УЦ для получения нового сертификата. В противном случае, любой электронный документ, подписанный данным сертификатом, может быть признан недействительным.

3. Меры, необходимые для обеспечения безопасности электронных подписей и их проверки.

3.1. Правовые и организационно-технические мероприятия для при осуществлении электронного взаимодействия с использованием электронной подписи.

3.1.1. В целях снижения вероятности возникновения и реализации указанных рисков владельцу квалифицированного сертификата необходимо предусмотреть обеспечение комплекса правовых и организационно-технических мероприятий по обеспечению информационной безопасности при осуществлении электронного взаимодействия с использованием электронной подписи.

3.1.2. Электронное взаимодействие с использованием электронной подписи и сертифицированных средств электронной подписи, осуществляется с учетом требований ФЗ «Об электронной подписи», других федеральных законов, принимаемых в соответствии с ними нормативных правовых актов, регулирующих отношения в области использования электронных подписей, в том числе:

- 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, утвержденной приказом ФАПСИ от 13.06.2001 N 152;

- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. N 66, в части эксплуатации средств криптографической защиты информации.

3.1.3. Средства усиленной квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата в соответствии с положениями эксплуатационной документации на применяемое средство усиленной квалифицированной электронной подписи.

3.1.4. На компьютерах с установленными средствами усиленной квалифицированной электронной подписи должно использоваться только лицензионное программное обеспечение. Для предотвращения заражения компьютера с установленными средствами усиленной квалифицированной электронной подписи необходимо обеспечить непрерывную комплексную защиту компьютера от вирусов, хакерских атак, спама, шпионского программного обеспечения и других вредоносных программ антивирусным программным обеспечением с рекомендуемым разработчиком периодом обновления антивирусных баз.

Владелец квалифицированного сертификата несет ответственность за то, чтобы на компьютере, на котором установлены средства криптографической защиты информации, не было установлено и не эксплуатировалось программное обеспечение (в том числе, - вирусы), которые могут нарушить функционирование программных средств криптографической защиты информации. При обнаружении на рабочем месте, оборудованном средствами криптографической защиты информации, 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.

3.1.5. Помещения, в которых установлены средства усиленной квалифицированной электронной подписи или хранятся носители ключей электронной подписи, должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

В помещениях, где установлены и применяются средства усиленной квалифицированной электронной подписи для хранения носителей ключей электронной подписи, эксплуатационной и технической документации, дистрибутивов программного обеспечения средств усиленной квалифицированной электронной подписи, необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, в целях предотвращения несанкционированного доступа к средствам усиленной квалифицированной электронной подписи.

Используемые или хранимые средства усиленной квалифицированной электронной подписи, эксплуатационная и техническая документация к ним, носители Ключей электронной подписи подлежат поэкземплярному учету в соответствии с требованиями 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».

3.2. Владелец квалифицированного сертификата обязан соблюдать определенные меры для обеспечения безопасности своих действий:

3.2.1. не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

3.2.2. для хранения ключа электронной подписи применять защищенный носитель информации, совместимый одновременно со средством электронной подписи, применяемым владельцем квалифицированного сертификата, и средствами УЦ;

3.2.3. применять для создания электронной подписи только действующий ключ электронной подписи;

3.2.4. прекратить использование ключа электронной подписи и немедленно обратиться в УЦ с заявлением о прекращении действия квалифицированного сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи;

3.2.5. не использовать сертификат ключа проверки электронной подписи, заявление на прекращение действия, которого подано в УЦ, в течение времени, исчисляемого с момента подачи заявления на прекращение действия сертификата в УЦ по момент официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия;

3.2.6. не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован;

3.2.7. использовать для создания и проверки квалифицированных электронных подписей, создания ключа электронной подписи и ключа проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи, и применять эти средства в соответствии с правилами, установленными нормативными правовыми актами Российской Федерации;

3.2.8. использовать при проверке электронной подписи в электронных документах актуальную информацию о сертификатах ключей проверки электронных подписей, которые на данный момент времени аннулированы, действие которых прекращено, содержащуюся в списке отозванных сертификатов, размещенном в сети Интернет на сайте УЦ;

3.2.9. в случае изменения персональных данных, включенных в сертификат ключа проверки электронной подписи, необходимо обратиться в УЦ с целью замены данного сертификата.

3.3. С учетом указанных правовых и организационно-технических мероприятий, обязанностей, владельцу квалифицированного сертификата запрещается:

3.3.1. осуществлять несанкционированное копирование ключевых носителей;

3.3.2. оставлять без контроля вычислительные средства, на которых эксплуатируется средства квалифицированной электронной подписи, после ввода ключевой информации либо иной конфиденциальной информации;

3.3.3. вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;

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

3.3.5. записывать на ключевые носители постороннюю информацию;

3.3.6. подключать к компьютеру с установленным средством квалифицированной электронной подписи дополнительные устройства и соединители;

3.4. Меры по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной электронной подписи.

3.4.1. Владелец квалифицированного сертификата обеспечивает безопасность ключей квалифицированной электронной подписи с помощью следующих методов:

3.4.1.1. ключи квалифицированной электронной подписи при их создании должны записываться на предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним;

3.4.1.2. ключевые носители должны иметь маркировку с учетным номером.

3.4.2. Владелец квалифицированного сертификата обеспечивает безопасное и надежное хранение и обращение с ключевой информацией и ключевыми носителями. Это достигается за счет соблюдения следующих способов и мер безопасности, которые гарантируют сохранность и конфиденциальность данных:

3.4.2.1. недопустимо пересыпать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме открытых ключей);

3.4.2.2. размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной электронной подписи, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками;

3.4.2.3. носители ключевой информации должны использоваться только владельцем квалифицированного сертификата и храниться в месте, не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.);

3.4.2.4. носитель ключевой информации должен быть вставлен вчитывающее устройство только на время выполнения средствами квалифицированной электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

3.4.2.5. на носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

3.4.3. Владелец квалифицированного сертификата обеспечивает безопасность автоматизированного рабочего места с установленными средствами квалифицированной электронной подписи.

3.4.3.1. С целью контроля исходящего и входящего подозрительного трафика технические средства с установленными средствами квалифицированной электронной подписи должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранования. На технических средствах, используемых для работы в информационных системах:

- на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям информационной безопасности;
- должно быть установлено только лицензионное программное обеспечение;
- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;
- должны регулярно устанавливаться обновления операционной системы;
- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами квалифицированной электронной подписи и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в соответствующей информационной системе;
- должна быть активирована регистрация событий информационной безопасности;
- должна быть включена автоматическая блокировка экрана после ухода владельца квалифицированного сертификата с автоматизированного рабочего места.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства квалифицированной электронной подписи, необходимо гарантированно удалить всю информацию (при условии исправности технических средств), использование которой третьими лицами может потенциально нанести вред владельцу квалифицированного сертификата и УЦ, в том числе средства квалифицированной электронной подписи, журналы работы систем обмена электронными документами и так далее.

3.4.4. В случае нарушения конфиденциальности ключей электронной подписи владелец квалифицированного сертификата, с учетом условий Порядка УЦ:

- незамедлительно обращается в УЦ;
- прекращение действия квалифицированного сертификата осуществляется по заявлению, которое оформляется в соответствии с Приложением № 3 к Порядку УЦ. Заявление о прекращении действия квалифицированного сертификата может подаваться в УЦ как на бумажном носителе, так и направляется в форме электронного документа, подписанного усиленной квалифицированной электронной подписью.